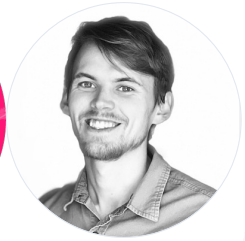
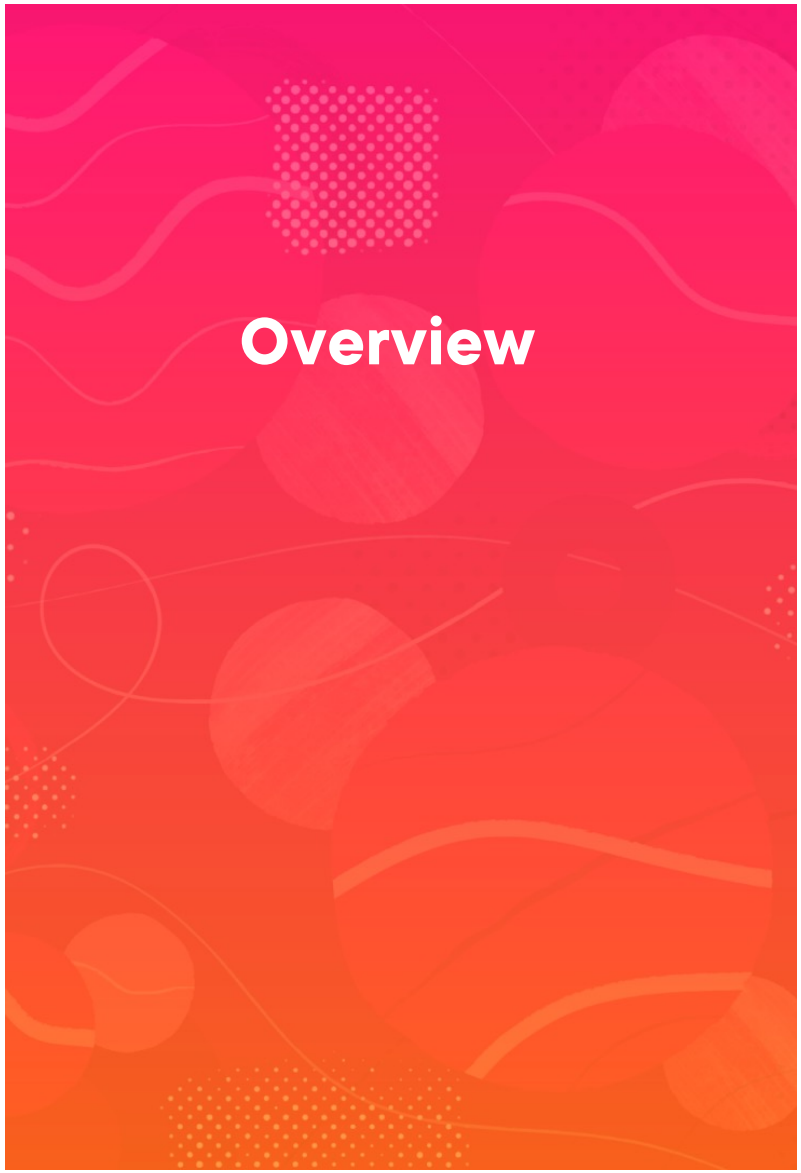
Troubleshooting Security Issues in the Cloud



Jacob Petrie
Network Administrator

@pwsh1996



Securing Software in the Cloud

Discovering Insecure Authentication

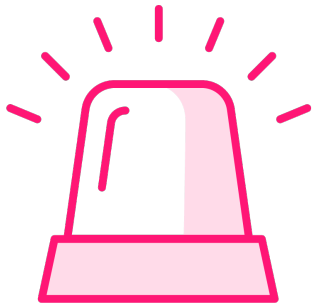
Understanding Authorization Issues

Dealing with Deprecated Cipher Suites

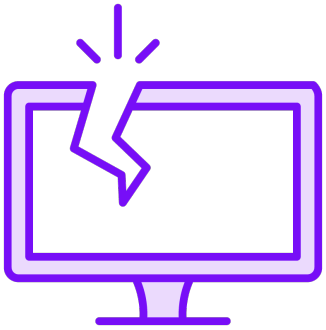
CompTIA Cloud+

Given a scenario, troubleshoot security issues.

When These Issues Manifest Themselves



Security incidents

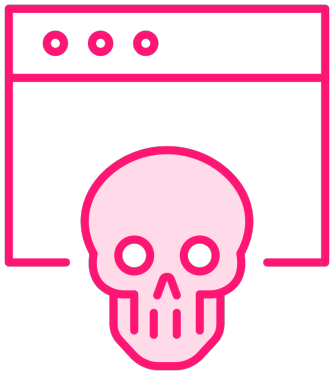


Services going down

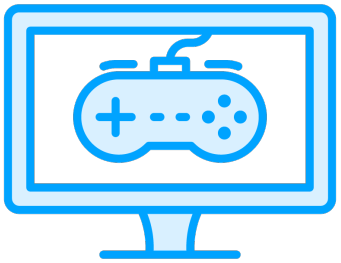
Loss of user data

Securing Software in the Cloud

Security Issues with Software



Vulnerable software
Known CVEs and other security issues that hackers can exploit



Unauthorized software
Admins installing unauthorized software like games and crypto miners

