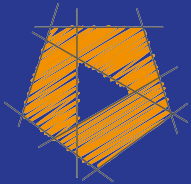


SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>



Exam Released May 2021

<https://t.me/learningnets>

Latest Update July 2024

<https://t.me/learningnets>

SCI - Security, Compliance, Identity

Microsoft Azure SCI Fundamentals

“familiar with Microsoft Azure and Microsoft 365 and want to understand how Microsoft security, compliance, and identity solutions can span across these solution areas to provide a holistic and end-to-end solution”

Microsoft Azure SCI Fundamentals

- Business stakeholders
- New or existing IT professionals
- Students who have an interest in security, compliance and identity solutions

Microsoft Azure SCI Fundamentals

- Describe the concepts of security, compliance, and identity
 - Describe the capabilities of Microsoft Entra
- Describe the capabilities of Microsoft security solutions
- Describe the capabilities of Microsoft compliance solutions

You'll be prepared
to take and pass
the SC-900 exam



Created by Adrien Coquet
from Noun Project

But you don't have to, if you just want to learn security, compliance, and identity concepts



Created by Adrien Coquet
from Noun Project

Security is a
fundamental design
requirement



Created by Alvida Biersack
from Noun Project

Exam covers
both Azure and
Microsoft 365

What Basic Azure Security Capabilities Exist?

Network Security Group

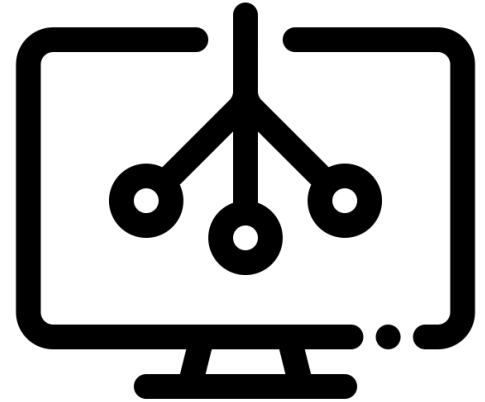
Azure DDoS Protection

Azure Firewall

Azure Bastion

Web Application Firewall (WAF)

Key Vault



Created by Timofei Rostilov
from Noun Project

What Azure Security Management Services Exist?

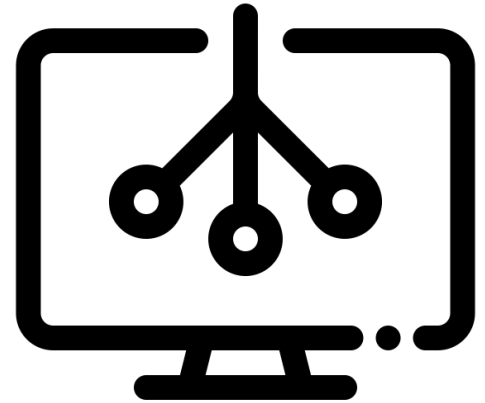
Microsoft Defender for Cloud
(was Azure Defender & Azure Security Center)

Cloud Security Posture Management (CSPM)

Secure score in Microsoft Defender for Cloud

Enhanced security in Microsoft Defender for Cloud

Microsoft Sentinel (was Azure Sentinel)



Created by Timofei Rostilov
from Noun Project

What Microsoft Defender XDR Capabilities Exist?

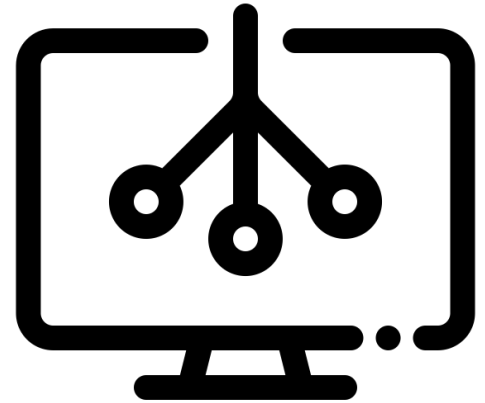
Microsoft 365 Defender XDR

Microsoft Defender for Identity
(formerly Azure ATP)

Microsoft Defender for Office 365
(formerly Office 365 ATP)

Microsoft Defender for Endpoint
(formerly Microsoft Defender ATP)

Microsoft Defender for Cloud Apps
(formerly Cloud App Security)



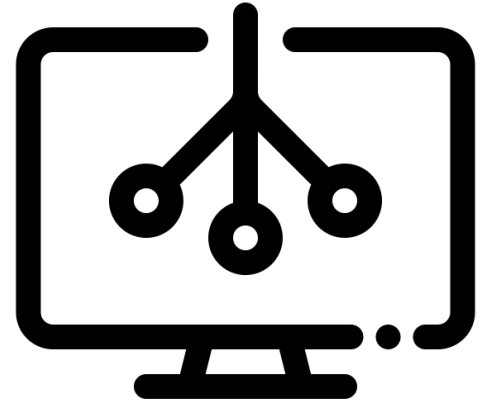
Created by Timofei Rostilov
from Noun Project

What Microsoft Defender XDR Capabilities Exist?

Microsoft Defender Vulnerability Management

Microsoft Defender Threat Intelligence (Defender TI)

Microsoft Defender portal



Created by Timofei Rostilov
from Noun Project

What M365 Compliance Capabilities Exist?

Microsoft Purview

Microsoft Priva

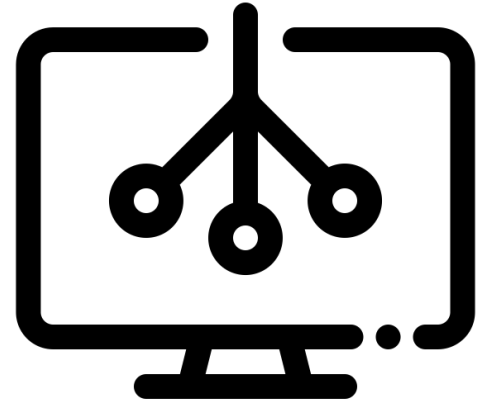
Retention Policies and Retention Labels

Records Management

Data Loss Prevention

eDiscovery

Advanced Auditing



Created by Timofei Rostilov
from Noun Project

What Basic Azure Identity Capabilities Exist?

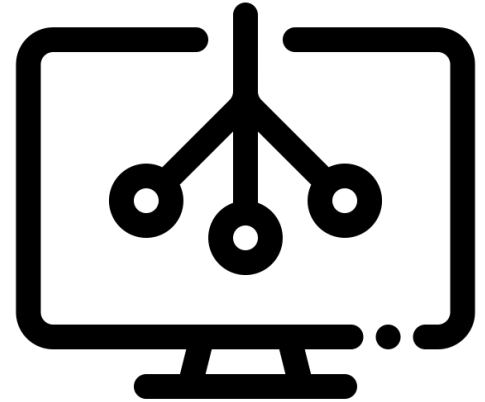
Active Directory

Entra ID (formerly Azure Active Directory)

Windows Hello for Business

Microsoft Entra ID Protection

Privileged Identity Management (PIM)



Created by Timofei Rostilov
from Noun Project



CERTIFICATION

Microsoft Certified: Security, Compliance, and Identity Fundamentals


Demonstrate foundational knowledge on security, compliance, and identity concepts and related cloud-based Microsoft solutions.




At a glance

 **Level**
Beginner

 **Role**
Security Engineer

 **Last Updated**
07/26/2024

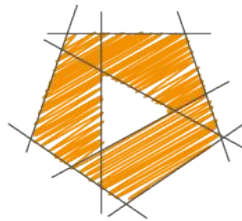
 **Product**
Azure

 **Subject**
Security

Jump to

[Prepare for the exam](#)
[Practice for the exam](#)
[Take the exam](#)

<https://t.me/learningnets>

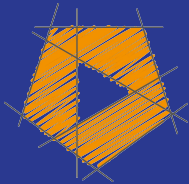


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>


Describe the Concepts of Security, Compliance, and Identity (10-15%)

Describe the concepts of security, compliance, and identity (10–15%)

Describe security and compliance concepts

- Describe the shared responsibility model
- Describe defense-in-depth
- Describe the Zero Trust model
- Describe encryption and hashing
- Describe Governance, Risk, and Compliance (GRC) concepts

Zero-Trust Model



Don't assume
everything behind
the firewall is safe



Zero Trust Principles

- Verify explicitly
- Use least privileged access
- Assume breach

Real-World Examples of Zero Trust:

Verify explicitly - my bank requires my secret code any time I try to transfer money, even after I have logged into the app

Real-World Examples of Zero Trust:

Least privileged access - every August, the boss (Sally) goes on vacation for the whole month, and Bob covers her role. Every time Bob needs to perform an administrative task, he needs to request permission from the system which only grants him short-term access. This is called “just in time (JIT) access”.

Real-World Examples of Zero Trust:

Assume breach - All sensitive data is encrypted at rest and in transit even between servers in the same data center. Even if a hacker was to find the data files, or could listen over the transmission wires inside your data center, they'd need the decryption keys to get the data.

Use every available
method to validate
identity and
authorization



Just-in-time (JIT)

Just-enough-access (JEA)

Security even inside
the network;
encryption,
segmentation,
threat detection




Identity: Verify and secure each identity



Devices: ensure
compliance and
health status

Applications:
appropriate in-app
permissions,
monitor user
actions

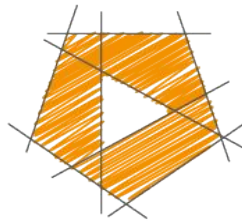
The top right corner of the slide features a decorative arrangement of overlapping geometric shapes, including triangles and squares, in various shades of pink and magenta.

Data: data-driven
protection, encrypt
and restrict access

Infrastructure:
robust monitoring
to detect attacks,
block and flag risky
behavior



Network: encrypt all communications

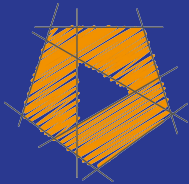


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe the concepts of security, compliance, and identity (10–15%)

Describe security and compliance concepts

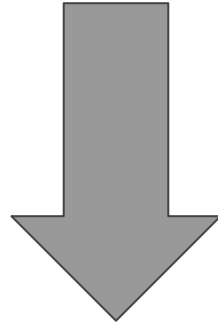
- Describe the shared responsibility model
- Describe defense-in-depth
- Describe the Zero Trust model
- Describe encryption and hashing
- Describe Governance, Risk, and Compliance (GRC) concepts

Encryption and hashing

Encryption (n):

the process of converting information or data into a code, especially to prevent unauthorized access.

“Hello.”



f7ff9e8b7bb2e09b70935a5d785e0cc5d9d0abf0

Symmetric Encryption

There is ONE KEY

Same key locks the message (encrypt) and unlocks the message (decrypts)

Example: **WhatsApp** uses symmetric encryption

There is a shared secret between two people - “master secret key”

And nobody in the middle (including Meta) can decrypt the message



Asymmetric Encryption

There are two keys - PUBLIC and PRIVATE

You can use either key to encrypt the message, and the other one decrypts

Public can be published to anyone, and private must stay private

Example: **HTTPS** is asymmetric encryption



<https://t.me/learningnets>

Hashing (Preventing Forgery)

Hashing uses cryptography but is not encryption

It is a way to turn plain text into a short unique code

The unique code cannot be turned back into plain text (one-way function)

But hashes can be used to ensure the data received has not been altered

Dear Student,

This is a message from the instructor, Scott Duffy.

This message is not encrypted, in that anyone can read it. But you can be 100% sure that it's from me because it's signed. I have used my private key to encrypt the hash, and you can use my public key to decrypt it. You can then check the SHA-1 signature attached to this message against an SHA-1 generator and verify that the contents have not been altered.

Generate

Clear All

MD5

SHA256

SHA512

Password Generator

Treat each line as a separate string Lowercase hash(es)

SHA1 Hash of your string: [[Copy to clipboard](#)]

63904A42D4114E0ED28F03FBA5767A0803017914

Enter your text below:

Dear Student,

This is a message from the instructor **John Doe.**

This message is not encrypted, in that anyone can read it. But you can be 100% sure that it's from me because it's signed. I have used my private key to encrypt the hash, and you can use my public key to decrypt it. You can then check the SHA-1 signature attached to this message against an SHA-1 generator and verify that the contents have not been altered.

Generate

Clear All

MD5

SHA256

SHA512

Password Generator

Treat each line as a separate string Lowercase hash(es)

SHA1 Hash of your string: [[Copy to clipboard](#)]

E642F6B6C9B0F72561C0EAFD8510E91FD88025B5

SHA1 Hash of your string: [[Copy to clipboard](#)]

63904A42D4114E0ED28F03FBA5767A0803017914

Scott Duffy.



SHA1 Hash of your string: [[Copy to clipboard](#)]

E642F6B6C9B0F72561C0EAFD8510E91FD88025B5

John Doe.

Hashing (Storing Passwords)

A lot of companies use “hashes” to store passwords in a database

So you'll see, when a company gets hacked, the hackers don't get passwords, they get hashes

Dropbox Sign hack: how it happened and what data was stolen

Unidentified attackers have managed to compromise the Dropbox Sign service account, and thus gain access to the platform's internal automatic configuration mechanism. Using this access, hackers were able to lay their hands on a database that contains information about Dropbox Sign users.

As a result, the following data of registered users of the Sign service was stolen:

- usernames;
- email addresses;
- phone numbers;
- passwords (hashed);
- authentication keys for the DropBox Sign API;
- OAuth authentication tokens;
- SMS and application two-factor authentication tokens.

How Passwords are Hashed

When you create a new account at a website

You enter your desired password (**not** “password123!”)

The company **should not** store your password as **plain-text** in their database!

They will hash the password (in some secure fashion) and store the hash

When you log into the website, they take the password you enter to log in and hash it, and compare that hash with what is stored

Salting involves
adding a random,
unique value to
each password
before hashing

Peppering involves
using a secret value
to hash the
password again
before storing

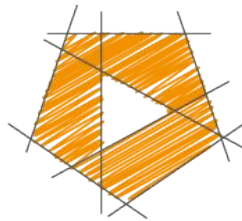
Work factors is a way of making the hash function more expensive in computing power

Examples of Symmetric Encryption Algorithms

- AES (Advanced Encryption Standard)
 - The most commonly used symmetric encryption algo
- DES (Data Encryption Standard)
 - Considered too weak for modern powerful computers
- IDEA (International Data Encryption Algorithm)
- Blowfish (Drop-in replacement for DES or IDEA)
- RC4 (Rivest Cipher 4)
- RC5 (Rivest Cipher 5)
- RC6 (Rivest Cipher 6)

Examples of Asymmetric Encryption Algorithms

- RSA
 - Encryption used by HTTPS/SSL (asymmetric in the most common usage)
- Diffie-Hellman
- ECC
 - Encryption used by Bitcoin
- ElGamal
 - Used in recent versions of PGP
- DSA
 - US Government FIPS standard for signing messages

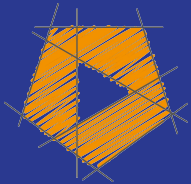


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe the concepts of security, compliance, and identity (10–15%)

Describe security and compliance concepts

- Describe the shared responsibility model
- Describe defense-in-depth
- Describe the Zero Trust model
- Describe encryption and hashing
- Describe Governance, Risk, and Compliance (GRC) concepts

Governance, Risk, and Compliance (GRC)


Governance - a set
of policies, rules or
frameworks
designed to achieve
business goals

Risk management -
identify the
different risks that a
business faces and
mitigate them

Compliance -
following rules,
laws and
regulations

Examples of compliance regulations:

- CCPA (California Consumer Privacy Act; USA)
- GDPR (General Data Protection Regulation; Europe)
- HIPAA (Health Insurance Portability and Accountability Act; USA)
- PCI DSS (Payment Card Industry Data Security Standard; international)
- SOX (Sarbanes–Oxley Act; US)



GRC is about
making better
decisions while
being aware of all
of the risks

GRC programs

- Data-driven decision making
- Responsible operations
- Improved cybersecurity

Microsoft 365 Maturity Model



Governance Risk and Compliance maturity levels



Level 100 and 200 technical controls

Any Business Plans

Any Enterprise Plans

Any Education plans

Level 300 technical controls

Business Premium

Enterprise E3

Education A3 plans

Level 400 technical controls

Enterprise E5 or E5
Compliance Plans

Education A5 or or A5
Compliance plans

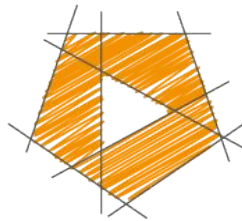
Level 500 technical controls

Enterprise E5 Plans

Education A5 plans

plus compliance add
on packages, e.g.

- HIPAA
- Subject Access Requests
- Audit logs

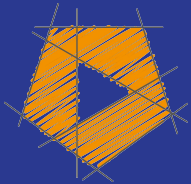


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Define identity concepts

- Define identity as the primary security perimeter
- Define authentication
- Define authorization
- Describe identity providers
- Describe the concept of directory services and Active Directory
- Describe the concept of federation

Identity as the Primary Security Perimeter

Security Perimeters

The person is who they say they are

Company owned network

Company owned device

Services are provided only inside company data center


Security Perimeters

The person is who they say they are - Verified identity

~~Company owned network~~ - Work from home

~~Company owned device~~ - Using your own computers/mobile

~~Services are provided only inside company data center~~ - Cloud computing



Identity is now the
primary security
perimeter

Identity is not just a “person”

Employees


Partners and customers

Cloud apps

On-prem apps

Devices

Zero trust model

The top right corner of the slide features a decorative arrangement of overlapping geometric shapes, including triangles and squares, in various shades of pink and magenta.

Advances in
security focus on
ensuring identity is
trustable

Ways to verify identity

Beyond the simple user id/password

Single sign-on (using AD everywhere)

Multi-factor authentication

Just-in-time access requests

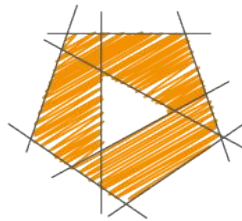
More granular security + logging

Intelligent monitoring that detects strange behavior

More granular security on data and documents

Restrict unrequired and unwanted lateral movement of traffic

Least privilege / default deny

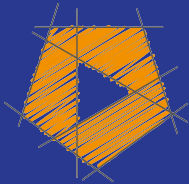


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Define identity concepts

- Define identity as the primary security perimeter
- Define authentication
- Define authorization
- Describe identity providers
- Describe the concept of directory services and Active Directory
- Describe the concept of federation

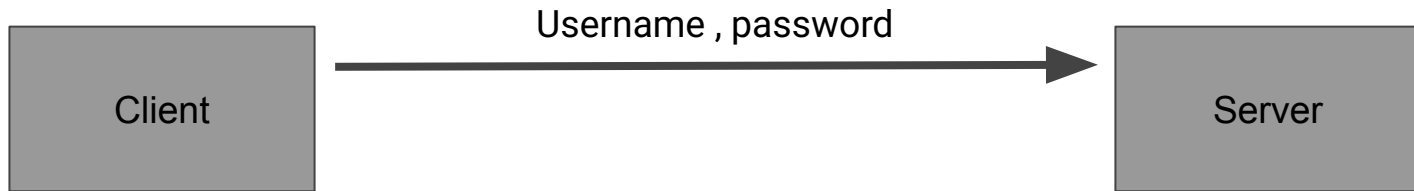
Define Authentication (AuthN)

How much proof do
you need for me to
prove my identity to
you?