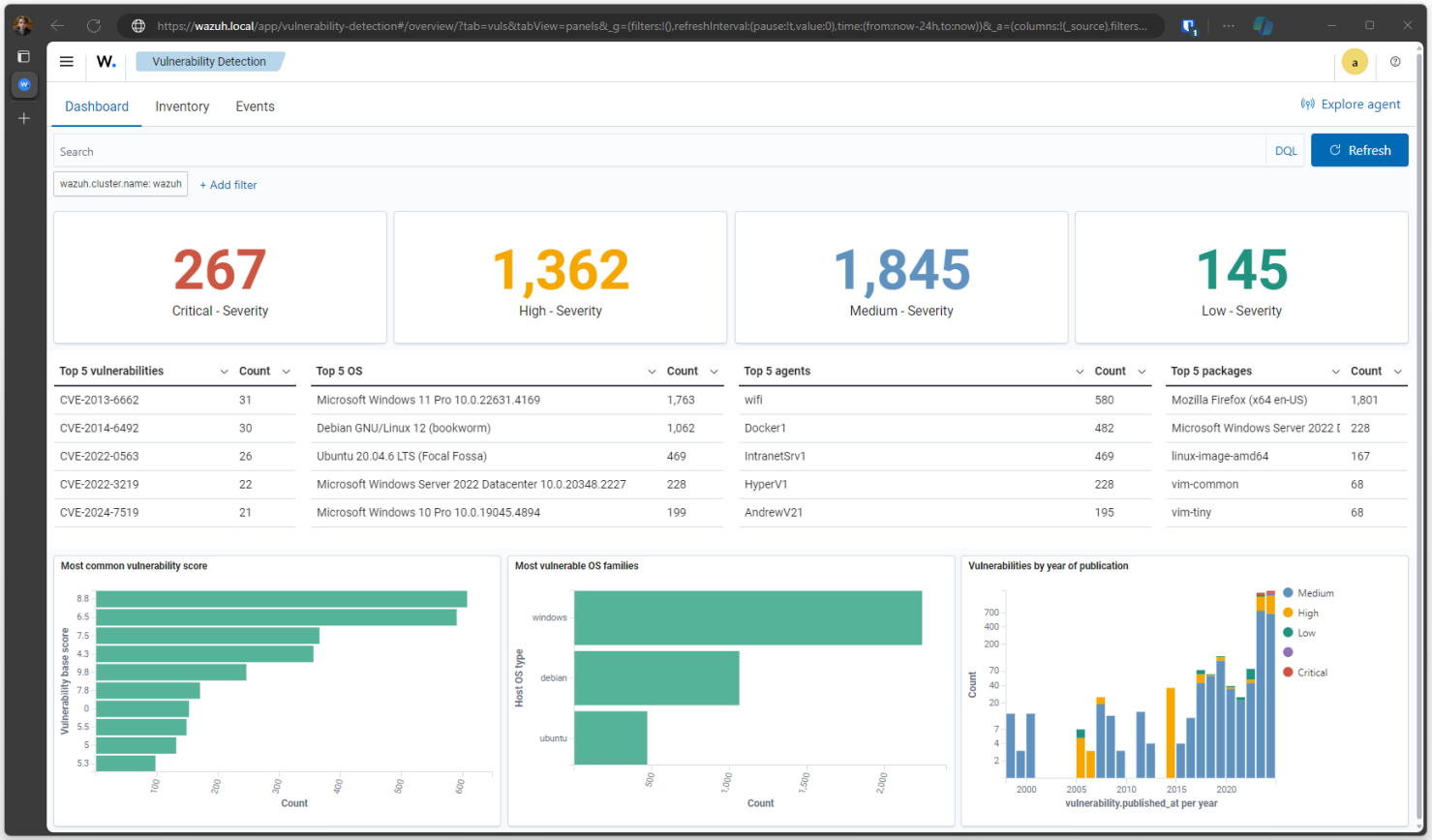
Problems Caused by Insecure Software

Data loss – SQL injection

Account compromise – session hijacking

Backdoored – remote code execution

Vulnerability Scanning



Software Types

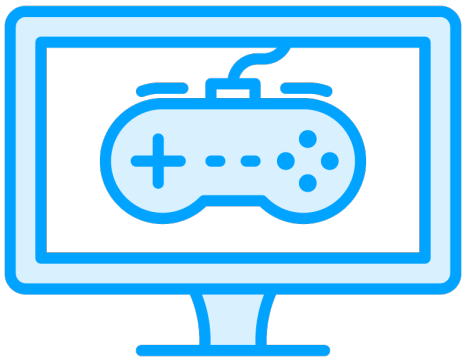
Authorized

Software that has a legitimate business use like SSH or Microsoft Exchange

Unauthorized

Software that has a no business use case, either for personal use or to make their job easier