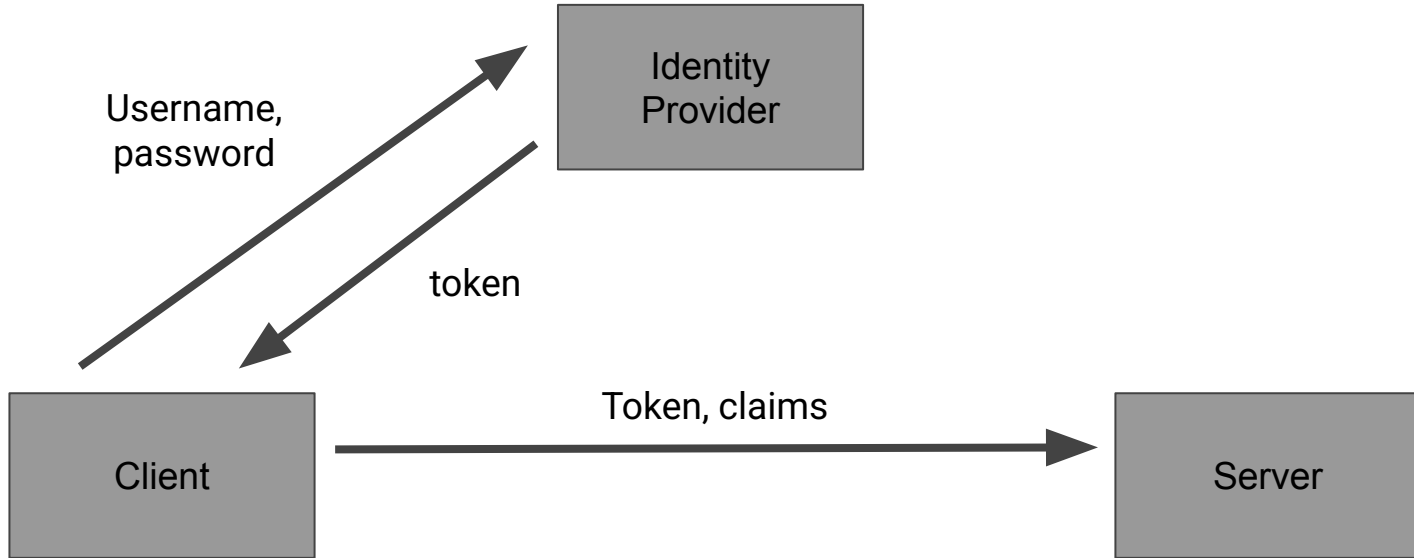
“Modern Authentication”

Server should use
an identity provider
to validate identity

The Old Way



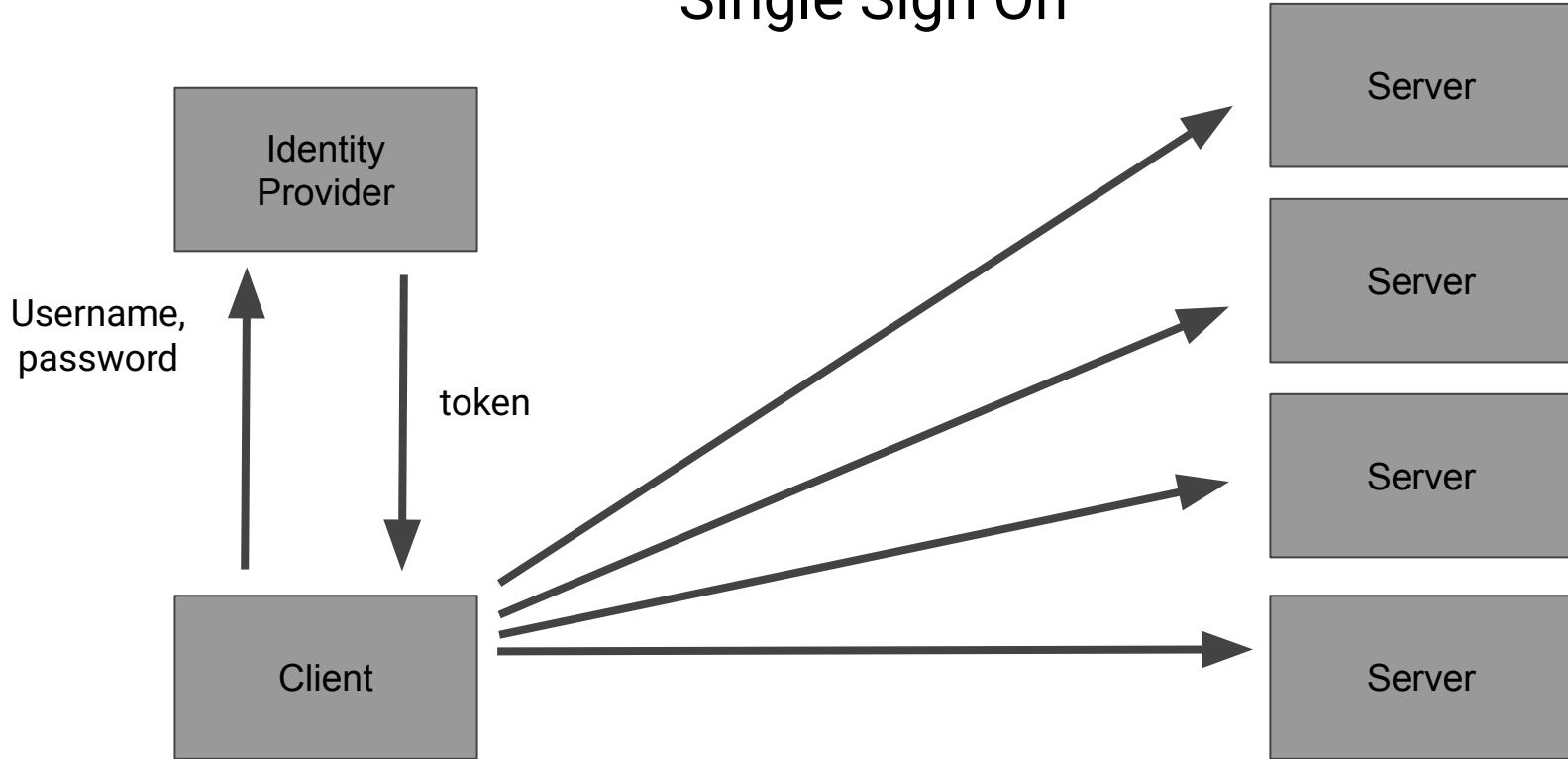
The New Way



A ***token*** is a digital credential, signed by the server, that verifies your identity

Claims are details
about the
authenticated user
such as username
or roles

Single Sign On



Define Authorization (AuthZ)

The level of access
an authenticated
person has

“Permissions”

Principle of least privilege

A user
is granted a set of
permissions to
perform some
tasks

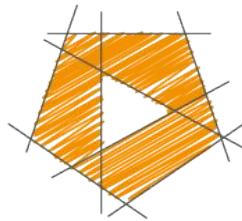
A ~~user~~ role
is granted a set of
permissions to
perform some
tasks

The top right corner of the slide features a decorative arrangement of overlapping triangles in various shades of pink and magenta, creating a modern, abstract geometric pattern.

What role do you have?



Users can have multiple roles

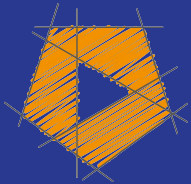


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



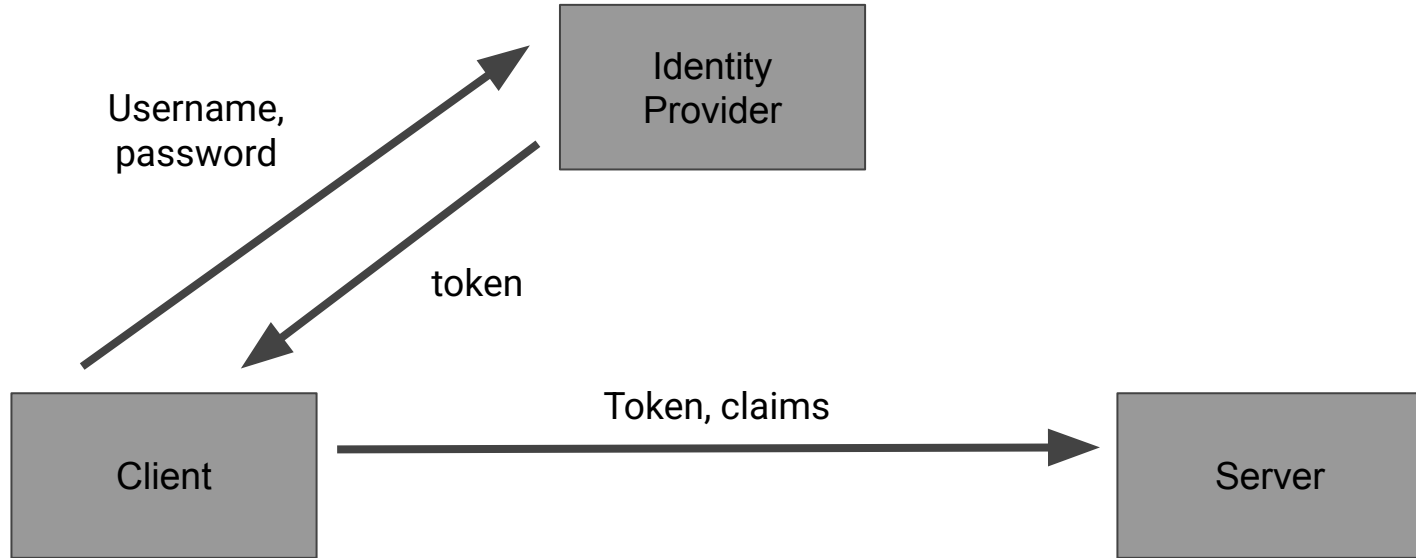
© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Define identity concepts


- Define identity as the primary security perimeter
- Define authentication
- Define authorization
- Describe identity providers
- Describe the concept of directory services and Active Directory
- Describe the concept of federation

Identity Providers

The New Way



Creates, maintains
and manages
identity
information...



Plus offers
authentication,
authorization and
auditing services

Microsoft Entra ID

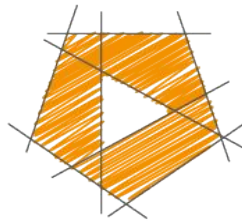
<https://t.me/learningnets>

Formerly Azure Active Directory (Azure AD)

Active Directory

<https://t.me/learningnets>

Google
Facebook
Twitter
LinkedIn
GitHub

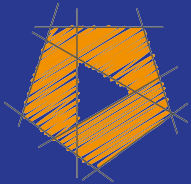


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Define identity concepts

- Define identity as the primary security perimeter
- Define authentication
- Define authorization
- Describe identity providers
- Describe the concept of directory services and Active Directory
- Describe the concept of federation

Active Directory

What is a “directory”?

“A **directory** is a **hierarchical structure** that stores information about users, groups, devices, applications, and other resources within an organization”

What is a “directory service”?

“A **directory service** stores **directory data** and makes this information accessible to network users, administrators, services, and applications”

What is “Active Directory”?

“**Active Directory (AD)** is a set of directory services developed by Microsoft, initially released as part of Windows 2000. It's primarily used for managing identities within **on-premises domain-based networks**”

What is “Active Directory Domain Services”?

“**Active Directory Domain Services (AD DS)** is the most well-known service within Active Directory. It acts as a **central repository** of information about domain members, including users and devices”

Key Functions of AD DS

Storing information: users, devices, groups, and other objects within the domain

Credential verification: verifies user credentials during login attempts

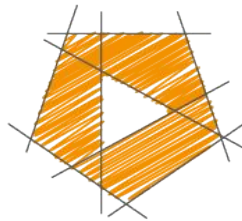
Access control: AD DS defines and enforces access rights, determining what resources users are permitted to access based on their roles and permissions

What is a “Domain Controller”?

This is a server running “Active Directory Domain Services”.

Limitations of AD DS

- Limited Support of Modern Authentication Methods
 - Old methods: Kerberos, NTLM, LDAP
 - New methods: OAuth 2.0, OpenID Connect, MFA, SSO across Federation
- On-Premises Focus

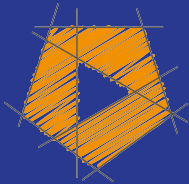


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Define identity concepts

- Define identity as the primary security perimeter
- Define authentication
- Define authorization
- Describe identity providers
- Describe the concept of directory services and Active Directory
- Describe the concept of federation

Federation

The use of multiple identity providers

The identity
providers have a
trust relationship
between each other

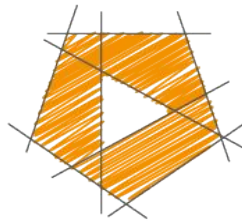
Company A AD
trusts
Company B AD

User from
Company B
can log in to
Company A app



Trust isn't always
bi-directional

Azure AD B2C
can be configured
to use social media
sites for identity

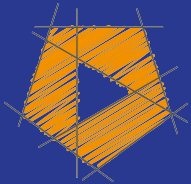


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe the capabilities of Microsoft Entra (25–30%)

Describe function and identity types of Microsoft Entra ID

- Describe Microsoft Entra ID
- Describe types of identities
- Describe hybrid identity

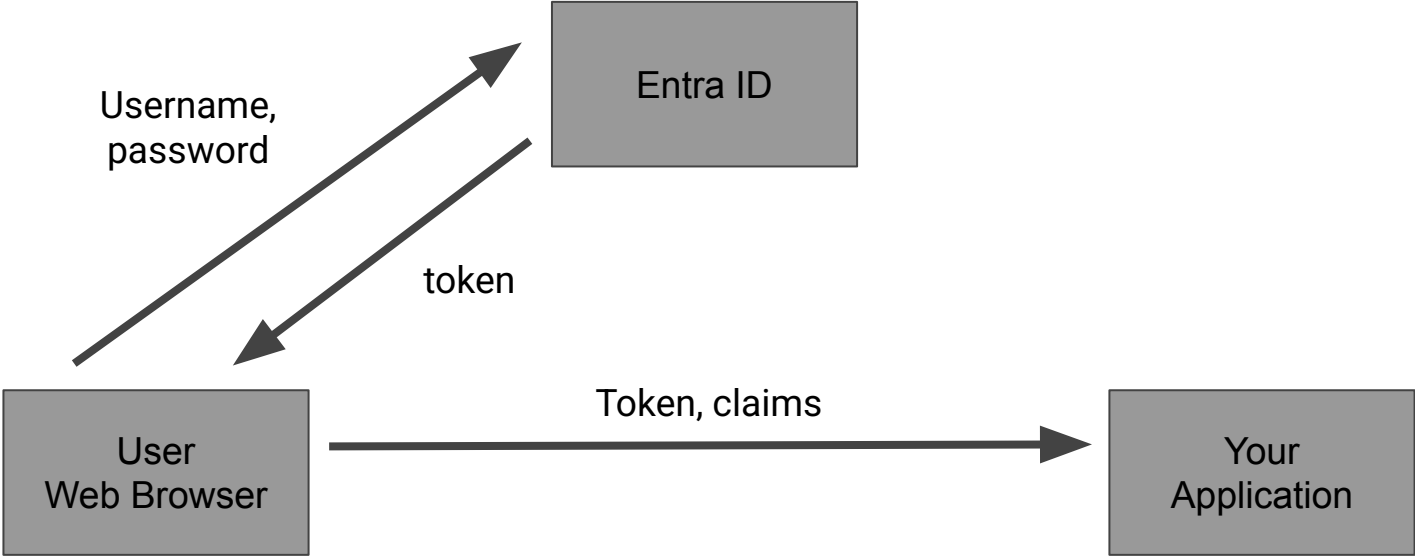
Microsoft Entra ID

Identity as a Service in Azure

What is a “directory”?

“A **directory** is a **hierarchical structure** that stores information about users, groups, devices, applications, and other resources within an organization”

Entra ID



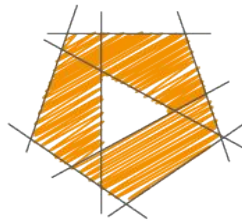
A Tenant =
An Organization

A tenant can have a subscription to enable compute resources to be created

Applications can register with Entra ID

Demo of Entra ID

<https://t.me/learningnets>

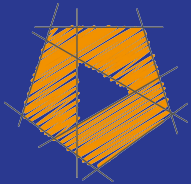


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Types of Identities

Man or Machine?

When it comes to the user...

They can be a **human** (employee, customer, partner, contractor...)

Or **computer program** (virtual machine, application, device, service...)

Inside or Outside?

They can be...

Managed by Entra ID (internal users)

Managed outside (external users / Federation)

Cloud Identities (Internal Users)

Identities that exist solely in the cloud

Typically only used for cloud-based resources and applications

Managed entirely in Entra ID

Users who access cloud-based application like Microsoft 365, Azure services, and other SaaS offerings

Suitable for cloud-native organizations

Cloud Identities (Internal System/Apps)

Sometimes called “**service principals**” or “**managed identities**”

Applications or services that need access to resources

Not associated with human users

Managed entirely in Entra ID

Assigned permissions based on their intended functions

On-Premises Identities

Identity originates from an on-premises directory such as Active Directory

For users who access the company internal network

Managed in AD

May be synchronized with Entra ID for hybrid scenarios

Suitable for organizations with significant on-prem infrastructure

External Identities (Internal Guest Users)

Users are from outside the company's primary directory

Granted access as partners, customers, contractors or guests

Suitable for collaboration scenarios

Managed entirely in Entra ID

Could be temporary access, or access to shared resources

External Identities (B2B)

Users are from outside the company's primary directory

Granted access as partners, customers, contractors or guests

Suitable for collaboration scenarios

Uses Federation - identity managed by an outside directory

Could be temporary access, or access to shared resources

Hybrid Identities

A bridge between on-premises and cloud identities

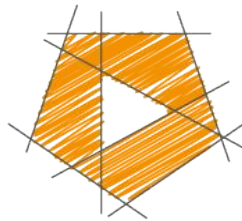
Users can access resources on-premises and in the cloud with a single set of credentials

Suitable for organizations transitions between two environments

Cloud Synchronized

Single Sign-on

Centralized identity management

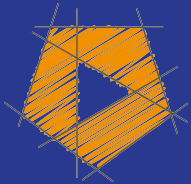


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe the capabilities of Microsoft Entra (25–30%)

Describe function and identity types of Microsoft Entra ID

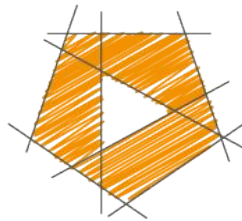
- Describe Microsoft Entra ID
- Describe types of identities
- Describe hybrid identity

Function of Entra ID

Entra ID can work with the on-premises Active Directory

To provide Single Sign On experience using:

- Your work computer
- Any custom apps your company creates that need authentication
- Third-party apps like Dropbox and Adobe (Enterprise Apps)

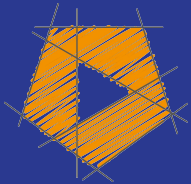


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe authentication capabilities of Microsoft Entra ID

- Describe the authentication methods
- Describe multi-factor authentication (MFA)
- Describe password protection and management capabilities

Azure AD Password Protection

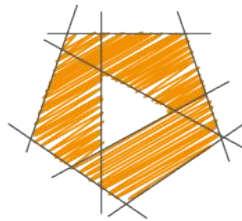
Global Banned Password List

<https://t.me/learningnets>

Custom Banned Password List

Bad password attempts and lockout duration

Can also protect
Windows Server
Active Directory

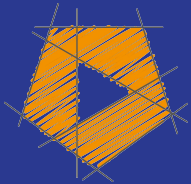


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe authentication capabilities of Microsoft Entra ID

- Describe the authentication methods
- Describe multi-factor authentication (MFA)
- Describe password protection and management capabilities

Something you are
Something you have
Something you know

Authenticator app
OATH Hardware token
SMS
Voice call

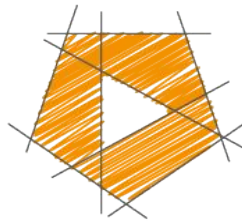
MFA: Enabled by administrators

MFA: Signed up by users

Conditional access

Session lifetime

<https://t.me/learningnets>

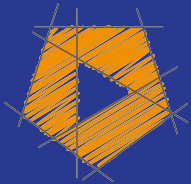


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

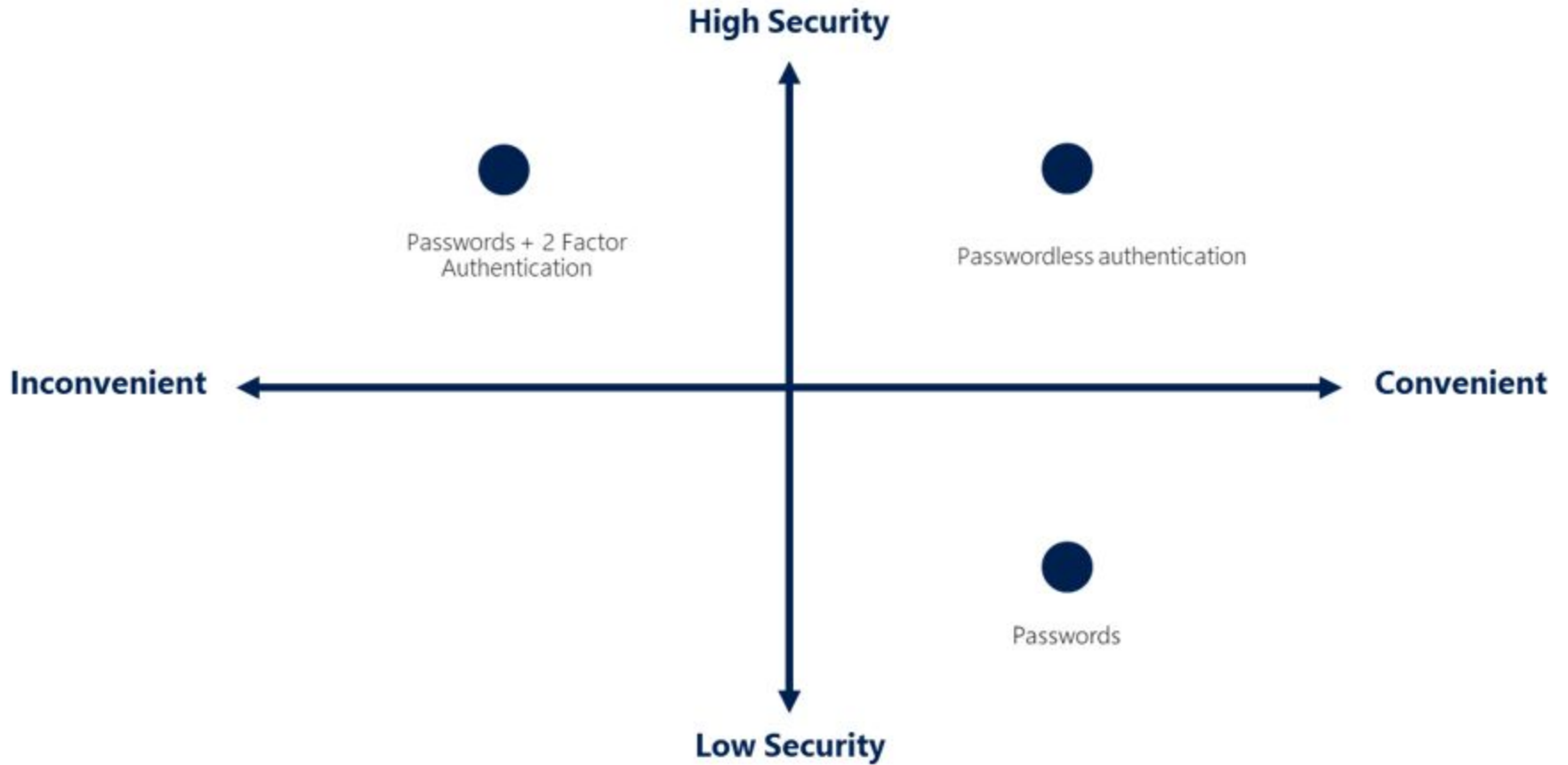
Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe authentication capabilities of Microsoft Entra ID

- Describe the authentication methods
- Describe multi-factor authentication (MFA)
- Describe password protection and management capabilities



Passwordless

<https://t.me/learningnets>

Gestures to sign in

Sign in using a PIN
or biometric
recognition (facial,
iris, or fingerprint)
with Windows
devices.