Reducing Unauthorized Software



Whitelisting software – specifies what can run on the system

Blacklisting software – specifies what can't run on the system

Auditing software using asset management solutions to check for unwanted apps

Troubleshooting Insecure Software

Vulnerability Scanners

Scan your environment for software that is vulnerable

Patch Management

Helps ensure that security patches are applied

Minimal Setups

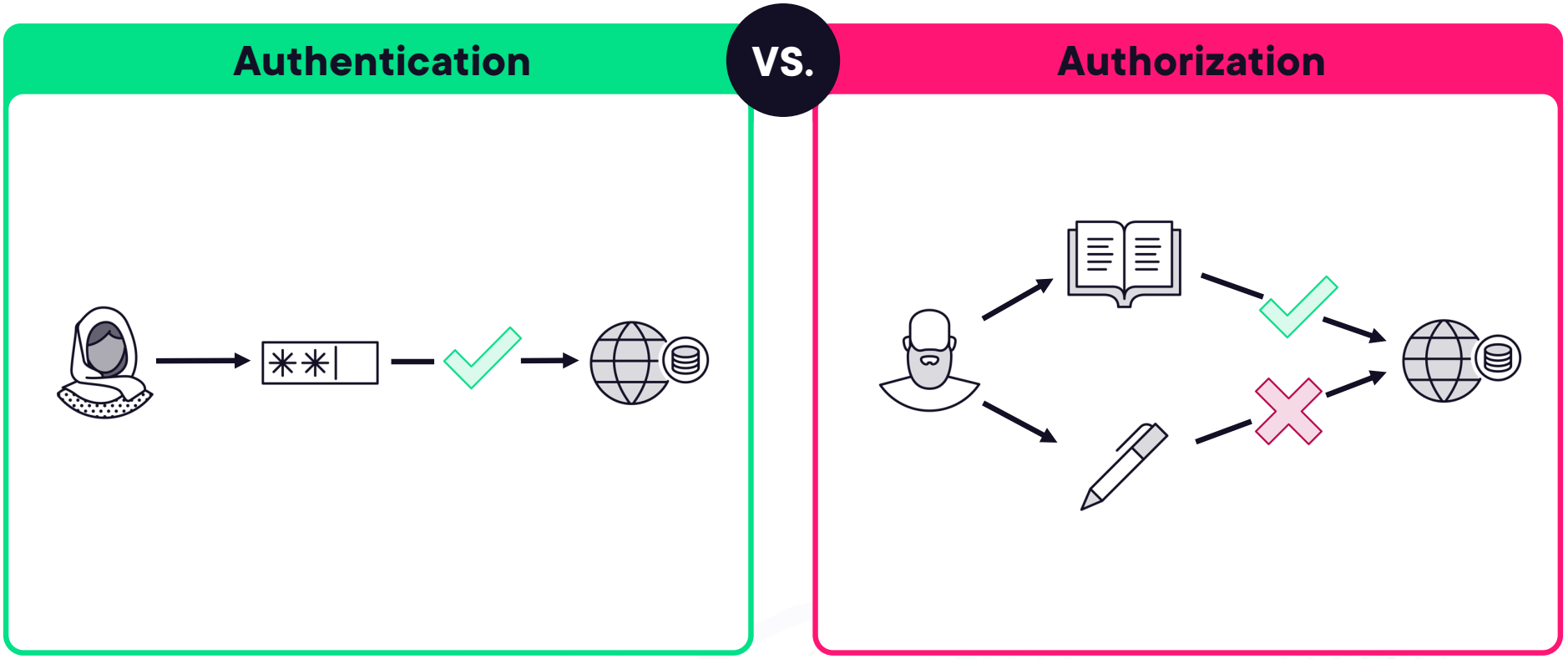
Ensure that unnecessary software isn't on the system

Product Security Notifications

Emails from vendors about security issues and patches

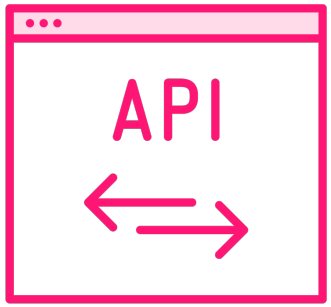
Discovering Insecure Authentication

Authentication vs. Authorization

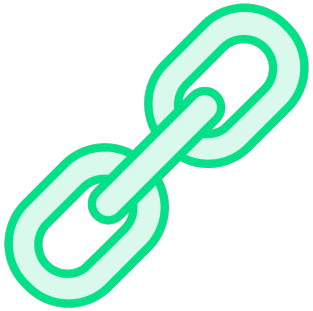


Authentication Issues

Multi Factor Authentication (MFA)



API Key Expiration



Single Sign On (SSO)

Credential Brute Forcing

Multi Factor Authentication (MFA)

Factors

- Something you know (password, pin)
- Something you have (phone)
- Something you are (fingerprint, face)

Most cloud providers are forcing admins to use MFA

If you are using a standard admin account as a service account, you may be unable to connect

You should switch to an actual service account using API keys

API Key Expiration

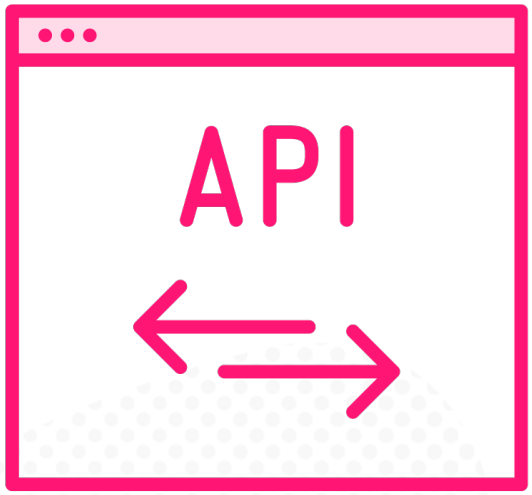
API keys should be rotated frequently

This prevents leaked keys from staying valid for an extended period of time

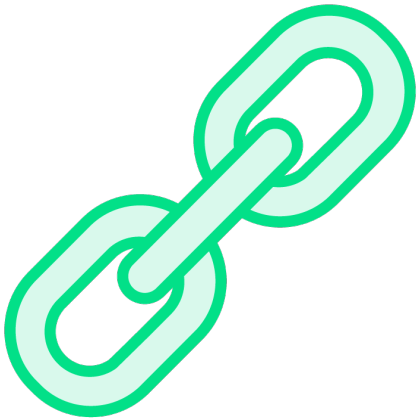
Avoid a “set it and forget it” mindset when it comes to API keys

Keys that expire and aren’t automatically rotated can cause connectivity issues

Read the HTTP headers, if you get “403 Forbidden” your key may have expired



Single Sign On (SSO)



SSO allows for the same credential provider to be used to sign into many cloud services

You can lock out or reset the account on all platforms with a single action

When the connector that syncs the account information breaks it can cause authentication issues

Check firewall rules to make sure you don't block this traffic when hardening your systems

Credential Brute Forcing

Cloud systems are often publicly accessible

Easy targets for hackers who try to brute force or use password spraying attacks

Check audit logs for failed login attempts

Security Orchestration, Automation and Response (SOAR) tools can be used to take actions like blocking an IP after failed logins

Leaked Credentials

Hackers will sell your credentials on the dark web

Use a service to find if your credentials have been in a leak

- HaveIBeenPwned.com
- Cavalier by Hudson Rock

API access can be used to programmatically find and notify you of leaks

Tips for Catching Leaked Credentials

Audit Account sign-ins

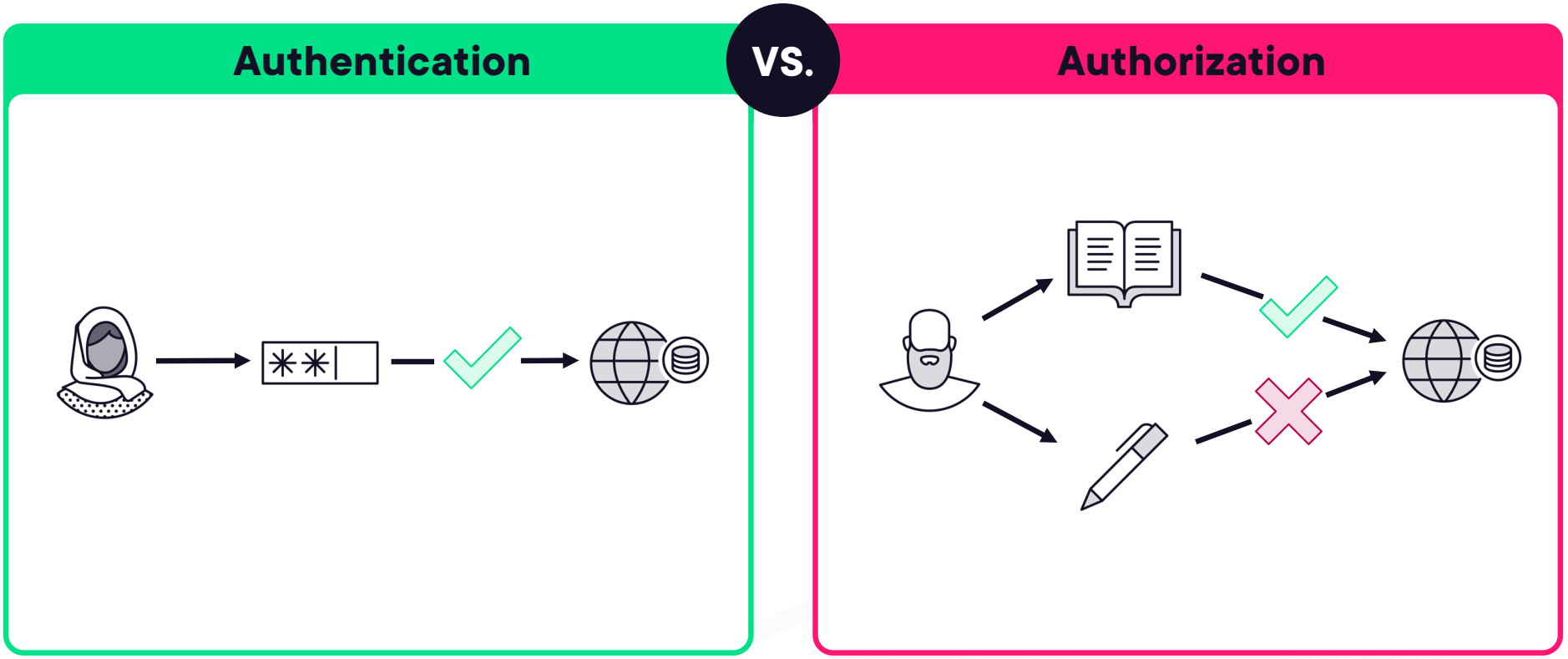
Look for unusual sign-in locations from service accounts and admins

Check Source Code

Use tools like TruffleHog to find credentials in code and config files uploaded to your repositories

Understanding Authorization Issues

Authentication vs. Authorization



Authorization Issues

Unauthorized Access
When someone is given more access than they should have, and access unauthorized resources

Privilege Escalation
Using an exploit in a system to gain more access than they were originally given