Hello Erwin McDaniel

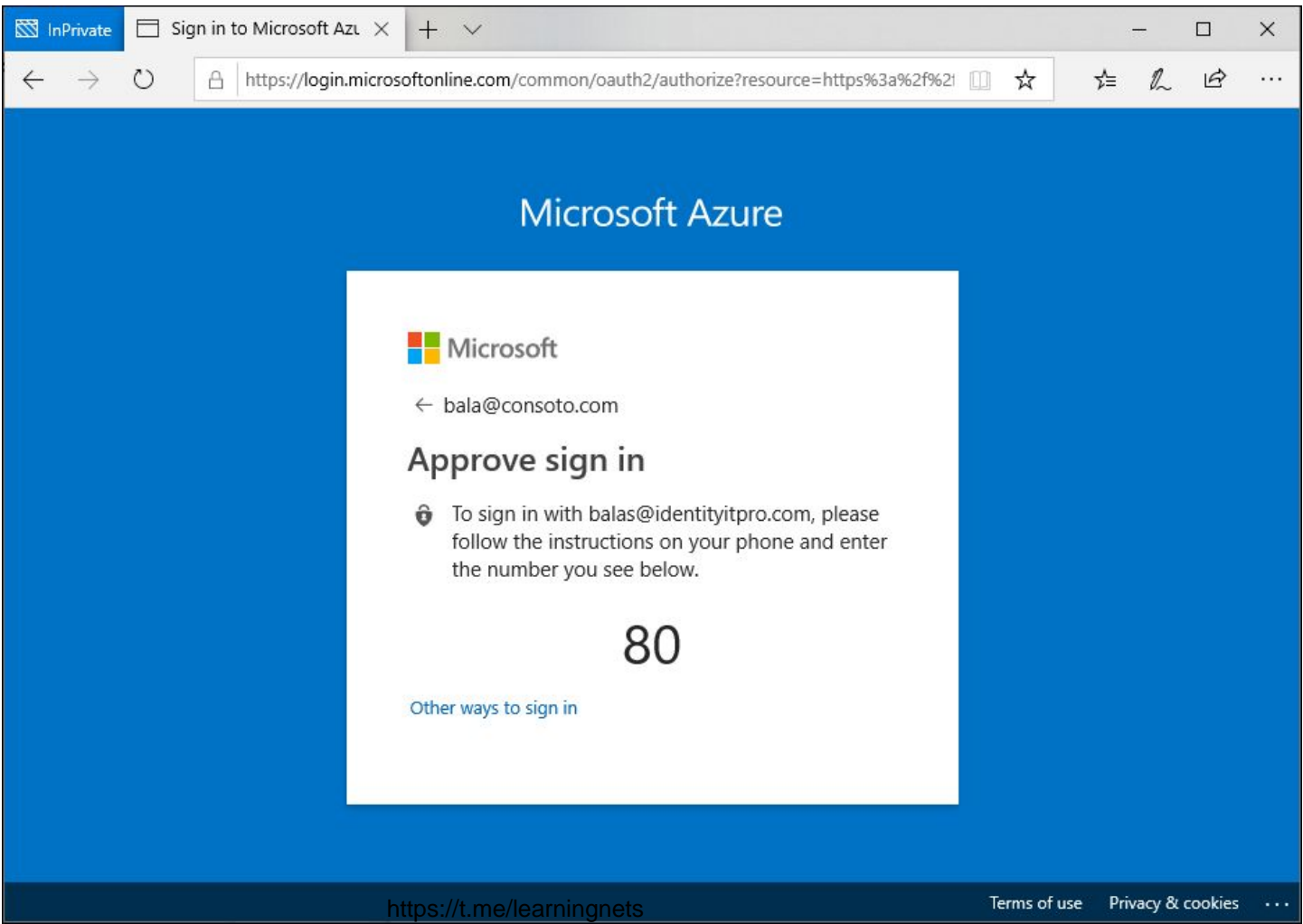
2:30^o

Tuesday, July 7

Project sync with Marc
Fourth Coffee
3:30 PM—4:30 PM



Your phone:
“Are you attempting
to sign in to this
app?”




Microsoft Azure



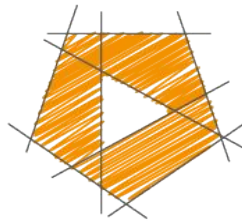
← bala@consoto.com

Approve sign in

 To sign in with balas@identityitpro.com, please follow the instructions on your phone and enter the number you see below.

80

[Other ways to sign in](#)

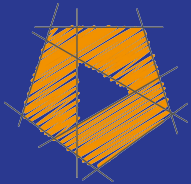


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe access management capabilities of Microsoft Entra ID

- Describe Conditional Access
- Describe Microsoft Entra roles and role-based access control (RBAC)

Conditional Access

The top right corner of the slide features a decorative arrangement of overlapping geometric shapes. These include a light pink triangle pointing downwards, a dark pink triangle pointing upwards, and a solid dark pink square. The background of the entire slide is a solid, vibrant pink color.


Using signals to make decisions and enforce policies

User and location Device Application Risk

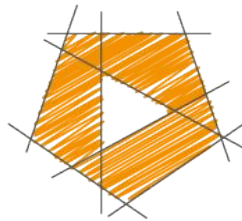
Allow access
Require MFA
Deny access

Require MFA for all Admin users

Require MFA signup
from trusted
locations

The top right corner of the slide features a decorative arrangement of overlapping triangles in various shades of pink and magenta, creating a modern, abstract design.

Some minimum
standard for device,
location, or risk

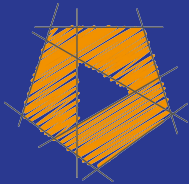


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe identity protection and governance capabilities of Microsoft Entra

- Describe Microsoft Entra ID Governance
- Describe access reviews
- Describe the capabilities of Microsoft Entra Privileged Identity Management
- Describe Microsoft Entra ID Protection
- Describe Microsoft Entra Permissions Management

Identity Governance



Balance the need
for security...

... and employee
productivity

Identity Lifecycle

From the time you start your first day with the company, to the time you retire

Integration with the HR system

Your role is managed by HR

And access is granted or revoked based on that HR system

Access Lifecycle

How to request access to things you need to get access to?

Understanding the data handling policies for different regions of the world

Dynamic groups

Azure AD Access Reviews

Azure AD Entitlement Management

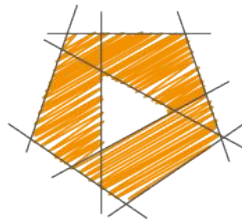
Conditional Access can enforce terms of use acceptance

Privileged Access Lifecycle

Azure AD Privileged Identity Management (PIM)

Just-in-time access

Access reviews

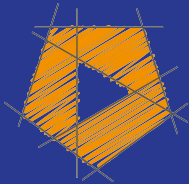


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe the capabilities of Microsoft Security solutions (25—30%)

Describe basic security capabilities in Azure

- Describe Azure DDoS protection
- Describe Azure Firewall
- Describe Web Application Firewall
- Describe Network Segmentation with VNet
- Describe Azure Network Security groups
- Describe Azure Bastion and JIT Access
- Describe ways Azure encrypts data

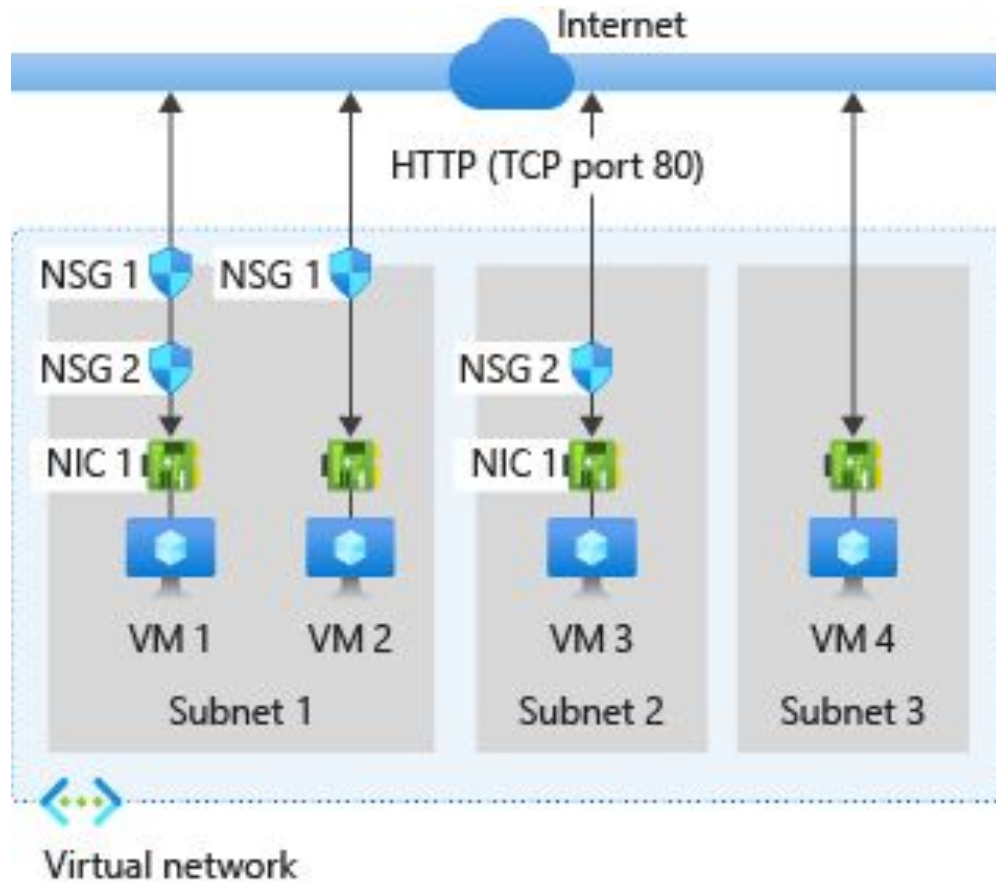
Network Security Group

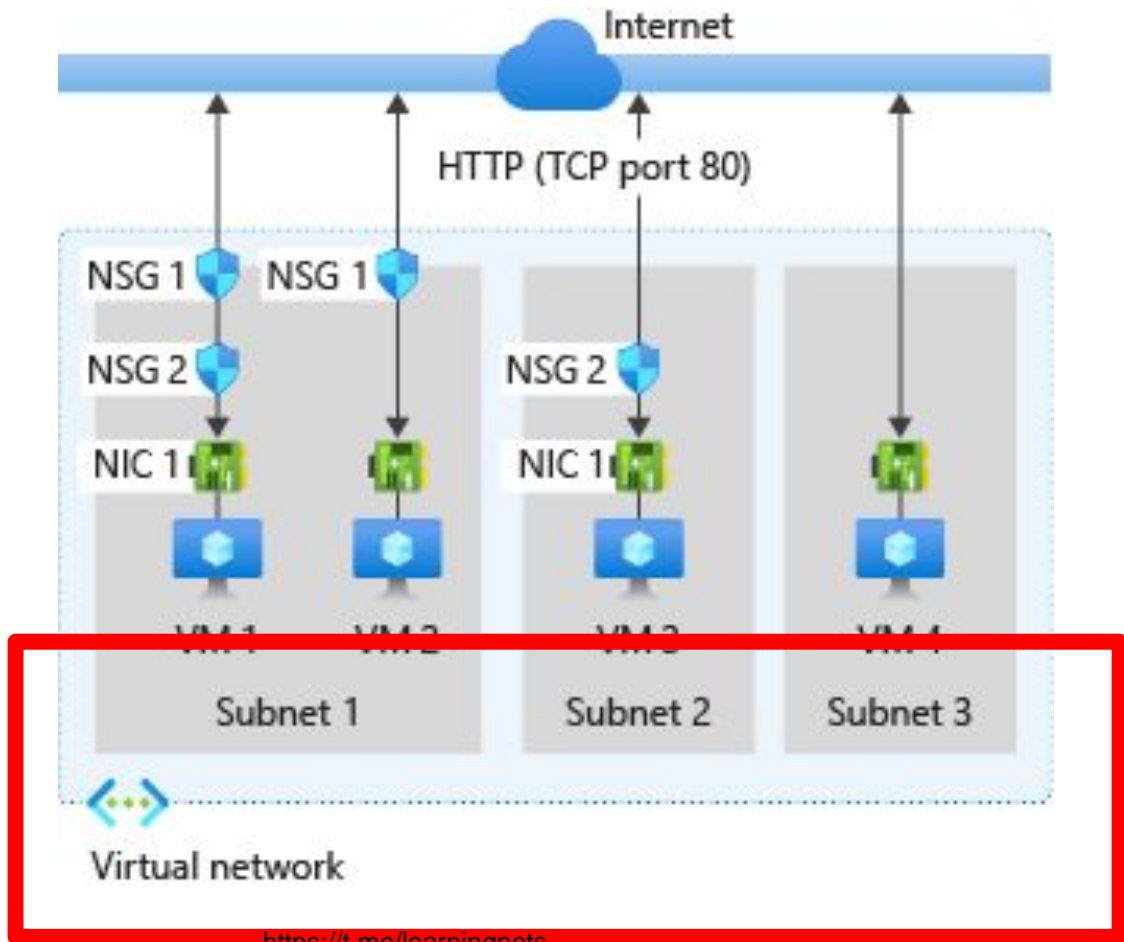
Simple, rules-based control that allows or denies traffic travelling over a network boundary

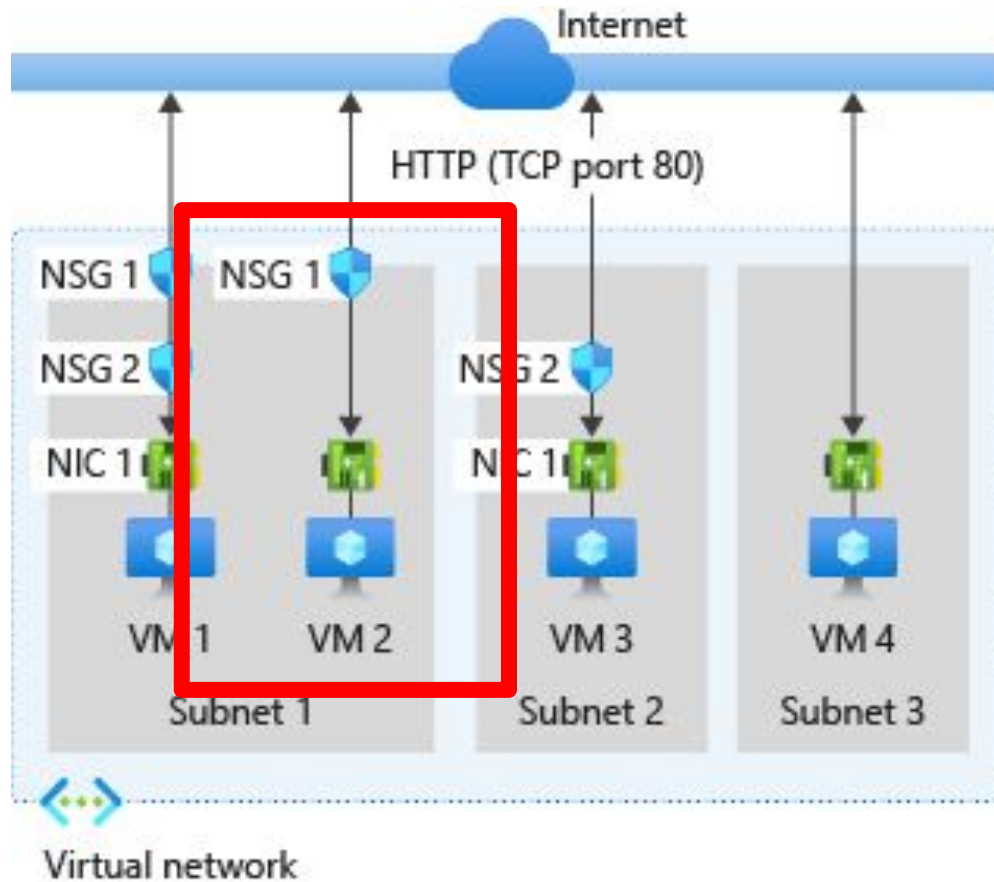
Inbound and outbound can have separate rules

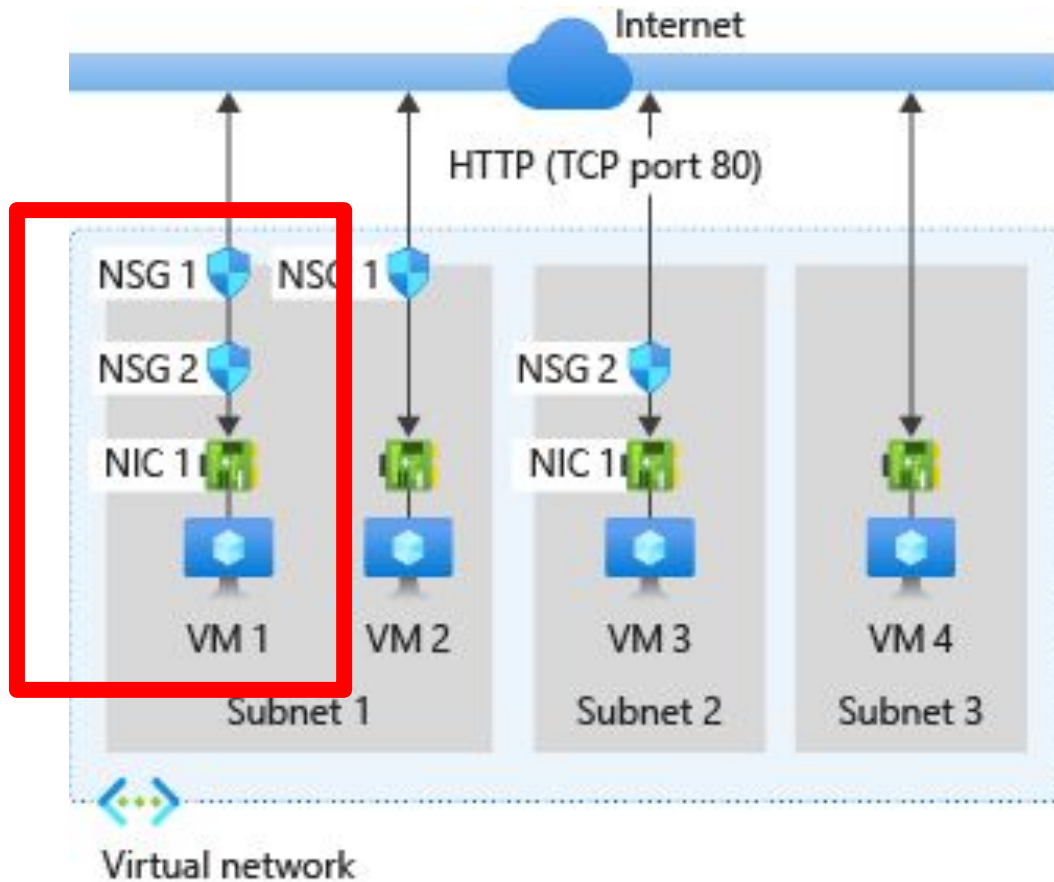
Two network boundaries - the subnet and a network interface card (NIC)