Unauthorized Access

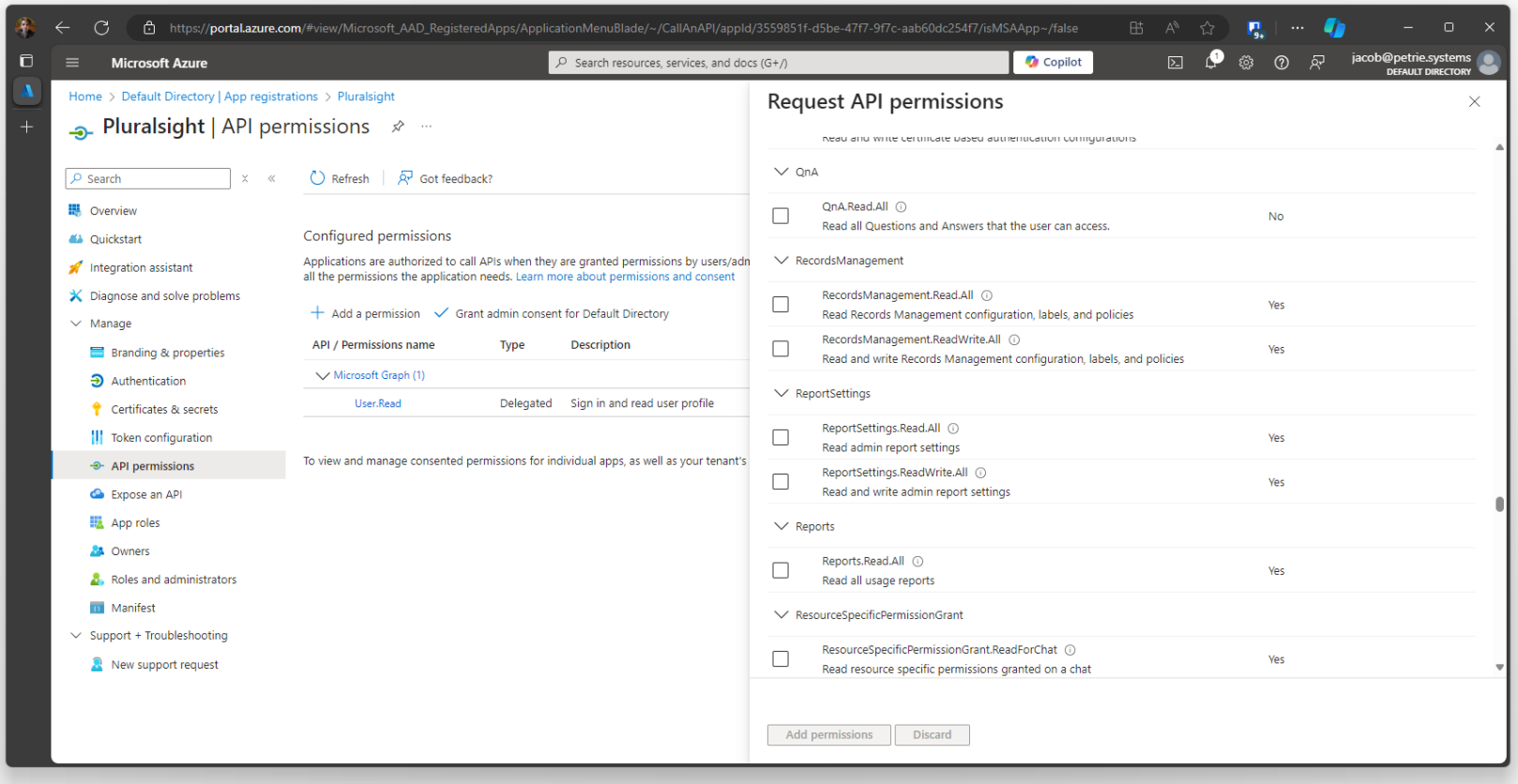
When people are in a hurry and don't take time to find the correct permissions

This can lead to security problems

- Insider threat
- Accidental data deletion
- High-value target for hackers

Always try to implement least privilege

API Permissions

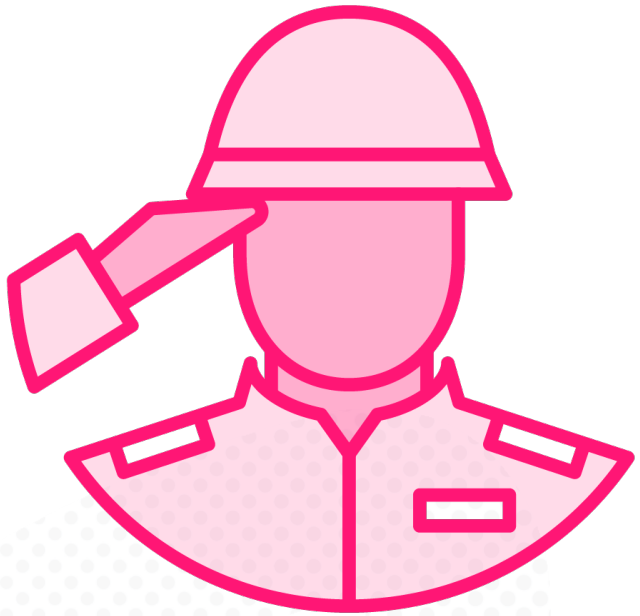


Privilege Escalation

Exploiting a system to gain higher privileges

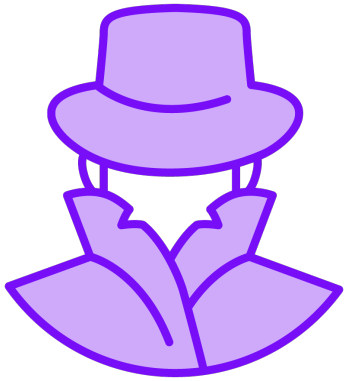
This can happen from either a vulnerability or a lack of understanding what a permission does

Read the documentation on the access and roles you assign to users and APIs



Real World Consequences

Unintended Damage
As admins or users accidentally make changes they shouldn't



Compromise to Systems
Hackers abuse the system to gain access to sensitive information