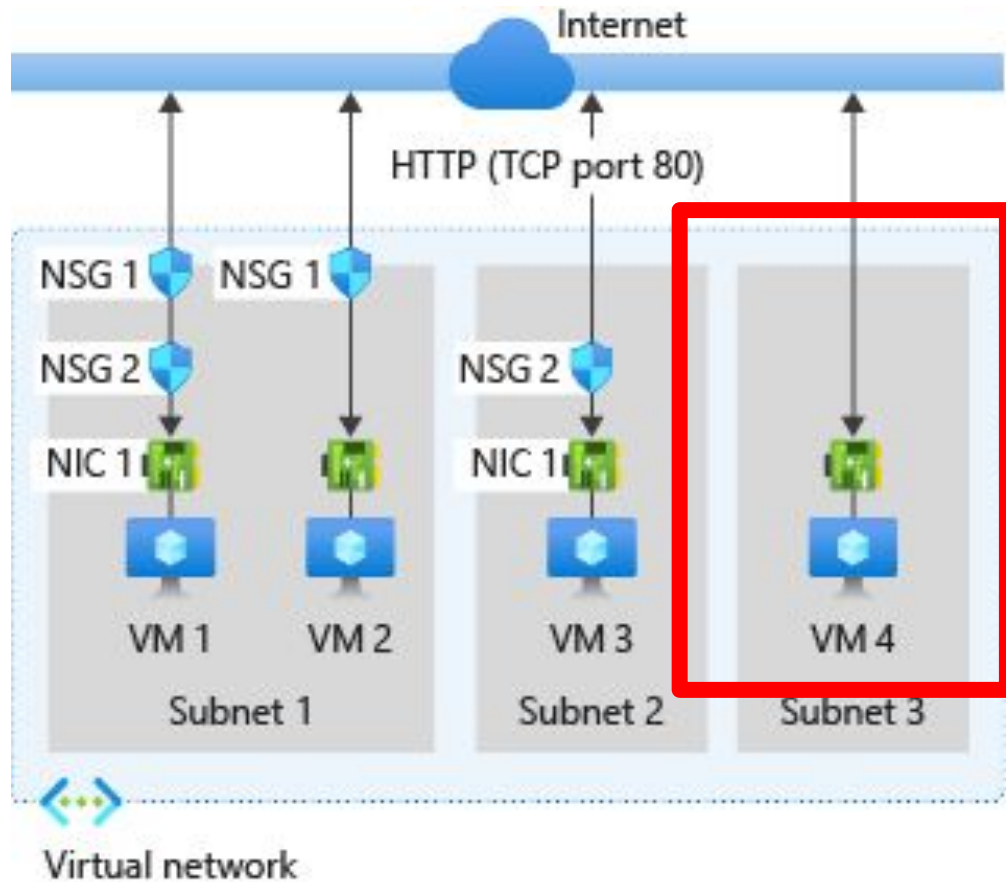
Deny by default

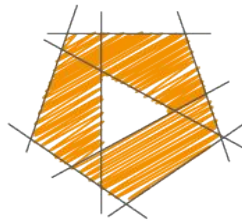










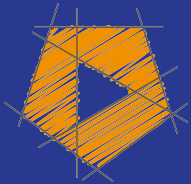


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



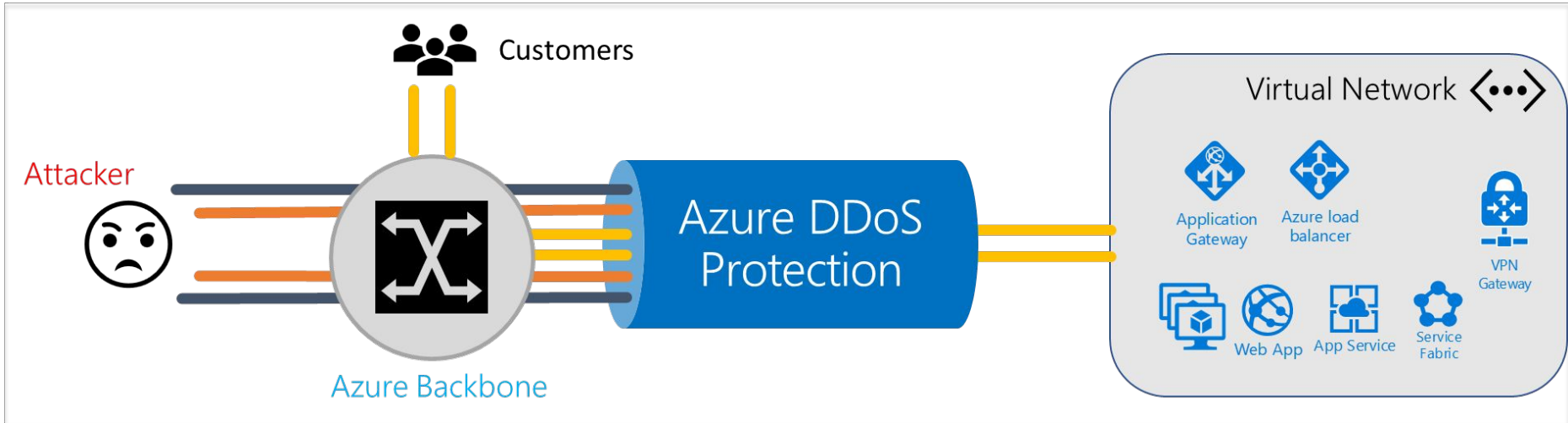
© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe the capabilities of Microsoft Security solutions (25—30%)

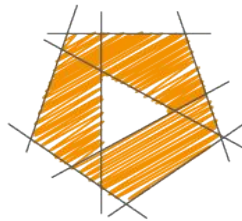
Describe basic security capabilities in Azure

- Describe Azure DDoS protection
- Describe Azure Firewall
- Describe Web Application Firewall
- Describe Network Segmentation with VNet
- Describe Azure Network Security groups
- Describe Azure Bastion and JIT Access
- Describe ways Azure encrypts data

Azure DDoS Protection



Feature	DDoS Protection Basic	DDoS Protection Standard
Active traffic monitoring & always on detection	●	●
Automatic attack mitigations	●	●
Availability guarantee	●	●
Cost Protection	●	●
Mitigation policies tuned to customers application	●	●
Metrics & alerts	●	●
Mitigation reports	●	●
Mitigation flow logs	●	●
DDoS rapid response support	●	●

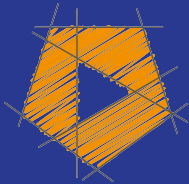


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor

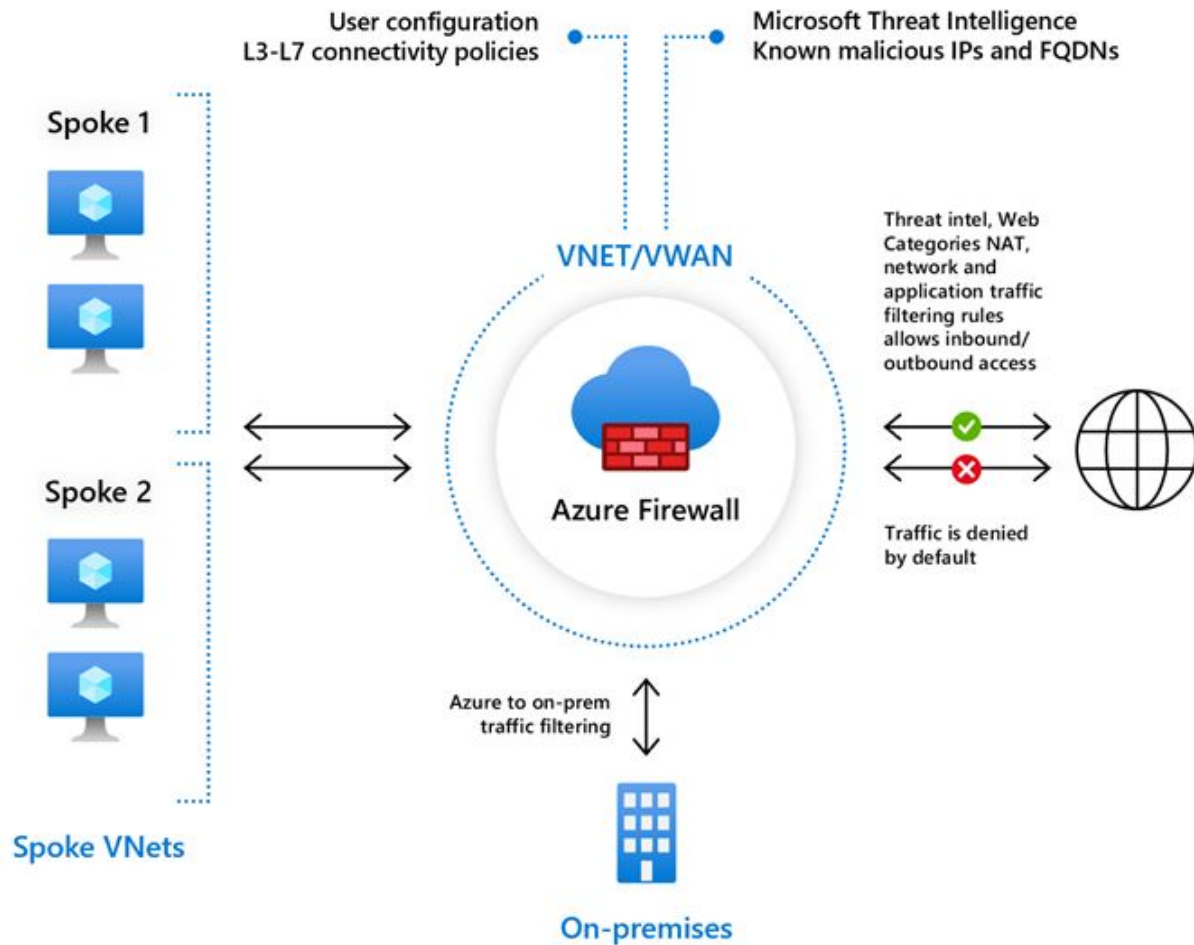


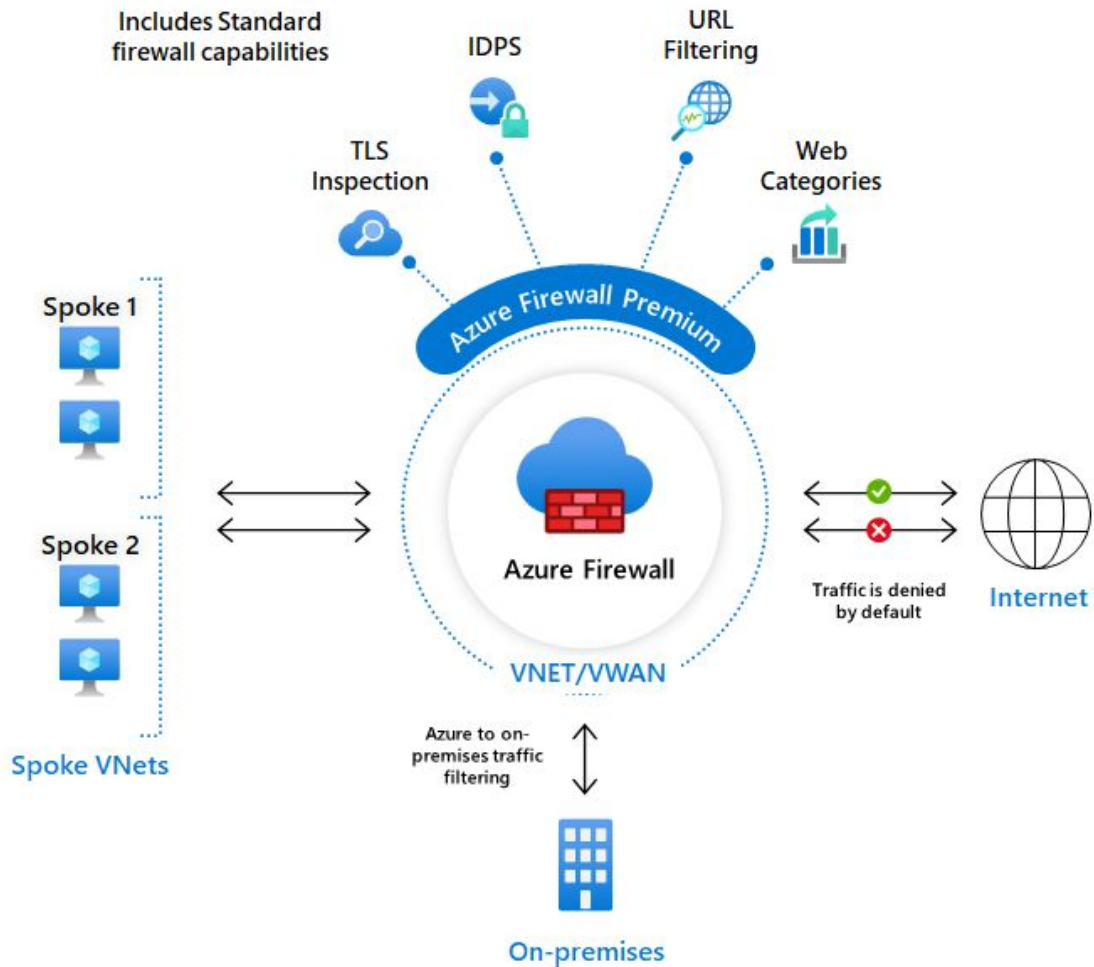
© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

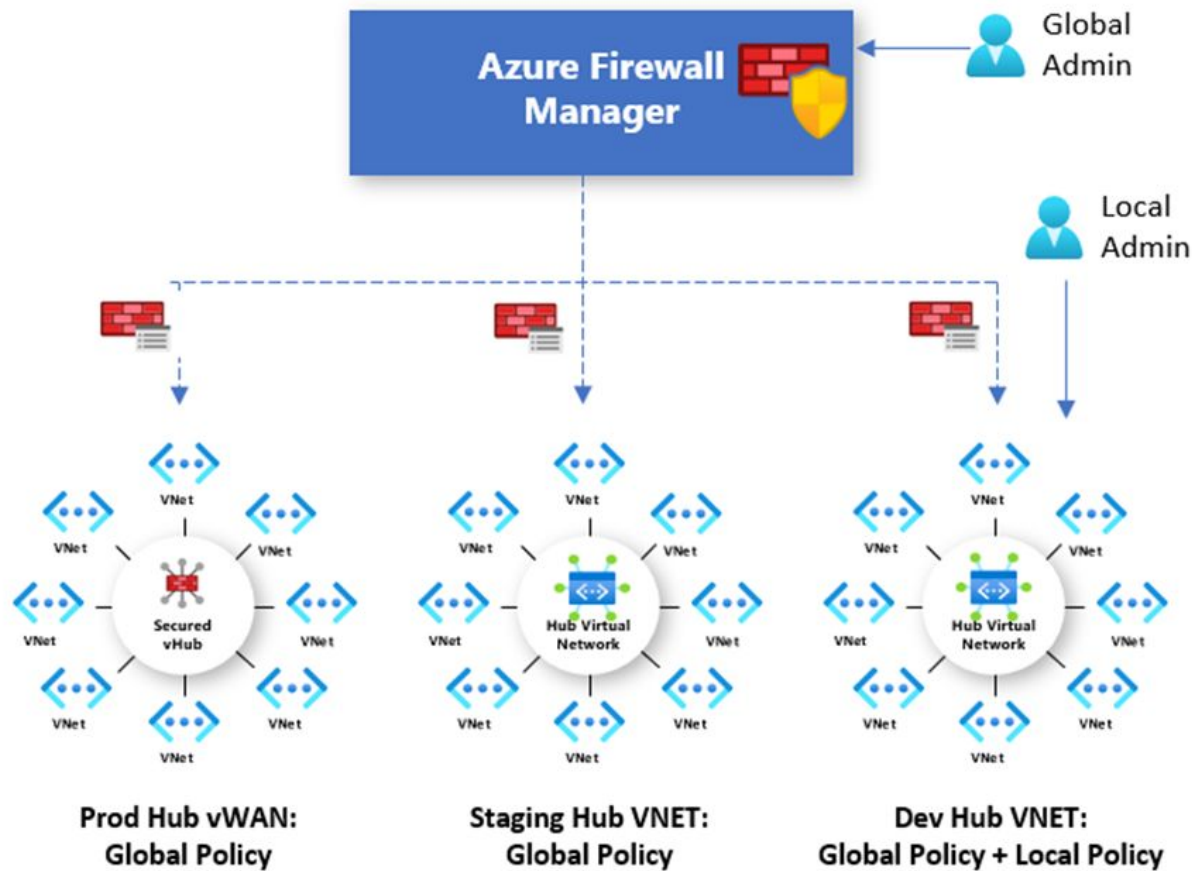
Describe the capabilities of Microsoft Security solutions (25—30%)

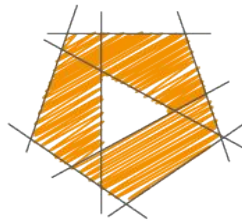
Describe basic security capabilities in Azure

- Describe Azure DDoS protection
- Describe Azure Firewall
- Describe Web Application Firewall
- Describe Network Segmentation with VNet
- Describe Azure Network Security groups
- Describe Azure Bastion and JIT Access
- Describe ways Azure encrypts data







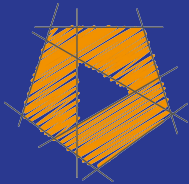


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor

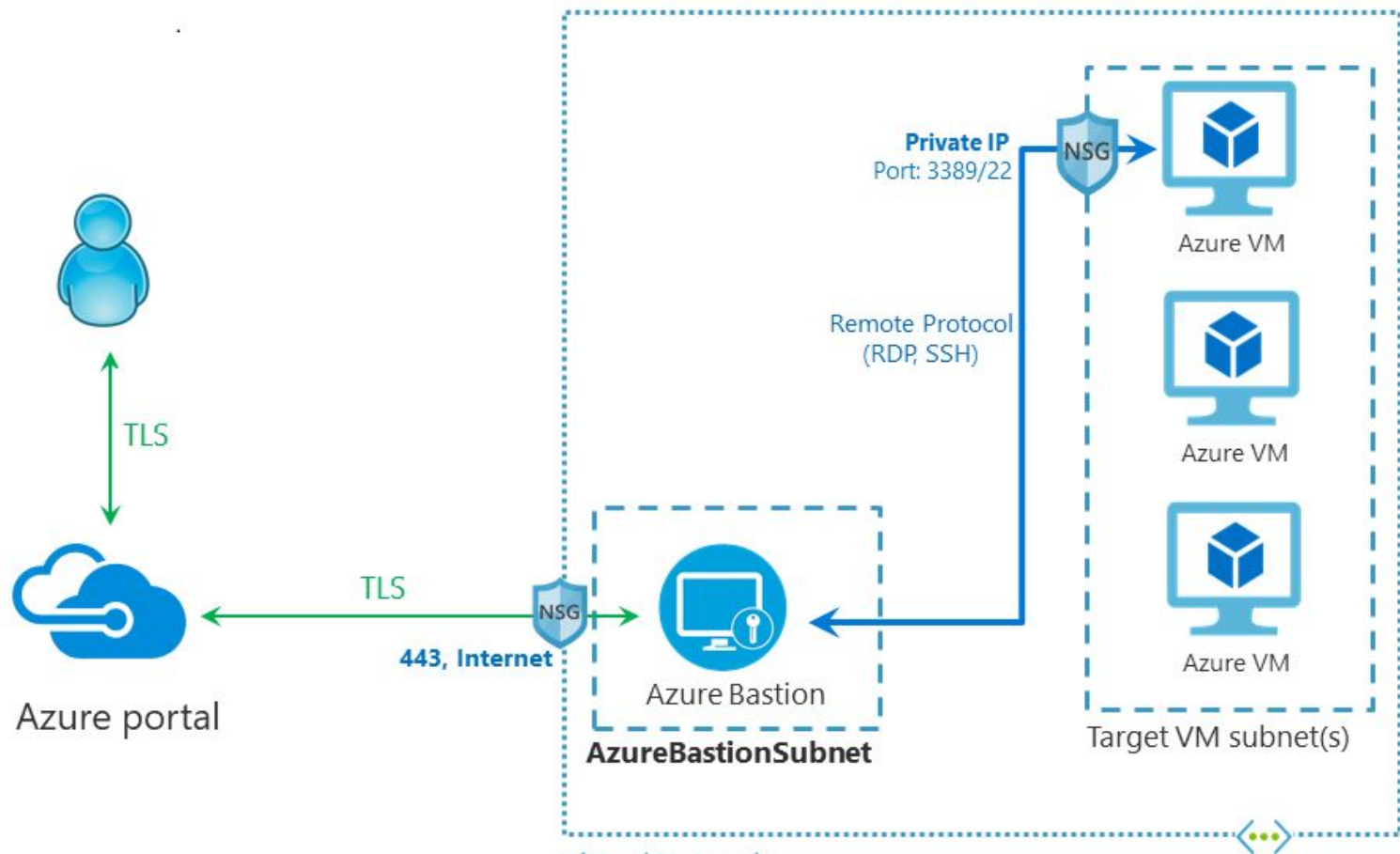







© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe the capabilities of Microsoft Security solutions (25—30%)






Describe basic security capabilities in Azure


- Describe Azure DDoS protection
- Describe Azure Firewall
- Describe Web Application Firewall
- Describe Network Segmentation with VNet
- Describe Azure Network Security groups
- Describe Azure Bastion and JIT Access
- Describe ways Azure encrypts data



-  Overview
-  Activity log
-  Access control (IAM)
-  Tags
-  Diagnose and solve problems

Settings

-  Networking
-  **Connect**
-  Windows Admin Center (preview)
-  Disks
-  Size

 This VM has a just-in-time access policy. Select "Request access" before co

RDP SSH Bastion

Connect with RDP

You need to request access to connect to your virtual machine. Select an IP number, and select "Request access". [Learn more](#)

IP address *

Port number *

Source IP 

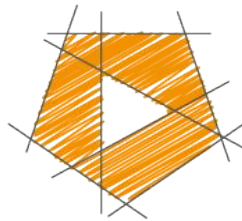
My IP

Other IP/IPs

All configured IPs

Request access

[Download RDP file anyway](#)