Minimizing Unauthorized Access

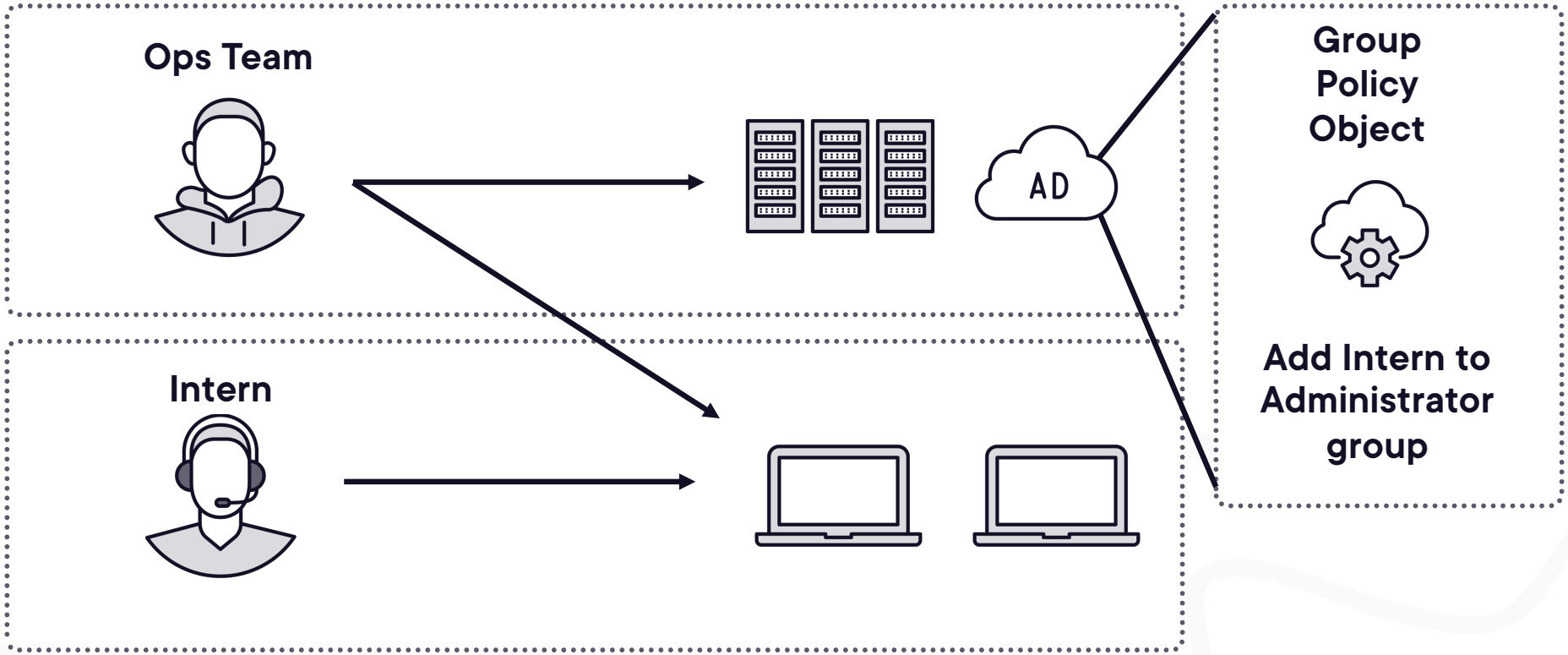
Enable audit logs

Security information and event management (SIEM) to centrally gather and alert on audit logs

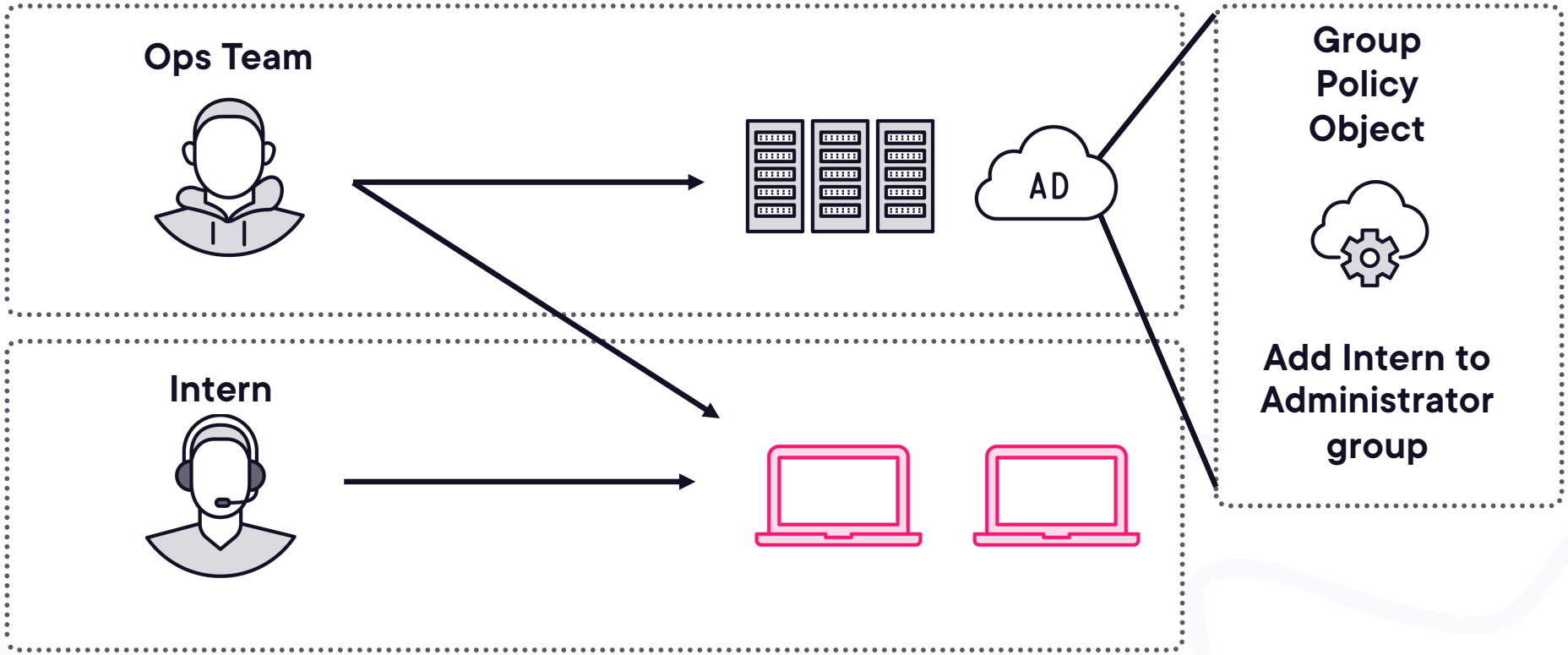
Solutions like Darktrace use AI to detect anomalies in user behavior

Implement least privilege where possible

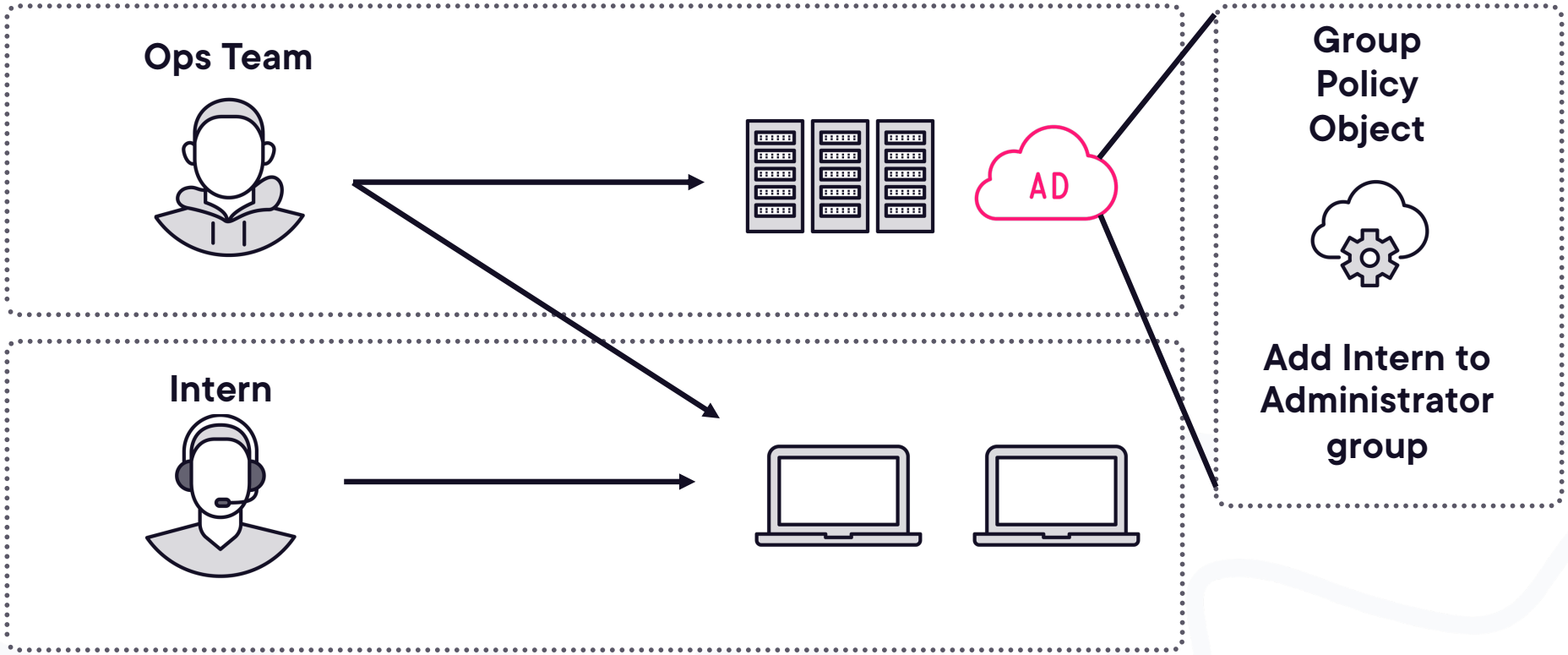
Story Time



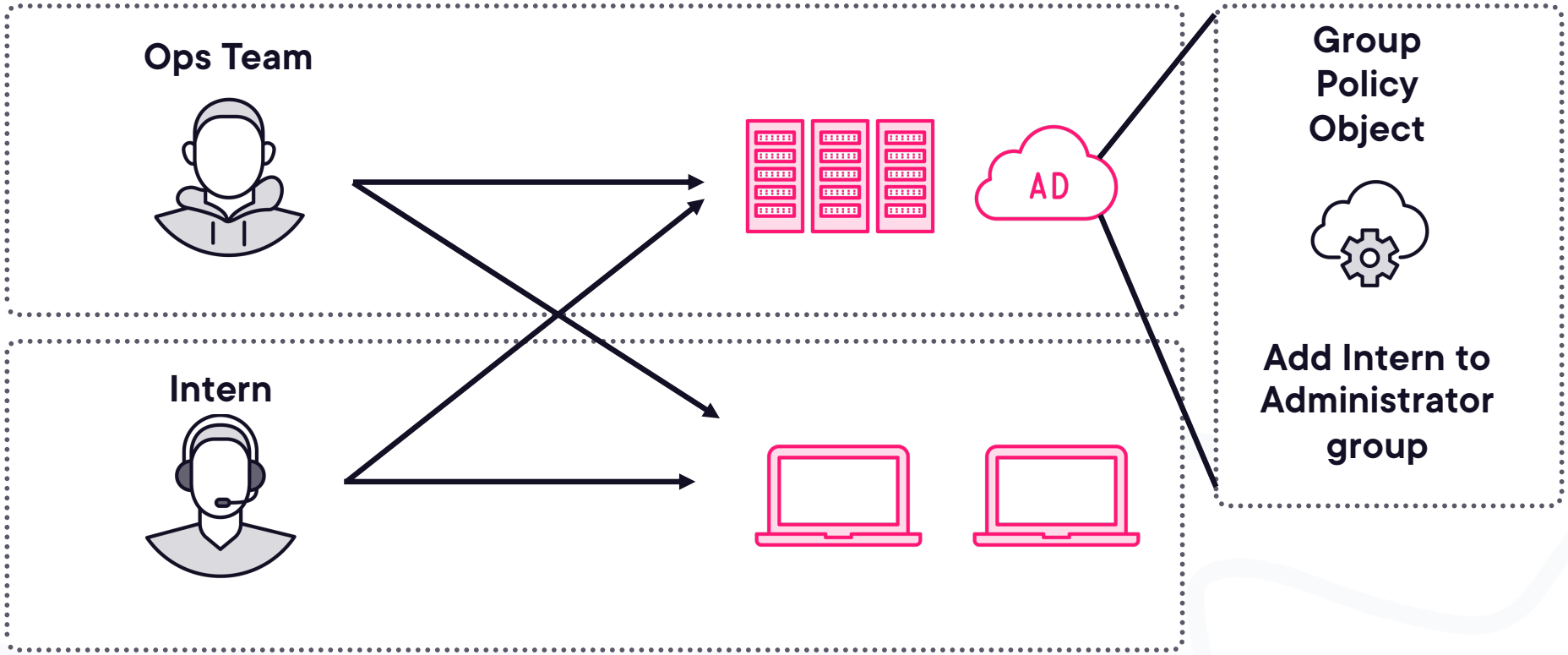
Story Time



Story Time



Story Time



Dealing with Deprecated Cipher Suites

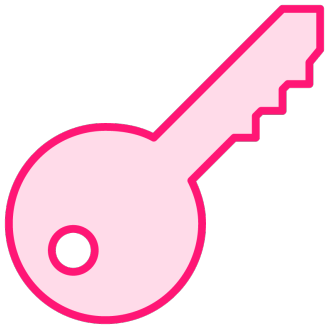
Cipher Suite

A cipher suite is a set of algorithms that help secure a network connection. Suites typically use Transport Layer Security (TLS) or it's deprecated predecessor Secure Socket Layer (SSL). The set of algorithms that cipher suites usually contain include: a key exchange algorithm, a bulk encryption algorithm, and a message authentication code (MAC) algorithm.

---

https://en.wikipedia.org/wiki/Cipher_suite

Examples of Algorithms in a Cipher Suite

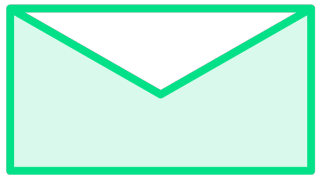


Key Exchange

Diffie-Hellman

Encryption

AES
3DES



MAC

HMAC
CMAC

Deprecation in Cipher Suites

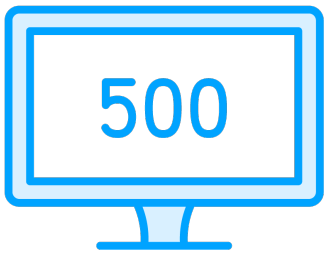
Each algorithm generally has different levels with weaker ones getting deprecated first

- Diffie-Hellman group 2 (1024 bit) – Not Secure
- Diffie-Hellman group 14 (2048 bit) - Secure

Read best practice documents from organizations like NIST