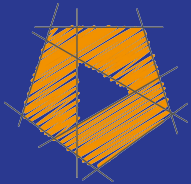


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor

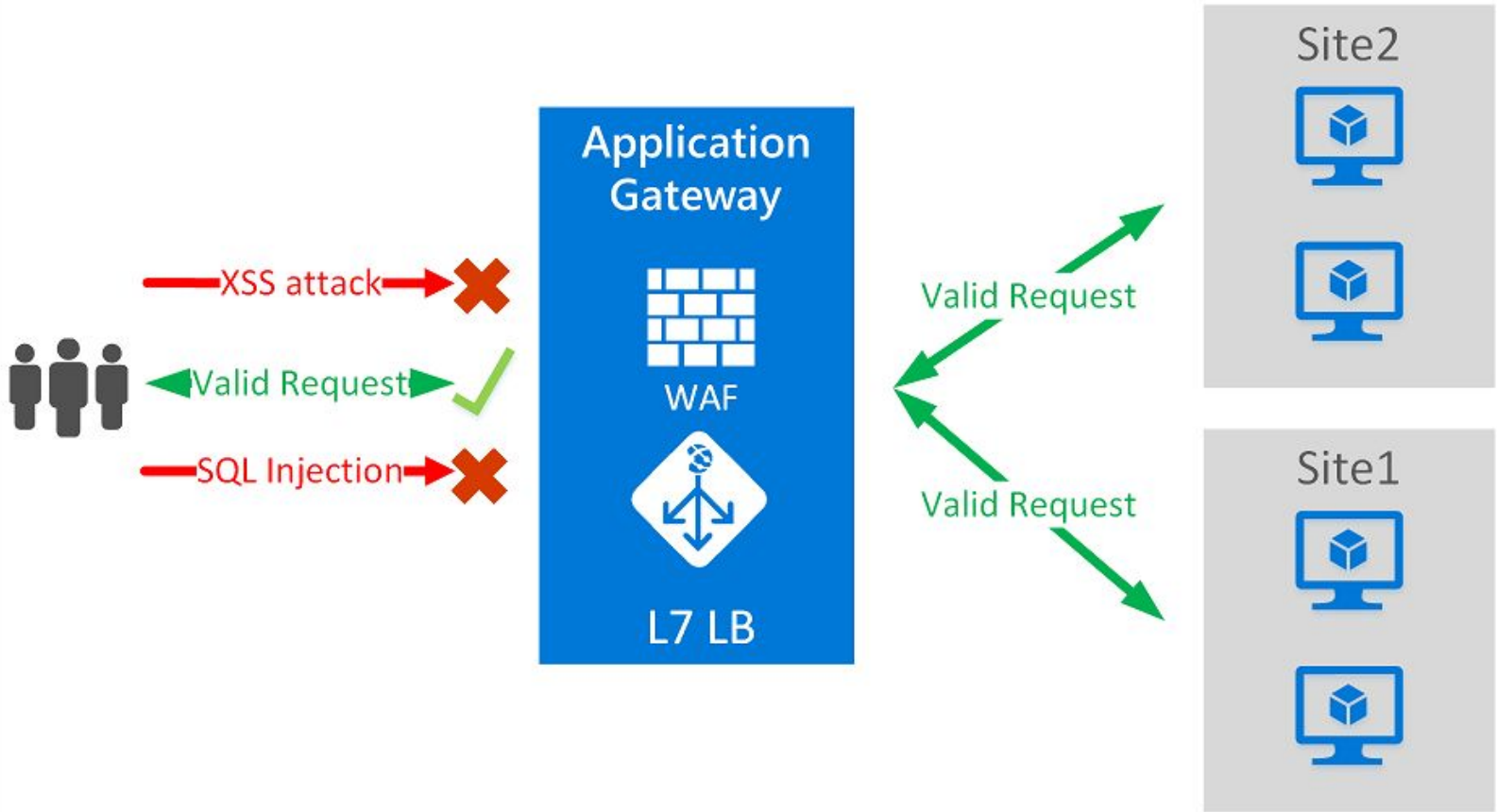


© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe the capabilities of Microsoft Security solutions (25—30%)

Describe basic security capabilities in Azure

- Describe Azure DDoS protection
- Describe Azure Firewall
- Describe Web Application Firewall
- Describe Network Segmentation with VNet
- Describe Azure Network Security groups
- Describe Azure Bastion and JIT Access
- Describe ways Azure encrypts data



WAF Features

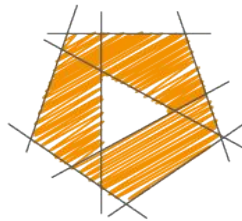
- SQL-injection attacks
- Cross-site scripting attacks
- Other common attacks, such as command injection, HTTP request smuggling, HTTP response splitting, and remote file inclusion
- HTTP protocol violations
- HTTP protocol anomalies, such as missing host user-agent and accept headers
- Bots, crawlers, and scanners
- Common application misconfigurations (for example, Apache and IIS)

OWASP Rule Sets

Core Rule Sets 3.1, 3.0, and 2.2.9

Custom Rules

Geomatch Rules

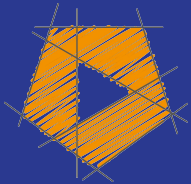


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe the capabilities of Microsoft Security solutions (25—30%)

Describe basic security capabilities in Azure

- Describe Azure DDoS protection
- Describe Azure Firewall
- Describe Web Application Firewall
- Describe Network Segmentation with VNet
- Describe Azure Network Security groups
- Describe Azure Bastion and JIT Access
- Describe ways Azure encrypts data

Data Encryption

Data at rest

Data in transit

Key management

Data At Rest

Server-Side Service-Managed Key - All Azure Database, Storage, AI, etc encrypted

Server-Side Customer-Managed Key - Using Azure Key Vault

Client-Side Client-Managed Key - SQL Server, SQL Database

Double Encrypted Option - VM managed disks

Data In Transit

SSL / HTTPS / TLS

Data encrypted internally between Azure datacenters (MACsec)

Option to enable for all data leaving Azure going to customers

You can force “HTTPS only” when accessing storage accounts

Can force “HTTPS only” for shared access signatures (SAS)

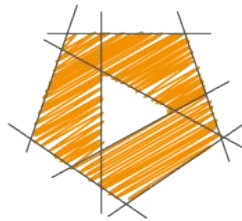
Azure Key Vault

Designed to securely store secrets, certifications and keys

Requires authenticated and authorized access to get key

Removes keys from common storage, code, source control

Can expire keys, generate new keys, etc.

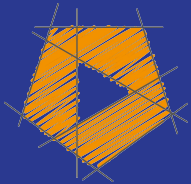


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe security management capabilities of Azure

- Describe Microsoft Defender for Cloud
- Describe Cloud Security Posture Management (CSPM)
- Describe how security policies and initiatives improve the cloud security posture
- Describe enhanced security features provided by cloud workload protection

Microsoft Defender for Cloud

Microsoft Defender for Cloud

Unify your DevOps
Security Management



Strengthen and manage your
cloud security posture



Protect your cloud
workloads



Defender for Cloud

1. Manage your cloud security posture
2. Prevent, detect, and respond quickly to modern threats
3. Unify DevOps security management

Manage Your Cloud Security Posture

- Identify the riskiest security issues
- Meet regulatory compliance requirements
- Assign recommendations

Security Dashboard

Microsoft Defender for Cloud | Overview
Showing subscription 'ContosoHotels'

Search (Ctrl+F) | Subscriptions | What's new

General

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Cloud Security Explorer (Preview)
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security

- Security posture
- Regulatory compliance
- Workload protections
- Firewall Manager
- DevOps Security (Preview)

Management

- Environment settings
- Security solutions
- Workflow automation

Key Metrics:

- 1 Azure subscriptions
- 2 AWS accounts
- 1 GCP projects
- 2536 Assessed resources
- 280 Active recommendations
- 1280 Security alerts

Security posture

135/161 Unassigned recommendation | 13/28 Overdue recommendations

Secure score: 37% SECURE SCORE

Cloud Provider	Score
Azure	40%
AWS	33%
GCP	34%

[Explore your security posture >](#)

Regulatory compliance

Azure Security Benchmark: 16 of 43 passed controls

Standard	Score
ISO 27001:2013	0/17
CMMC Level 3	0/55
Canada Federal PBMM	1/14

[Improve your compliance >](#)

Workload protections

Resource coverage: 99% For full protection, enable 2 resource plans

Alerts by severity: High 49, Medium 1

Firewall Manager

- 1 Firewalls
- 2 Firewall policies
- 1 Regions with firewalls

Network protection status by resource: 0/0

Virtual hubs: 0/0

OMI vulnerabilities detected (CVE-2022-29149):

The OMI elevation of privilege vulnerability (CVE-2022-29149) can allow attackers that abuse this vulnerability to execute arbitrary code and potentially take full control of a running host.

Microsoft supports auto-update for the OMI vulnerability. Please refer to the following link to activate it: [Auto-update](#)

[Read guidance >](#)

Upgrade to New Containers plan

Cloud-native **Kubernetes security** capabilities including environment hardening, vulnerability assessment, and run-time threat protection. The **new plan** merges two existing Defender plans, in addition to new and improved features.

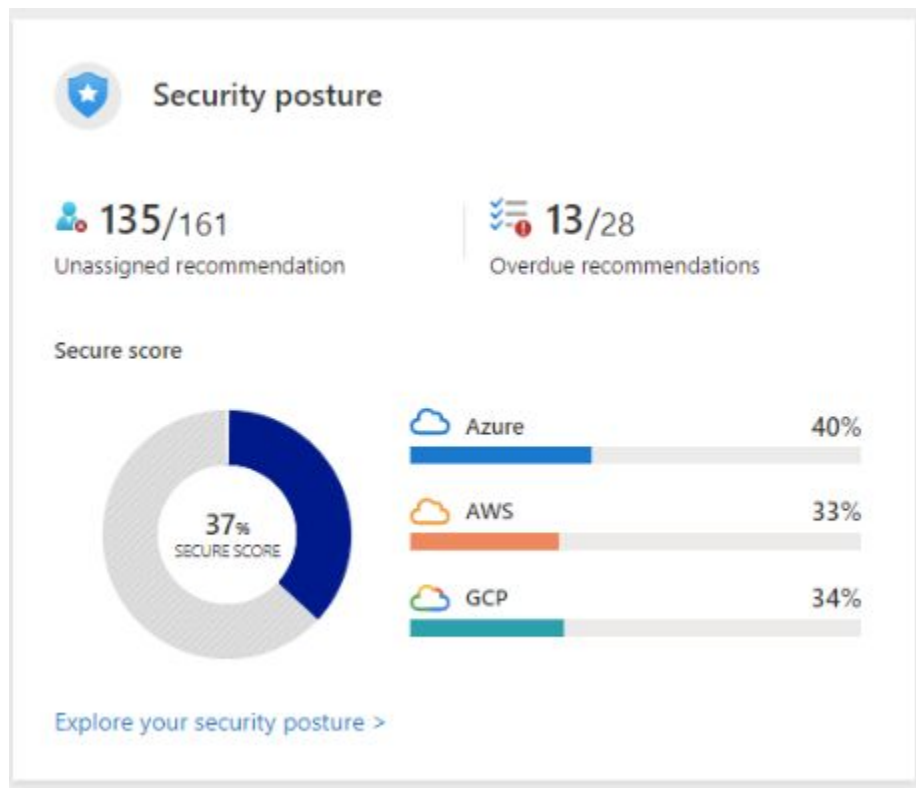
[Click here to upgrade >](#)

2 machines and 0 container images are vulnerable to Log4j vulnerabilities

All three log4j vulnerabilities (CVE-44228, CVE-2021-45105, CVE-2021-45046) can be remotely exploited, allowing an attacker that exploits the vulnerabilities to execute arbitrary code and potentially take full control of a running host or container.

[View machines](#) | [Read guidance](#)

Security Posture



Recommendations

Recommendations

Refresh Download CSV report Open query Governance report (preview) Guides & Feedback

Secure score recommendations All recommendations

34%
Secure score

158/231
Active recommendations

140 Attack path
With the riskiest recommendations. Open >

Click or tap
Open.

Azure AWS GCP

Search recommendations

Recommendation status == None

Severity == None

Resource type == None

Recommendation maturity == None

Add filter

More (2)

Show my items only: Off

Name	Max score	Current score	Potential score increase	Status	Unhealthy resources	Insights
Enable MFA	10	0.00	+ 18%	Overdue	3 of 3 resources	
Secure management ports	8	3.92	+ 6%	Overdue	27 of 177 resources	
Remediate vulnerabilities	6	2.27	+ 5%	Overdue	74 of 207 resources	
Apply system updates	6	3.31	+ 5%	Overdue	24 of 184 resources	
Encrypt data in transit	4	1.60	+ 4%	On time	81 of 180 resources	
Manage access and permissions	4	2.20	+ 4%	Overdue	77 of 792 resources	
Enable encryption at rest	4	0.70	+ 7%	Overdue	124 of 275 resources	
Remediate security configurations	4	1.74	+ 4%	Overdue	58 of 225 resources	
Restrict unauthorized network access	4	1.54	+ 6%	Overdue	164 of 553 resources	
Apply adaptive application control	3	1.18	+ 2%	Overdue	43 of 174 resources	
Enable endpoint protection	2	0.82	+ 1%	Overdue	42 of 180 resources	
Protect applications against DDoS attacks	2	0.92	+ 2%	Unassigned	11 of 86 resources	
Enable auditing and logging	1	0.19	+ 2%	Unassigned	309 of 426 resources	

Complex Scenarios

Microsoft Azure | Search resources, services, and docs (G+/) | admin@contoso.com | CONTOSOHOTELS.COM

Home > Microsoft Defender for Cloud | Recommendations > Microsoft Defender for Cloud | Attack paths (Preview) >

Internet exposed VM has high severity vulnerabilities and read permission to a Key Vault

1 Paths count | 3 Active Recommendations | 24:00:00 Freshness interval

Potential impact

Attacker with network access to the machine can exploit the vulnerabilities, gain remote code execution, and use the permission of the identity steal credentials
[Show more](#)

Resource types

- Managed Identity (1)
- Virtual Machine (1)
- Network interface (1)

[Show more](#)

Category

CREDENTIALS EXPOSURE COMPUTE ABUSE

Remediation steps

- Go to 'recommendations' tab and resolve all Defender for Cloud recommendations associated with the attack path
- Apply additional security best practices to reduce risk:
 - Harden the internet exposure to the minimum required

Attack path Recommendations

Below you can find all instances of the attack path in the selected subscriptions

mdc-demo-w2019 Entry point → mdc-demo-kv Target

Description

Virtual machine 'mdc-demo-w2019' is reachable from the internet, has high severity vulnerabilities allowing remote code execution on the machine and assigned with Managed Identity with read permission to Key Vault 'mdc-demo-kv'

```
graph LR; IP[13.94.184.26 IP Address] -- routes traffic to --> NIC[mdc-demo-w2019-nic Network Interface]; NIC -- routes traffic to --> VM[mdc-demo-w2019 Virtual Machine]; VM -- can authenticate as --> MI[mdc-demo-w2019 Managed Identity]; MI -- has permissions on --> KV[mdc-demo Key vault];
```

Steps to Fix

Management ports should be closed on your virtual machines ...

 Exempt  View policy definition  Open query

Severity

Medium

Freshness interval

 24 Hours

Tactics and techniques

 Initial Access

^ Description

Open remote management ports are exposing your VM to a high level of risk from Internet-based attacks. These attacks attempt to brute force credentials to gain admin access to the machine.

^ Remediation steps

Manual remediation:

We recommend that you edit the inbound rules of some of your virtual machines, to restrict access to specific source ranges.

To restrict access to your virtual machines:

1. Select a VM to restrict access to.
2. In the 'Networking' blade, click on each of the rules that allow management ports (for example, RDP-3389, WINRM-5985, SSH-22).
3. Either change the 'Action' property to 'Deny', or, improve the rule by applying a less permissive range of source IP ranges.
4. Click 'Save'.


Use Defender for Cloud's Just-in-time (JIT) virtual machine (VM) access to lock down inbound traffic to your Azure VMs by demand. Learn more in [Understanding just-in-time \(JIT\) VM access](#).

^ Affected resources

Unhealthy resources (1)

Healthy resources (10)

Not applicable resources (38)

<input type="checkbox"/>	Name	↑↓	Subscription	Owner
<input type="checkbox"/>	 mdc-demo-w2019		ContosoHotels	

Assign an Owner


^ **Affected resources**

Unhealthy resources (1) Healthy resources (10) Not applicable resources (38)

🔍 Search virtual machines

<input checked="" type="checkbox"/> Name	↑↓ Subscription
<input checked="" type="checkbox"/> 🖥️ mdc-demo-w2019	ContosoHotels

Trigger logic app Exempt **Assign owner** Change owner and set ETA



Risk Hunting

Cloud Security Explorer

The screenshot shows the Microsoft Defender for Cloud Cloud Security Explorer interface. At the top, there's a navigation bar with the Microsoft Azure logo, a search bar, and user information (admin@contoso.com). Below the navigation bar, the page title is "Microsoft Defender for Cloud | Cloud Security Explorer (Preview)". A search bar is present, along with links for "Guides & Feedback" and "Share query link".

The left sidebar contains a navigation menu with categories: "General" (Overview, Getting started, Recommendations, Security alerts, Inventory, Cloud Security Explorer (Preview), Workbooks, Community, Diagnose and solve problems), "Cloud Security" (Security posture, Regulatory compliance, Workload protections, Firewall Manager, DevOps Security (Preview)), and "Management" (Environment settings, Security solutions, Workflow automation).

The main content area features a "What would you like to search?" section with a "Select resource types" dropdown and a "Start creating a query" button. Below this is a "Query templates" section with a "Scope: All" filter and a search bar. A callout bubble points to the first template, stating "Click or tap the query template." The templates are arranged in a grid:

- Internet exposed VMs**: Returns all internet exposed virtual machines. [Open query >](#)
- Internet exposed VMs with high severity vulnerabilities**: Returns all internet exposed virtual machines that have high severity vulnerabilities. [Open query >](#)
- VMs vulnerable to a specific vulnerability**: Returns all internet exposed virtual machines vulnerable to Log4Shell vulnerabilities. [Open query >](#)
- Internet exposed SQL servers with managed identity**: Returns all internet exposed SQL servers with managed identity assigned. [Open query >](#)
- User accounts without MFA and with permissions to Storage Accounts**: Returns all user accounts that do not have MFA enabled, and have permissions on a storage account. [Open query >](#)
- Azure Kubernetes pods running images with high severity vulnerabilities**: Returns all kubernetes pods running an image with vulnerability severity. [Open query >](#)
- Key Vault keys and secrets without any expiration period**: Returns all Azure key vaults where expiration is not set for secrets or keys. [Open query >](#)
- User accounts with permission to vulnerable VMs**: Returns all user accounts with permission to VMs that have high severity vulnerabilities. [Open query >](#)
- Internet exposed SQL Servers tagged as production**: Returns all SQL Servers which tagged as production and exposed to the internet. [Open query >](#)
- External users with permission to SQL VMs allow code execution on the host**: Returns all the users with permissions to a SQL VM that can run scripts on the host. [Open query >](#)

Query for Conditions



AND

- Azure Storage accounts
- That Exposed to the internet
- That Contains sensitive data

Fix Recommendations

Secure transfer to storage accounts should be enabled ...

 Exempt  Deny  View policy definition  Open query

Severity

High

Freshness interval

 30 Min

Tactics and techniques

 Credential Access +1

^ Description

Secure transfer is an option that forces your storage account to accept requests only from secure connections (HTTPS). Use of HTTPS ensures authentic

^ Remediation steps

Quick fix:

Select the unhealthy resources and click "Fix" to launch "Quick fix" remediation. [Learn more >](#)

Note: After the process completes, it may take up to 30 min until your resources move to the 'healthy resources' tab.

Quick fix logic

Manual remediation:

To enable secure transfer required:

1. In your storage account, go to the 'Configuration' page.
2. Enable 'Secure transfer required'.

Fixing resources

Fix 1 resource

This action updates your storage account security to only allow requests by secure connections. (HTTPS).



- Any requests using HTTP will be rejected.
- When you are using the Azure files service, connection without encryption will fail, including scenarios using SMB 2.1, SMB 3.0 without encryption, and some flavors of the Linux SMB client. [Learn more.](#)

See Hacking Attempts

























Recommendations Alerts

Subscription == All

Status == Active X

Severity == Low, Medium, High X

 Add filter

Severity 	Alert title 	Activity start time (UTC-7) 	MITRE ATT&CK® tactics	Status 
Medium	 Suspected brute-force attack attempt	08/23/22, 09:00 PM	 Pre-attack	Active
Medium	 Suspected brute-force attack attempt	08/18/22, 09:00 PM	 Pre-attack	Active
Medium	 Suspected brute-force attack attempt	08/16/22, 09:00 PM	 Pre-attack	Active
Medium	 Suspected brute-force attack attempt	08/11/22, 09:00 PM	 Pre-attack	Active
Medium	 Suspected brute-force attack attempt	08/04/22, 09:00 PM	 Pre-attack	Active
Medium	 Suspected brute-force attack attempt	08/02/22, 09:00 PM	 Pre-attack	Active
Medium	 Suspected brute-force attack attempt	07/28/22, 09:00 PM	 Pre-attack	Active
Medium	 Suspected brute-force attack attempt	07/26/22, 09:00 PM	 Pre-attack	Active
Medium	 Suspected brute-force attack attempt	07/21/22, 09:00 PM	 Pre-attack	Active
Medium	 Suspected brute-force attack attempt	07/19/22, 09:00 PM	 Pre-attack	Active

<https://t.me/learningnets>

Compliance Posture

Regulatory Compliance

[Home](#) > [Microsoft Defender for Cloud | Overview](#) >

Regulatory Compliance ...

[Download report](#) [Manage compliance policies](#) [Open query](#) [Compliance over time workbook](#) [Audit reports](#)

i You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above. →

Azure Security Benchmark

16 of 43 passed controls



Lowest compliance regulatory standards

[Show all 27](#)

ISO 27001:2013	0/17
CMMC Level 3	0/55
Canada Federal PBMM	1/14
SWIFT CSP CSCF v2020	1/14

Where You Are Out of Compliance

NS. Network Security

NS-1. Establish network segmentation boundaries [Control details](#) MS C

NS-2. Secure cloud services with network controls [Control details](#) MS C

Customer responsibility

Storage accounts should restrict network access using virtual network rules

Resource type

Storage accounts

Failed resources

72 of 72

Resource compliance status



Storage account should use a private link connection

Storage accounts

71 of 72



Access to storage accounts with firewall and virtual network configurations should be restricted

Storage accounts

69 of 72



Storage account public access should be disallowed [Quick Fix](#)

Storage accounts

58 of 72



Private endpoint should be configured for Key Vault

Key vaults

22 of 23



1 2 3 4 5 6 < >

Implement Policies to Prevent Violations

Home > Microsoft Defender for Cloud | Overview > Regulatory Compliance >

Storage account public access should be disallowed

Azure Security Benchmark

[Exempt](#) [Deny](#) [View policy definition](#) [Open query](#)

Severity

Medium

Freshness interval

30 Min

Tactics and techniques

Initial Access

Description

Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data, but might present security risks. To prevent data breaches caused by undesired anony

Remediation steps

Deny - Prevent resource creation

1 subscriptions

Set the scope for the deny effect of your Azure Policy. The deny effect prevents the creation of resources that don't satisfy the recommendation.

[Learn more about the Azure Policy deny effect.](#)

Item	Current status	More
<input type="checkbox"/>  Tenant Root Group (1 of 1 subscriptions)		
<input type="checkbox"/>  Root (1 of 1 subscriptions)		
<input type="checkbox"/>  Demo (1 of 1 subscriptions)		
<input checked="" type="checkbox"/>  ContosoHotels	Audit	

Audit Reports

Microsoft Azure

Home > Regulatory Compliance >

Audit reports

US Government ISO **PCI** SOC Industry & Regional HITRUST

Showing 1 to 5 of 5 results

Region : All Regulatory standard : All Industry : All

Title ↑↓	Download	Description
2021 - Azure PCI DSS 3.2.1 Package	Download	Certificate demonstrating Microsoft Azure, Dynamics 365, and various Microsoft Online Services are PCI DSS certified
2021 - Azure PCI 3DS 1.0 Package	Download	Certificate demonstrating Microsoft Azure, Dynamics 365, and various Microsoft Online Services are PCI 3DS certified
Microsoft Azure Commercial System Security Plan (SSP) v3.6 20201124	Download	Public copy of the Azure Commercial SSP.
2020 - PCI DSS 3.2.1 - Azure Shared Responsibility Matrix	Download	PCI DSS Shared Responsibility Matrix
Azure PCI DSS 3.2.1 AOC Package	Download	PCI AOC reports covering Azure (Public) and Azure Government

Security Governance

Overdue Recommendations









Environment Owner (preview)



Pa|

Owner == **None** X

Recommendation severity == **None** X

Name ↑↓	Overdue recommendations ↑↓	Affected resources ↑↓	Recommendations
 AllanD@contoso.com	● 20/52 overdue ⓘ	 96 of 262	View recommendations >
 AlexW@contoso.com	● 1/1 overdue ⓘ	 8 of 8	View recommendations >
 ChristieC@contoso.com	● 0/2 overdue	 0 of 2	View recommendations >
 IrvinS@contoso.com	● 0/1 overdue	 0 of 3	View recommendations >

Governance Rules

Home > Microsoft Defender for Cloud | Environment settings > Settings

Settings | Governance rules (preview) ...

ContosoHotels

Search (Ctrl+/)

+ Add rule Refresh | Enable Disable Delete | Governance report (preview) Guides & Feedback

Settings

- Defender plans
- Auto provisioning
- Email notifications
- Integrations
- Workflow automation
- Continuous export

Policy settings

- Security policy
- Governance rules (preview)

Set recommendations' ownership assignment and expected remediation timeframe rules.

<input type="checkbox"/> Rule name ↑↓	Status ↑↓	Priority ↑↓	Affected reco
<input type="checkbox"/> Ensure Defender plans enablement	Enabled	1	10 recommen
<input type="checkbox"/> Remediate high severity recommendations	Enabled	2	High severity
<input type="checkbox"/> Secure transfer should be enabled by default	Enabled	102	1 recommend

Email Nag

Action required: Implement Microsoft Defender for Cloud recommendations



Microsoft Defender for Cloud <DefenderCloudnoreply@microsoft.com>
To Christie Cline

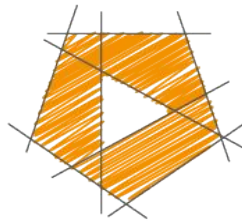


Action required

Implement active recommendations assigned to you in Microsoft Defender for Cloud

You're assigned as the owner of several active Microsoft Defender for Cloud security recommendations in subscription ContosoHotels (d1d8779d-38d7-4f06-91db-9cbc8de0176f).

Recommendation	Severity	Number of affected resources
Machines should have a vulnerability assessment solution	Medium	110 (0 overdue)
Windows Defender Exploit Guard should be enabled on machines	Medium	97 (0 overdue)

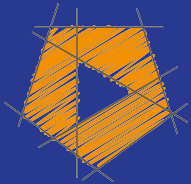


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe security management capabilities of Azure

- Describe Microsoft Defender for Cloud
- Describe Cloud Security Posture Management (CSPM)
- Describe how security policies and initiatives improve the cloud security posture
- Describe enhanced security features provided by cloud workload protection

Cloud security posture management (CSPM)


The top right corner of the slide features a decorative graphic consisting of several overlapping triangles in various shades of pink and magenta, creating a modern, abstract design.

CSPM identifies and remediates risk

CSPM

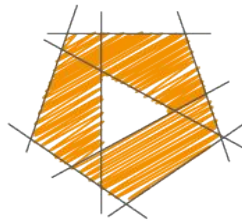
- automating visibility
- uninterrupted monitoring
- threat detection
- remediation workflows

Highest percentage
of errors still comes
from cloud
misconfigurations
and human error

The background is a solid pink color with several dark pink triangles of varying sizes and orientations scattered across the top right and middle sections.

Defender for Cloud
helps identify
vulnerabilities and
manage mitigations

CSPM continuously analyzes the security state of your entire cloud platform, not just individual apps or resources

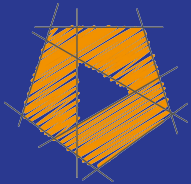


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe capabilities of Microsoft Sentinel

- Define the concepts of security information and event management (SIEM) and security orchestration automated response (SOAR)
- Describe threat detection and mitigation capabilities in Microsoft Sentinel

Microsoft Sentinel

Microsoft Sentinel is a scalable, cloud-native, security information and event management (SIEM) and security orchestration automated response (SOAR) solution.

Intelligent security
analytics and threat
intelligence across
an enterprise.

- alert detection
- threat visibility
- proactive hunting
- threat response

Key Capabilities (SIEM):

Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.

Detect previously uncovered threats and minimize false positives.

Investigate threats with artificial intelligence (AI).

Respond to incidents rapidly.

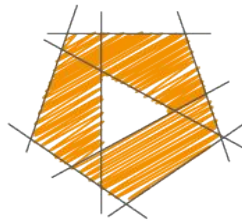
Key Capabilities (SOAR):

Takes alerts from many sources including SIEM

Triggers action-driven automated workflows and processes

Run security tasks that mitigate the issue

Security insights and security automation

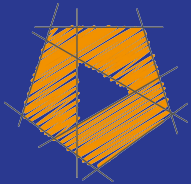


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe threat protection with Microsoft Defender XDR

- Describe Microsoft Defender XDR services
- Describe Microsoft Defender for Office 365
- Describe Microsoft Defender for Endpoint
- Describe Microsoft Defender for Cloud Apps
- Describe Microsoft Defender for Identity
- Describe Microsoft Defender Vulnerability Management
- Describe Microsoft Defender Threat Intelligence (Defender TI)
- Describe the Microsoft Defender portal

Security Products in Azure / M365

Microsoft Defender for Cloud - CSPM (security posture, configuration and settings)

Microsoft Sentinel - SIEM/SOAR (log ingestion)

Microsoft Defender XDR - XDR (unified pre- and post-breach enterprise defense suite)

XDR - Extended Detection and Response

United suite of enterprise defense services

Detection
Prevention
Investigation
Response



Not just network protection...

... apps and
services that run on
the network, the
identities, devices,
M365, etc

- Home
- Investigation & response
 - Incidents & Alerts
 - Hunting
 - Actions & submissions
 - Partner catalog
- Microsoft Sentinel
 - Search
 - Threat management
 - Content management
 - Configuration
- Threat intelligence
- Assets
- Identity
- Endpoints
- Email & collaboration
- Cloud apps
- IoT
- Optimize
- Reports
- Learning hub

Key metrics indicate a positive trend in your organization's efficiency

The average time it takes to respond to and close incidents has decreased.

Mean time to acknowledge

10 minutes

↓ 65%

Mean time to close

3 minutes

↓ 25%

Time saved by automation

300 hours

↑ 82%

Guided Tour Customize page

Unified incidents and alerts

145 active incidents

Service sources: Defender XDR, Sentinel, Defender for Cloud, Endpoint, Office, Identity, Applications, and IoT



Active incidents by severity



Closed incidents by classification

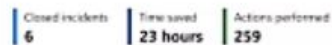


Closed incidents and alerts over time



Sentinel automation

33 automation rules



Actions performed by type



[Configure automation rules](#) [View workbook](#)

Entities from Sentinel

Discovered entities related to incidents

12.3K Hosts

11.8K IPs

Featured Threat intelligence articles

Storm-0062 attempts to exploit CVE 2023-22515 in Atlassian Confluence

1 day ago | 5 indicators

Diamond Sleet compromises TeamCity servers

6 day ago | 15 indicators

WS FTP Server critical vulnerabilities

7 days ago | no indicators

Microsoft Defender XDR services

Integrated Microsoft 365 Defender experience



+



+



+



Identity

Microsoft Defender
for Identity

Endpoints

Microsoft Defender
for Endpoint

Apps

Microsoft Cloud
App Security

Email/Collaboration

Microsoft Defender
for Office 365

Microsoft Cloud App Security
SaaS apps and data

Microsoft Defender for Endpoint
Devices

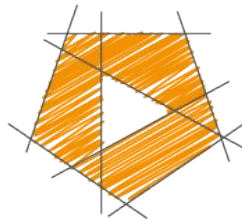
Microsoft Defender for Office 365
Microsoft 365 cloud apps and data

Identity

On-premises

Microsoft
Defender for
Identity

MFA
Conditional Access
Azure AD Identity Protection

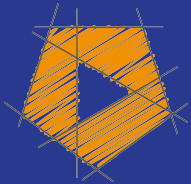


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe threat protection with Microsoft Defender XDR

- Describe Microsoft Defender XDR services
- Describe Microsoft Defender for Office 365
- Describe Microsoft Defender for Endpoint
- Describe Microsoft Defender for Cloud Apps
- Describe Microsoft Defender for Identity
- Describe Microsoft Defender Vulnerability Management
- Describe Microsoft Defender Threat Intelligence (Defender TI)
- Describe the Microsoft Defender portal

Microsoft Defender for Identity

Formerly Advanced Threat Protection (ATP)

Entra ID Signals

<https://t.me/learningnets>

Microsoft Defender for Identity

Monitor user behavior and activities

Protect users identities and reduce attack surface

Identify suspicious activities and attacks across the kill-chain

Alerts

License plans:

- EMS E5 or stand alone

Understanding what
is normal behavior
for each user?

Identify behavior anomalies

Security reports and user profile analytics

Kill-chain: attacks
start with
low-hanging fruit

Then try to move
over (lateral) or
move up

Defender for Identity is designed to reduce general alert noise, providing only relevant, important security alerts in a simple, real-time organizational attack timeline.

Identity Risks

Anonymous IP Address

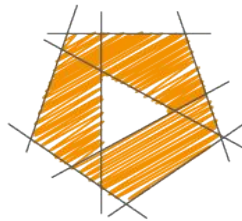
Atypical travel

Malware linked IP address

Leaked credentials

Password spray

Inbox forwarding

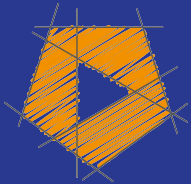


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe threat protection with Microsoft Defender XDR

- Describe Microsoft Defender XDR services
- Describe Microsoft Defender for Office 365
- Describe Microsoft Defender for Endpoint
- Describe Microsoft Defender for Cloud Apps
- Describe Microsoft Defender for Identity
- Describe Microsoft Defender Vulnerability Management
- Describe Microsoft Defender Threat Intelligence (Defender TI)
- Describe the Microsoft Defender portal

Microsoft Defender for Office 365

Formerly Office 365 Advanced Threat Protection (ATP)

Microsoft Defender for O365

E-mails

Links (URLs)

Collaboration tools (Teams, Sharepoint Online, OneDrive for Business, etc)

Licenses:

- O365 Plan 1, O365 Plan 2
- M365 E5, O365 E5/A5, and M365 Business Premium

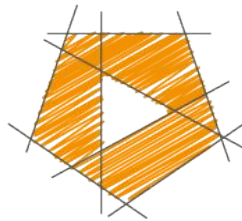
Plan 1

- Safe Attachments
- Safe Links
- Protection for SharePoint, OneDrive, and Microsoft Teams
- Anti-phishing protection
- Real-time detections

Plan 2

All features of Plan 1 plus...

- Threat Trackers
- Threat Explorer
- Automated investigation and response (AIR)
- Attack Simulator

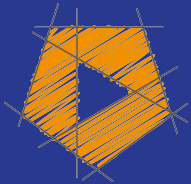


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe threat protection with Microsoft Defender XDR

- Describe Microsoft Defender XDR services
- Describe Microsoft Defender for Office 365
- Describe Microsoft Defender for Endpoint
- Describe Microsoft Defender for Cloud Apps
- Describe Microsoft Defender for Identity
- Describe Microsoft Defender Vulnerability Management
- Describe Microsoft Defender Threat Intelligence (Defender TI)
- Describe the Microsoft Defender portal

Microsoft Defender for Endpoint

Formerly Microsoft Defender Advanced Threat Protection (ATP)

Microsoft Defender for Endpoint

Endpoints are “devices”

Think of your laptop, phone, tablet - regardless of operating system

Microsoft Defender for Endpoint

 Expand table



Core Defender
Vulnerability
Management



Attack
surface
reduction



Next-
generation
protection



Endpoint
detection and
response



Automated
investigation and
remediation



Microsoft
Threat
Experts

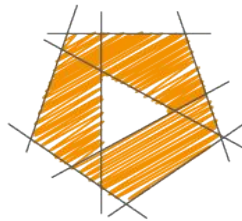
Centralized configuration and administration, APIs

Microsoft Defender XDR

Microsoft Defender for Endpoint

- Threat and vulnerability management (core)
- Attack surface reduction
- Next generation protection
- Endpoint detection and response
- Automated investigation and remediation
- Microsoft Threat Experts
- Management and APIs

Microsoft Secure Score for Devices

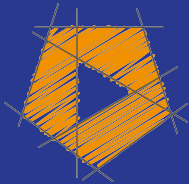


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe threat protection with Microsoft Defender XDR

- Describe Microsoft Defender XDR services
- Describe Microsoft Defender for Office 365
- Describe Microsoft Defender for Endpoint
- Describe Microsoft Defender for Cloud Apps
- Describe Microsoft Defender for Identity
- Describe Microsoft Defender Vulnerability Management
- Describe Microsoft Defender Threat Intelligence (Defender TI)
- Describe the Microsoft Defender portal

Microsoft Defender for Cloud Apps



Microsoft Defender for Cloud Apps (CASB)

CAS Security Framework

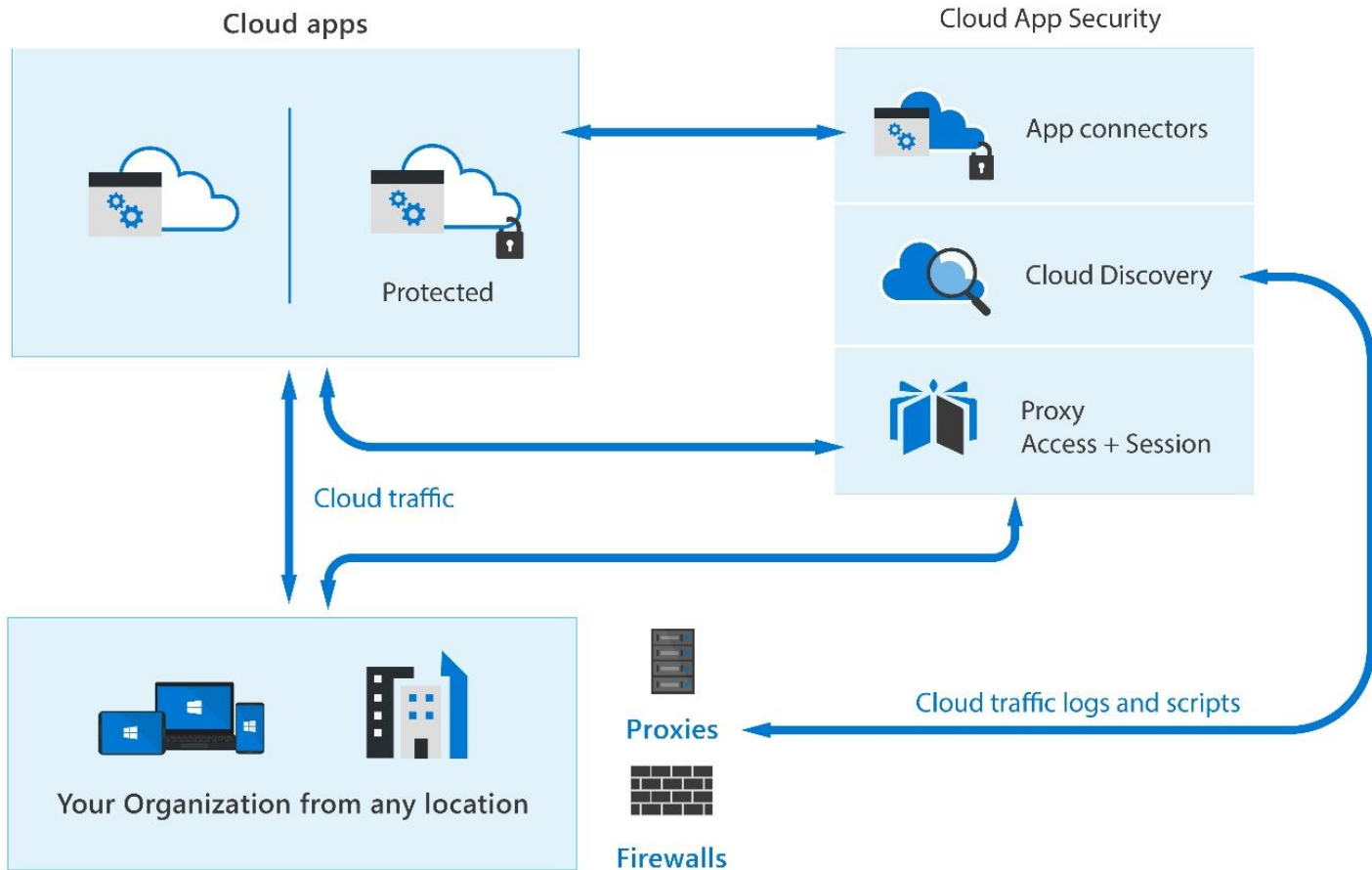
O365 CAS

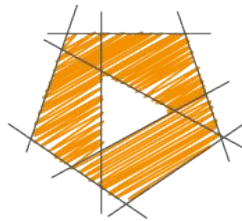
Enhanced Cloud App Discovery in AAD

CAS architecture

Discover Shadow IT

<https://t.me/learningnets>



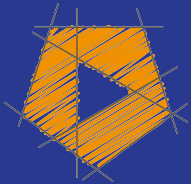


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



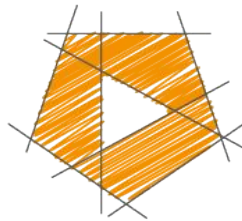
© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe threat protection with Microsoft Defender XDR

- Describe Microsoft Defender XDR services
- Describe Microsoft Defender for Office 365
- Describe Microsoft Defender for Endpoint
- Describe Microsoft Defender for Cloud Apps
- Describe Microsoft Defender for Identity
- Describe Microsoft Defender Vulnerability Management
- Describe Microsoft Defender Threat Intelligence (Defender TI)
- Describe the Microsoft Defender portal

Microsoft Defender Vulnerability Management

Add-on for Defender for Endpoint (Plan 2)

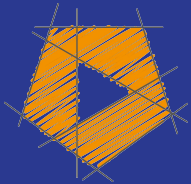


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor

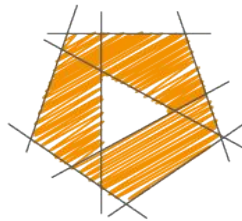


© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe threat protection with Microsoft Defender XDR

- Describe Microsoft Defender XDR services
- Describe Microsoft Defender for Office 365
- Describe Microsoft Defender for Endpoint
- Describe Microsoft Defender for Cloud Apps
- Describe Microsoft Defender for Identity
- Describe Microsoft Defender Vulnerability Management
- Describe Microsoft Defender Threat Intelligence (Defender TI)
- Describe the Microsoft Defender portal

Microsoft Defender Threat Intelligence

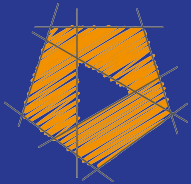


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe threat protection with Microsoft Defender XDR


- Describe Microsoft Defender XDR services
- Describe Microsoft Defender for Office 365
- Describe Microsoft Defender for Endpoint
- Describe Microsoft Defender for Cloud Apps
- Describe Microsoft Defender for Identity
- Describe Microsoft Defender Vulnerability Management
- Describe Microsoft Defender Threat Intelligence (Defender TI)
- Describe the Microsoft Defender portal

Microsoft Defender Portal

<https://t.me/learningnets>

<https://security.microsoft.com>

<https://t.me/learningnets>



Manage security
across identities,
data, devices, apps,
and infrastructure

Microsoft Defender Portal

The screenshot displays the Microsoft 365 Defender portal for the domain `contosohotels.com`. The interface is organized into several key sections:

- Home:** The main dashboard area.
- Threat analytics:** Shows 2 active threats, including "NOBOLM mass email campaign" and "Living off the land binaries".
- Active incidents:** Displays 112 active incidents. A line graph shows incident activity over time. Below the graph is a table of recent incidents:

Incident name	Type	Severity	Last activity	Scope
Unsanctioned cloud app access was blocked on multiple endpoints	Informational	Low	Dec 10, 2021 11:37...	IT, 2
Activity from infrequent country involving one user	Medium	Medium	Dec 10, 2021 12:08...	IT, 1
"Minikatz" detected on multiple endpoints	High	High	Dec 10, 2021 12:00...	IT, 6
Malicious credential theft tool execution detected on one endpoint	High	High	Dec 10, 2021 11:58...	IT, 1

- Users at risk:** Shows 88 users at risk, categorized by risk level (High, Medium, Low).
- Device health:** Shows 682 active devices. A bar chart indicates the status of devices: Misconfigured (0) and Inactive (12,402).
- Devices at risk:** Shows 10 device(s) at risk, with a table listing device types and risk levels.
- Discovered devices:** Shows a total of 14,116 discovered devices, broken down into 1 IoT device, 14,085 endpoints, and 3 high-value devices.
- Security news feed:** Features a Microsoft Security Intelligence article about a vulnerability update.

- Protection
- Detection
- Investigation
- Response

- Email
- Collaboration
- Identity
- Device
- Cloud App

- Defender for Office 365
- Defender for Endpoint
- Defender for Identity
- Defender for Cloud Apps

A Set of Unified Experiences For...

- Incidents & alerts
- Hunting
- Actions & submissions
- Threat analytics
- Secure score
- Learning hub
- Trials



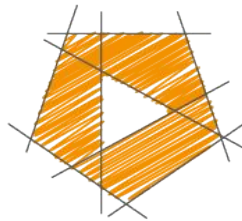
Incidents

Create a notification rule

Most recent incidents and alerts

1-7 < > 6 months Choose columns 30 items per page Filters

✓	Incident name	Tags	Severity	Investigation state
>	Multi-stage incident involving Initial access & Exfiltration on one endpoint ...	asdf tag test02	■■■ High	2 investigation states
>	Multi-stage incident involving Initial access & Exfiltration on multiple endp...	asdf tag test02 IT Team +3	■■■ High	2 investigation states
>	Multi-stage incident involving Initial access & Exfiltration on one endpoint ...	ar test01 asdf tag test02	■■■ High	4 investigation states
>	Multi-stage incident on one endpoint reported by multiple sources	asdf tag test02	■■■ Medium	2 investigation states
>	Multi-stage incident involving Persistence & Exfiltration on one endpoint r...	asdf tag test02	■■■ Medium	2 investigation states
>	Multi-stage incident involving Initial access & Discovery on multiple endpo...	test01 test02 test03 +7	■■■ High	4 investigation states

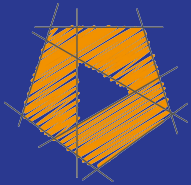


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe the capabilities of Microsoft compliance solutions (20–25%)

Describe Microsoft Service Trust Portal and privacy principles

- Describe the Service Trust Portal offerings
- Describe the privacy principles of Microsoft
- Describe Microsoft Priva

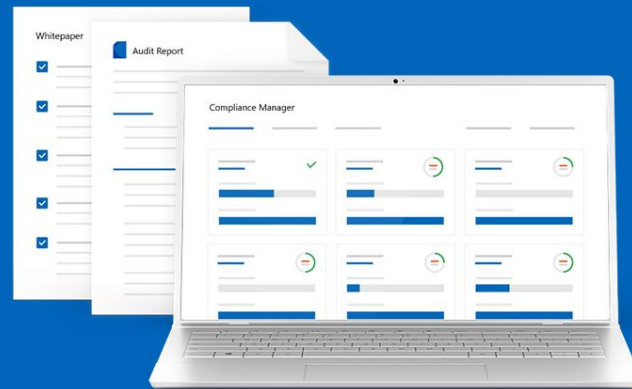
Service Trust Portal

<https://t.me/learningnets>

<https://servicetrust.microsoft.com/>

<https://aka.ms/STP>

Built upon a foundation of
trust, security and
compliance



Audit Reports

Review the available independent audit reports for Microsoft's Cloud services, which provide information about compliance with data protection standards and regulatory requirements, such as International Organization for Standardization (ISO), Service Organization Controls (SOC), National Institute of Standards and Technology (NIST), Federal Risk and Authorization Management Program (FedRAMP), and the General Data Protection Regulation (GDPR)



SOC



<https://t.me/learningnets>

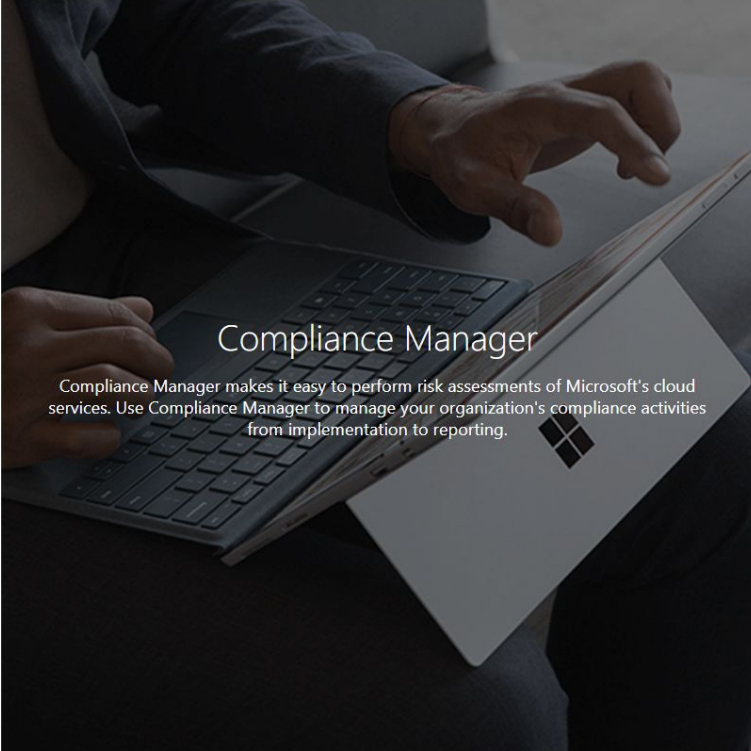


ISO 27001



PCI/DSS

Documents & Resources



Compliance Manager

Compliance Manager makes it easy to perform risk assessments of Microsoft's cloud services. Use Compliance Manager to manage your organization's compliance activities from implementation to reporting.

Pen Tests & Security Assessments

View reports from independent third-party penetration tests and security assessments of Microsoft's cloud services

Azure Blueprints

Define a repeatable set of Azure resources that implement and adhere to your organization's standards, patterns, and requirements and rapidly build new environments with a set of built-in components to speed up development and delivery

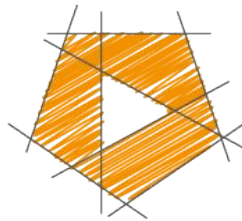
White Papers, FAQs, & Compliance Guides

Review the wealth of available security implementation and design information with the goal of making it easier for you to meet regulatory compliance objectives by understanding how Microsoft Cloud services keep your data secure

[More Documents & Resources >](#)

<https://t.me/learningnets>



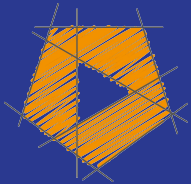


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe the capabilities of Microsoft compliance solutions (20–25%)

Describe Microsoft Service Trust Portal and privacy principles

- Describe the Service Trust Portal offerings
- Describe the privacy principles of Microsoft
- Describe Microsoft Priva

Privacy Principles

Microsoft's Six Privacy Principles

- Control
- Transparency
- Security
- Strong legal protections
- No content-based targeting
- Benefits to you

You're in control of
your privacy with
easy tools and clear
choices.

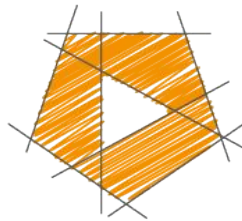
Transparent about
the data they
collect

Strong security and the use of encryption

Respecting local privacy laws and fighting for privacy

They won't use the
content of
documents and
emails to target ads

They only collect
data to make your
experience better

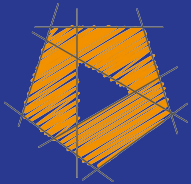


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>


Describe the capabilities of Microsoft compliance solutions (20–25%)

Describe Microsoft Service Trust Portal and privacy principles

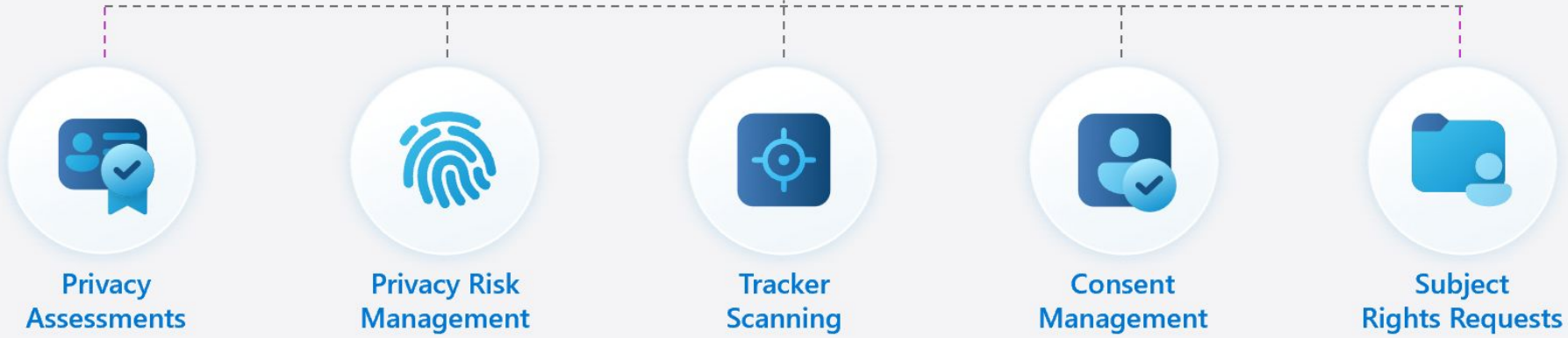
- Describe the Service Trust Portal offerings
- Describe the privacy principles of Microsoft
- Describe Microsoft Priva

Microsoft Priva

<https://t.me/learningnets>



Automate the
management,
definition, and
tracking of privacy
operations at scale



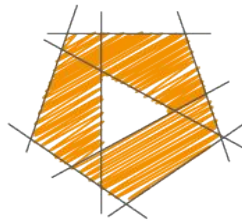
Consent Management (preview)

Privacy Assessments (preview)

Privacy Risk Management

Subject Rights Requests

Tracker Scanning (preview)

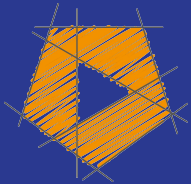


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe the compliance management capabilities of Microsoft Purview

- Describe the Microsoft Purview compliance portal
- Describe compliance manager
- Describe the use and benefits of compliance score

Microsoft Purview

<https://t.me/learningnets>

Microsoft Purview is a comprehensive data governance service offered by Microsoft.

It helps organizations manage their data across various environments including on-premises, multi-cloud, and SaaS.

The goal of **Microsoft Purview** is to provide a unified platform for governing, protecting, and managing data, regardless of where it resides.

Purview Features:

- Up-to-date map of your data landscape
 - Data discovery
 - Sensitive data classification
 - End-to-end data lineage
- Enable data curators to manage and secure data
- Empower data consumers to find valuable, trustworthy data



Microsoft Purview governance portal



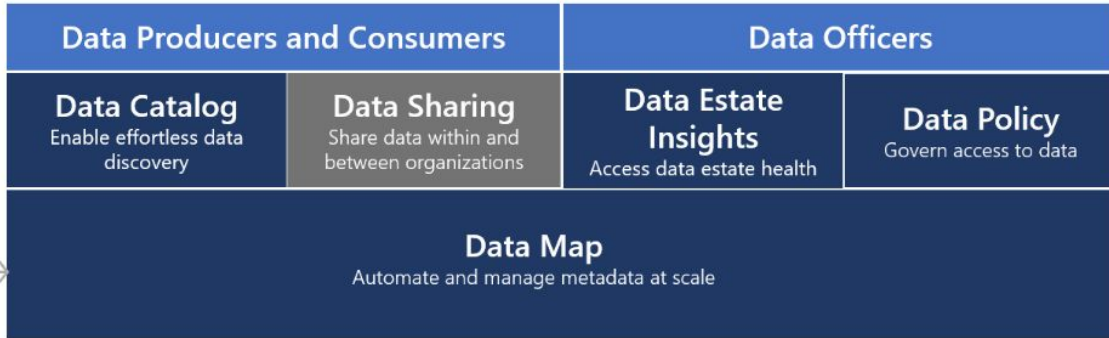
On-premises



Cloud



SaaS Applications



Azure Synapse Analytics



SQL Server



Power BI



Azure SQL



Microsoft 365

Generally Available


Preview

Microsoft Purview Compliance Portal

<https://t.me/learningnets>

<https://purview.microsoft.com/>

<https://t.me/learningnets>



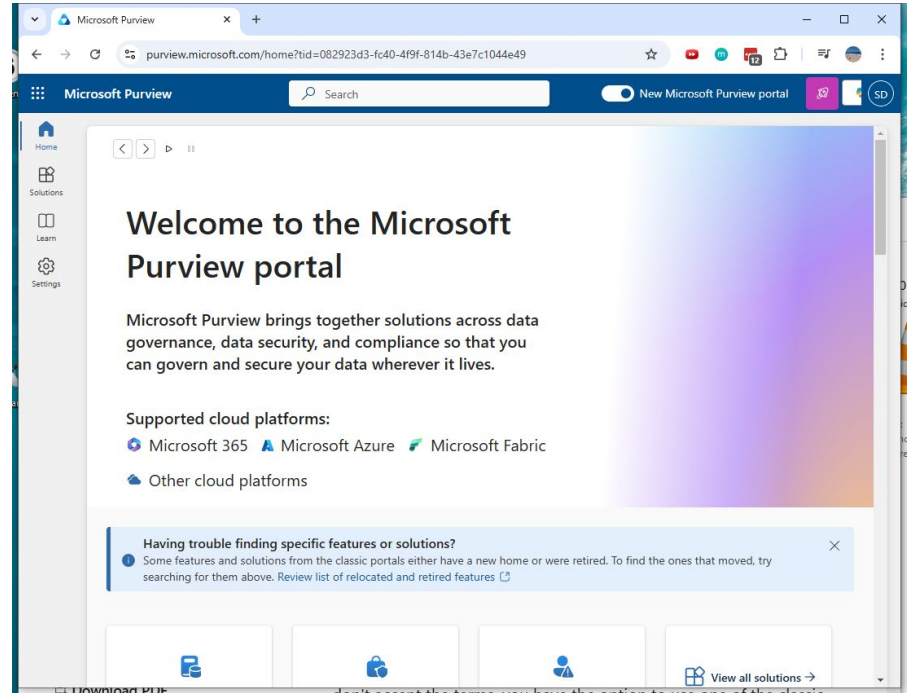
Help understand
and manage an
organization's
compliance needs

Microsoft Purview Compliance Portal

Compliance score

Solution catalog

Active alerts



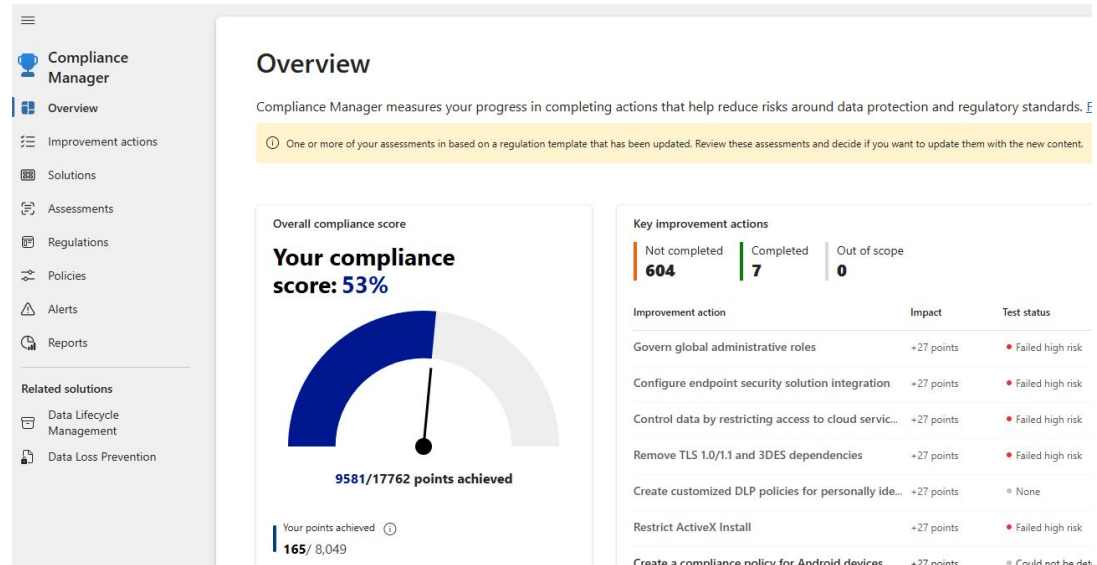
Compliance manager

Prebuilt assessments

Workflow capabilities

Step-by-step improvement actions

Compliance score

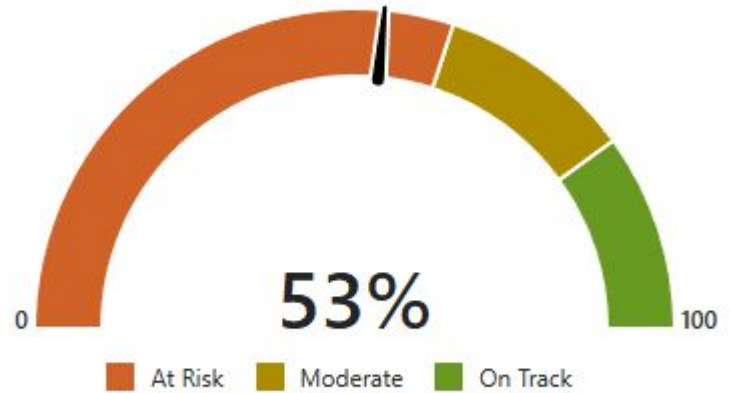


Compliance score

Helps an organizations:

Understand its current compliance posture

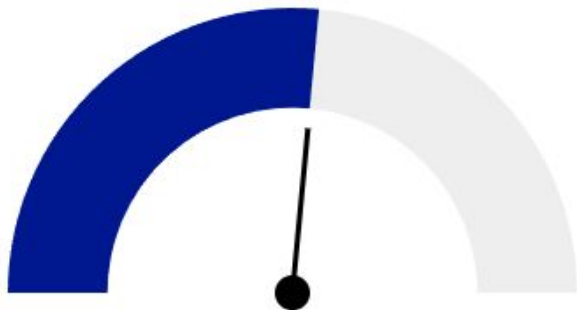
Prioritize actions based on their potential to reduce risk



Compliance score

Overall compliance score

Your compliance score: 53%



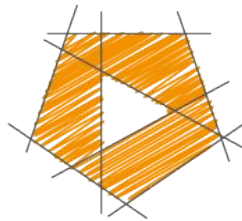
9581/17762 points achieved

Your points achieved ⓘ
165 / 8,049

Key improvement actions

Not completed **604** | Completed **7** | Out of scope **0**

Improvement action	Impact	Test status
Govern global administrative roles	+27 points	• Failed hig
Configure endpoint security solution integration	+27 points	• Failed hig
Control data by restricting access to cloud servic...	+27 points	• Failed hig
Remove TLS 1.0/1.1 and 3DES dependencies	+27 points	• Failed hig
Create customized DLP policies for personally ide...	+27 points	• None
Restrict ActiveX Install	+27 points	• Failed hig

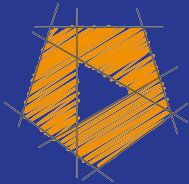


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe information protection and data lifecycle management capabilities of Microsoft Purview

- Describe data classification capabilities
- Describe the benefits of content and activity explorer
- Describe sensitivity labels
- Describe Data Loss Prevention (DLP)
- Describe Records Management
- Describe Retention Policies and Retention Labels

Data Classification

Data classification



Sensitive information types

Trainable classifiers

Content explorer

<https://t.me/learningnets>

Activity explorer

<https://t.me/learningnets>

Content Explorer

A current snapshot of individual items that have been classified across the organization




Explore the email and docs in your organization that contain sensitive info or have labels applied. You drill down further by reviewing the content that's currently stored in Exchange, SharePoint, and OneDrive. Support for more locations is coming soon. [Learn more](#)

Search for specific categories or labels

All locations > SharePoint Online > redmondhq.contoso.com >

Sensitive labels	
General	345
Confidential	344
MnA Legal Top Secret	34

Manage label definition

<input checked="" type="checkbox"/>	 Name ↓	Sensitive info types
<input type="checkbox"/>	 DLP test policy	Credit Card Number +6 more
<input checked="" type="checkbox"/>	 Contoso Ignite trip pla...	Credit Card Number +3 more

Activity Explorer

Provides visibility into what content has been discovered, labeled, and where that content is

Activity Explorer

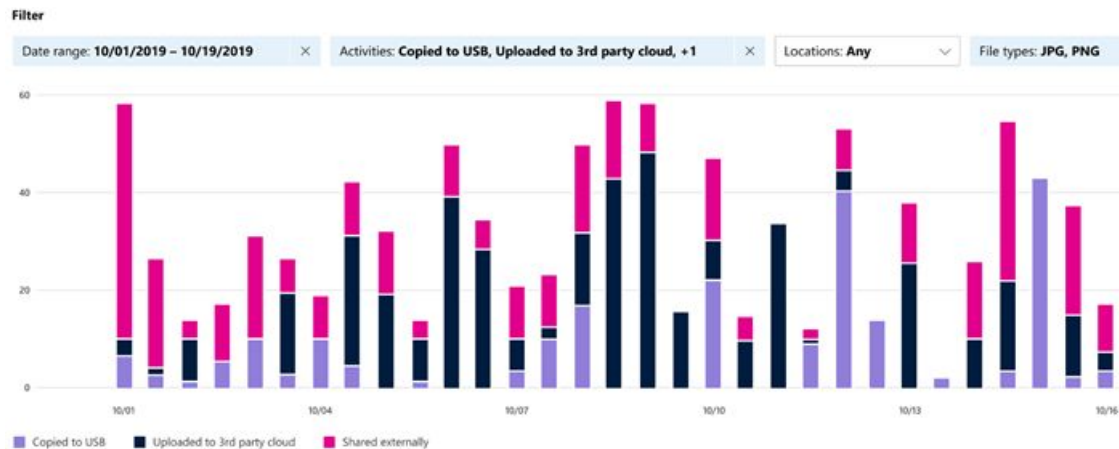
Some activity types that can be analyzed:

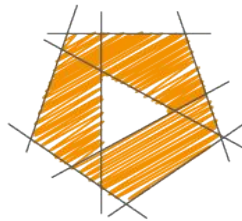
File copied to removable media

File copied to network share

Label applied

Label changed



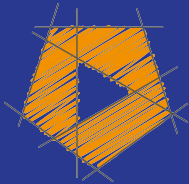


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe information protection and data lifecycle management capabilities of Microsoft Purview

- Describe data classification capabilities
- Describe the benefits of content and activity explorer
- Describe sensitivity labels
- Describe Data Loss Prevention (DLP)
- Describe Records Management
- Describe Retention Policies and Retention Labels

Sensitivity labels

Sensitivity labels

Customizable

Clear text

Persistent

The screenshot displays the Microsoft Outlook interface. At the top, there is a blue ribbon with tabs for 'Home', 'Organize', and 'Tools'. Below the ribbon is a toolbar with various icons for actions like 'New Email', 'Delete', 'Reply', 'Forward', 'Move', 'Junk', 'Rules', 'OneNote', 'Tags', 'Filter Email', 'Find a Contact', 'Address Book', 'Send & Receive', 'Store', and 'MyAnalytics'. The left sidebar shows the 'Inbox' folder selected, with other folders like 'Drafts', 'Archive', 'Sent', 'Groups', 'Trash', 'Junk', 'Clutter', and 'Conversation History' listed below. The main pane shows an email titled 'Marketing material' received on Wednesday, September 19, 2018, at 1:17 PM. The email content is partially visible, starting with 'Hi Kartik & Mas, Please publish the following mes...'. A yellow highlight is placed over a 'Public' sensitivity label in the email header, with a 'Learn more' button next to it. The right pane shows the 'Marketing material' header and the 'Public' label. Below the label, there is a section titled 'Sensitivity Labels' with a brief explanation and a numbered list of steps: 1. In the Home tab, select Sensitivity. 2. Choose the sensitivity label that applies to your document or email.

Try the Preview Search

Home Organize Tools

New Email New Items Delete Archive Reply Reply All Forward Move Junk Rules OneNote Tags Filter Email Find a Contact Address Book Send & Receive Store MyAnalytics

Focused Other By: Conversations

Today

Marketing material 1:17 PM

Hi Kartik & Mas, Please publish the following mes...

Public [Learn more](#)

Please publish the following message to our public blog:

Sensitivity Labels
You can apply a sensitivity label to your documents and emails to keep them compliant with your organization's information protection policies.

1. In the **Home** tab, select **Sensitivity**.
2. Choose the sensitivity label that applies to your document or email.

Smart Folders

<https://t.me/learningnets>

AutoSave OFF FinancialReport Search Sheet

Home Insert Draw Page Layout Formulas Data Review Tell me what you want to do Share

Paste Calibri (Body) 12 A A Alignment Number Conditional Formatting Format as Table Cell Styles Cells Editing

D12 fx 80083

	A	B	C	D	E	F
1	Financial Highlights					
2	Year Ended June 30	2017	2016	2015		
3	Revenue	\$ 89,950.00	\$ 85,320.00	\$ 93,580.00		
4	Gross margin	\$ 55,689.00	\$ 52,540.00	\$ 60,542.00		
5	Operating income	\$ 22,326.00	\$ 20,182.00	\$ 18,161.00		
6	Net income	\$ 21,204.00	\$ 16,798.00	\$ 12,193.00		
7	Diluted earnings per share	\$ 2.71	\$ 2.10	\$ 1.48		
8	Cash dividends declared per share	\$ 1.56	\$ 1.44	\$ 1.24		
9	Cash, cash equivalents, and short-term investments	\$ 132,981.00	\$ 113,240.00	\$ 96,526.00		
10	Total assets	\$ 241,086.00	\$ 193,468.00	\$ 174,303.00		
11	Long-term obligations	\$ 104,165.00	\$ 62,114.00	\$ 44,574.00		
12	Stockholders' equity	\$ 72,394.00	\$ 71,997.00	\$ 80,083.00		
13						
14						

Public
General
Confidential
✓ Highly Confidential
Learn More...

Sheet1 +

Ready Highly Confidential 120%

Sensitivity label usage

Encrypt email or both email and documents

Mark content

Apply a label automatically

Protect content in containers (sites and groups)

Extend sensitivity labels (third-party apps and services)

Classify content without protection settings

Labels need to be
published to make
them available to
people and services

Sensitivity label policies

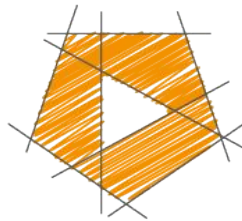
Choose the users and groups that can see labels

Apply a default label to all new emails and documents

Require justifications for label changes

Require users to apply a label (mandatory labeling)

Link users to custom help pages

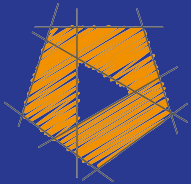


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe information protection and data lifecycle management capabilities of Microsoft Purview

- Describe data classification capabilities
- Describe the benefits of content and activity explorer
- Describe sensitivity labels
- Describe Data Loss Prevention (DLP)
- Describe Records Management
- Describe Retention Policies and Retention Labels

Retention policies and labels

Ensuring content is kept only for a required time, and then permanently deleted

Works with:

Sharepoint, OneDrive, Teams, Yammer and Exchange

The top right corner of the slide features a decorative arrangement of overlapping triangles in various shades of pink and magenta, creating a modern, abstract design.

Comply proactively
with industry
regulations and
internal policies

Reduce risk when
there's litigation or
a security breach

Ensure users work
only with content
that's current and
relevant to them

Retention labels

Applied at item level (file, doc, email)

Only 1 label supported

Labels travel with content if moved to a different location within your M365 tenant

Applied manually/automatically

Support disposition review: review content before permanent deletion

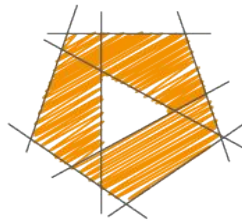
Retention policies

Applied at site or mailbox level

Applied to multiple locations, specific locations or users

Items inherit the retention settings from their container

If an item is moved, the retention setting doesn't travel to new location

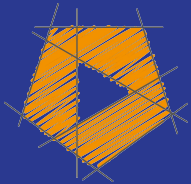


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe information protection and data lifecycle management capabilities of Microsoft Purview

- Describe data classification capabilities
- Describe the benefits of content and activity explorer
- Describe sensitivity labels
- Describe Data Loss Prevention (DLP)
- Describe Records Management
- Describe Retention Policies and Retention Labels

Records Management

Used to look after your companies legal obligations and helps to demonstrate compliance with regulations

Disposition of items that are:

No longer required to be kept, have no value or no business purpose

Three Types of Retention:

- Retention Label
- Record (locked / unlocked)
- Regulatory Record

Retention labels
enable admins to
mark items as
records

Action	Retention label	Record - locked	Record - unlocked	Regulatory record
Edit contents	Allowed	Blocked	Allowed	Blocked
Edit properties, including rename	Allowed	Allowed	Allowed	Blocked
Delete	Allowed ¹	Blocked	Blocked	Blocked
Copy	Allowed	Allowed	Allowed	Allowed
Move within container ²	Allowed	Allowed	Allowed	Allowed
Move across containers ²	Allowed	Allowed if never unlocked	Blocked	Blocked

Action	Retention label	Record - locked	Record - unlocked	Regulatory record
Open/Read	Allowed	Allowed	Allowed	Allowed
Change label	Allowed	Allowed - container admin only	Allowed - container admin only	Blocked
Remove label	Allowed	Allowed - container admin only	Allowed - container admin only	Blocked

During the retention period

Retain items even if users delete

Mark items as a record

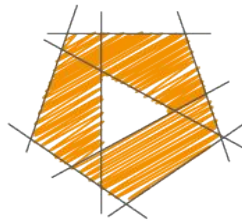
Users won't be able to edit or delete emails, and only certain users will be able to change or remove the label. They won't be able to delete SharePoint or OneDrive files, but other actions are blocked or allowed based on whether the item's record status is locked or unlocked. [Learn more](#)

Mark items as a regulatory record

At the end of the retention period

Delete items automatically

We'll delete items from where they're currently stored.

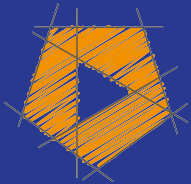


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe information protection and data lifecycle management capabilities of Microsoft Purview

- Describe data classification capabilities
- Describe the benefits of content and activity explorer
- Describe sensitivity labels
- Describe Data Loss Prevention (DLP)
- Describe Records Management
- Describe Retention Policies and Retention Labels

Data Loss

Prevention: Protect
sensitive information
and prevent its
inadvertent
disclosure

Data Loss Prevention (DLP)

Identify, monitor, and automatically protect sensitive information across M365:
OneDrive for Business, SharePoint Online, Microsoft Teams, Exchange Online

Help users learn how compliance works

View DLP reports

Data Loss Prevention (DLP)

DLP policies protect information by identifying and automatically protecting sensitive data, eg.:

Credit card number

Personal Information

Data loss prevention policy

Locations
to apply
the policy

Rule 1

Conditions

Actions

Rule 2

Conditions

Actions

Rule n...

Conditions

Actions

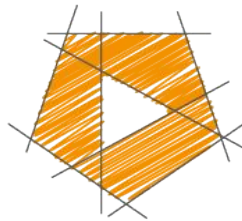
Endpoint Data Loss Prevention

To audit and manage activities that users complete on sensitive content on Windows 10 devices, eg.:

Creating an item

Renaming an item

Copying items to removable media

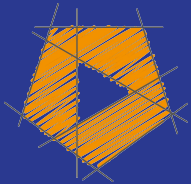


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals


Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe insider risk capabilities in Microsoft Purview

- Describe Insider Risk Management
- Describe communication compliance
- Describe information barriers



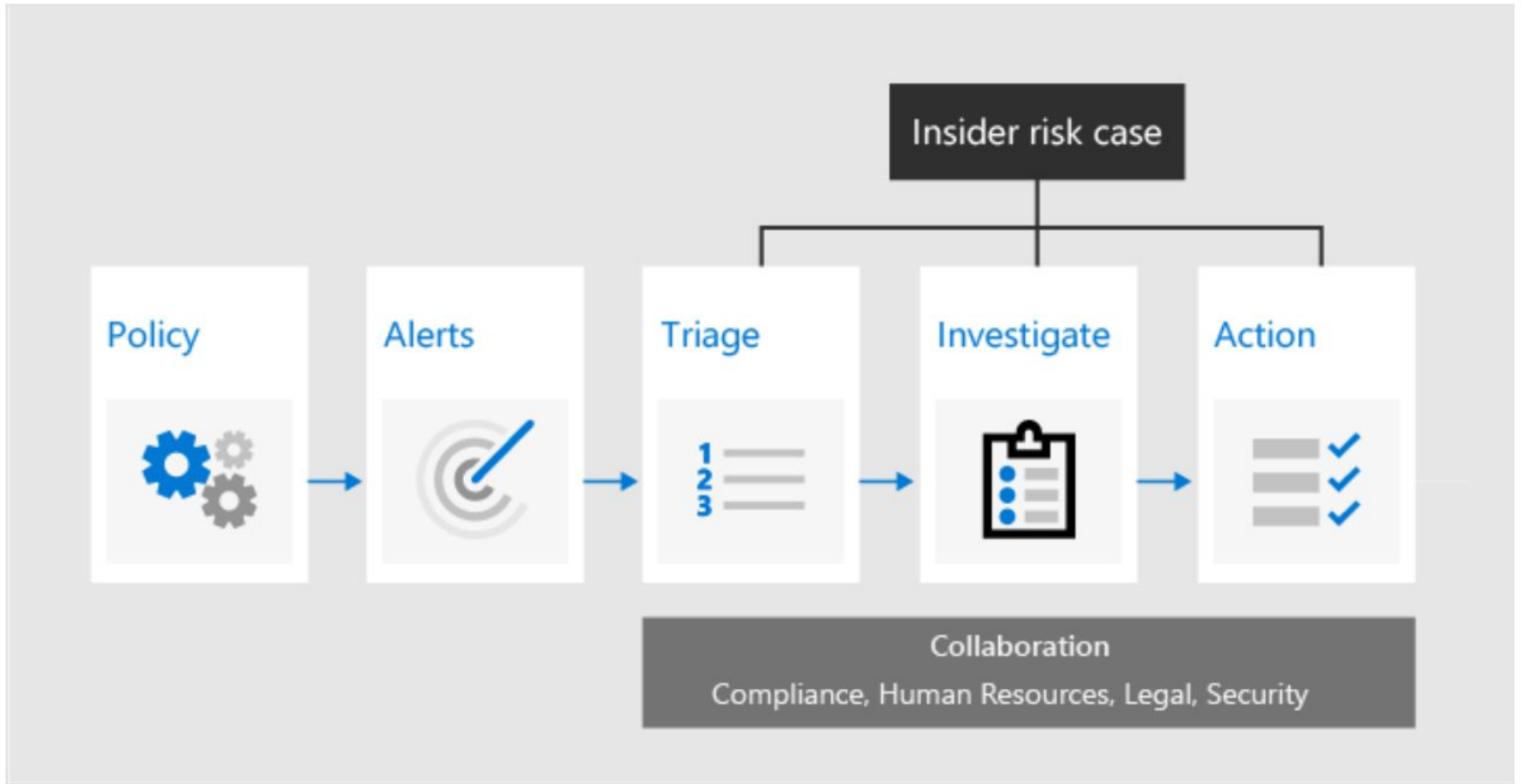
Insider Risk
Management is
used to minimize
internal risks

Leaks of sensitive data and data spillage

Confidentiality violations

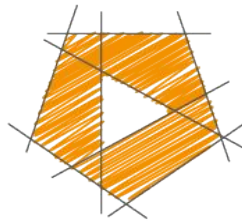
Intellectual property (IP) theft





Four Insider Risk solutions in M365:

- Communication compliance
- Insider risk management
- Information barriers
- Privileged access management

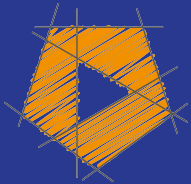


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe insider risk capabilities in Microsoft Purview

- Describe Insider Risk Management
- Describe communication compliance
- Describe information barriers

Communication Compliance

Minimize communication risks by detecting, capturing, and take remediation actions for inappropriate messages

- Microsoft Teams
- Exchange Online
- Yammer
- Third-party communications

Monitoring email and chat for compliance risks

Inappropriate Communications

Profanity

Threats

Harassment

Sharing sensitive information inside and outside your organization



Communication compliance



Communication compliance settings



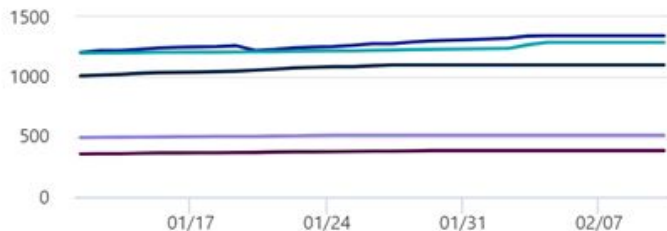
Show in navigation

Policies Alerts Reports

Get quick insights into how your policies are performing, including recent activity, escalations, and user matches. Or view detailed reports to drill down more and export results for further analysis. [Learn more](#)

Recent policy matches

Last 30 days, updated 3:38 PM today



- Custom Test Policy OL
- Top secret project
- Insiders
- Privacy breach
- Teams msgs only

Resolved items by policy

Last 30 days, updated 3:38 PM today



- Custom Test Policy OL
- Offensive messages
- Insiders
- Top secret project
- Teams msgs only





Configure



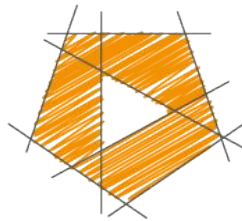
Investigate



Remediate



Monitor

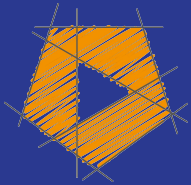


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe insider risk capabilities in Microsoft Purview

- Describe Insider Risk Management
- Describe communication compliance
- Describe information barriers

Information barriers
restrict
communications
among specific
groups of users

I.e. User in the day
trader group should
not communicate
or share files with
the marketing team

Information barriers

Only support two-way restrictions

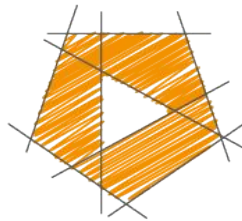
Can prevent the following in Teams:

Searching for a user

Adding a member to a team

Starting a chat session with someone

And more..

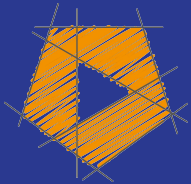


GetCloudSkills
.com

<https://t.me/learningnets>

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2024 Scott Duffy, getcloudskills.com... get the course for these slides at:
<https://t.me/learningnets>
<http://sjd.ca/sc900>

Describe resource governance capabilities in Azure

- Describe Azure Policy
- Describe Azure Blueprints
- Describe the Microsoft Purview unified data governance solution

Prevent resources
from being
accidentally deleted
or changed

Azure Resource Locks

Apply a lock at a parent scope, all resources within that scope inherit that lock

Apply only to operations that happen in the management plane

Changes to the actual resource are restricted, but resource operations aren't restricted

CanNotDelete
ReadOnly

A way to define a repeatable set of Azure resources

Azure Blueprints

Always in line with the organization's compliance requirements

Provision Azure resources across several subscriptions simultaneously

Blueprint objects are replicated to multiple Azure regions

Azure Blueprints

Declarative way to orchestrate the deployment of various resource templates and artifacts, including:

- Role Assignments
- Policy Assignments
- ARM templates
- Resource Groups

Azure Policy is
designed to help
enforce standards
and assess
compliance

Azure Policy
evaluates all
resources in Azure
and Arc enabled
resources

Azure Policy uses cases

Implementing governance for resource consistency

Regulatory compliance

Security, cost, and management

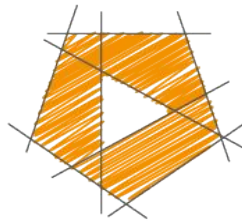
Azure Policy responses

Deny a change to a resource

Log changes to a resource

Alter a resource before or after a change

Deploy related compliant resources



GetCloudSkills
.com

<https://t.me/learningnets>



Thank you!