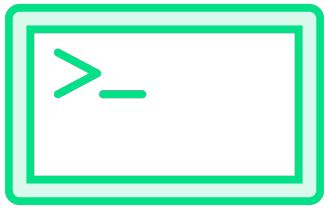
Follow best practice when choosing cipher suites even if the cloud provider allows for weaker options

Issues That Might Occur



Users unable to connect

Site-to-Site VPN stop connecting



Unable to connect to SSH using weak key pairs

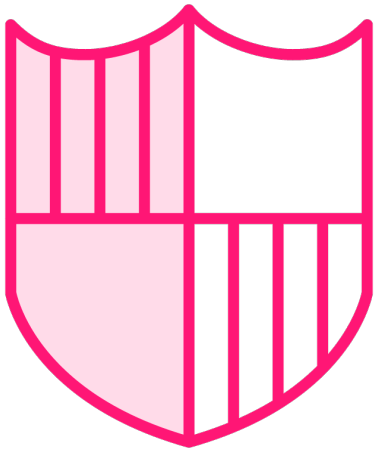
Tips for Troubleshooting

Enable alerts in your cloud providers console for technology you use

Don’t use minimum viable cipher suites when deploying new solutions

Stay up to date on security news and feature releases and deprecations

A Note on Hardening Systems



Hardening systems may produce similar symptoms to deprecated cipher suites

Hardening guides usually recommend disabling weak cipher suites

- Security Technical Implementation Guide (STIG)
- Center for Information Security (CIS) benchmarks

Beware just auto enabling a hardening tool on a production system

Summary

Securing your software

- Vulnerability Scans
- Application Whitelisting

Finding your leaked credentials

Handling Unauthorized access and privilege escalation

Dealing with deprecated cipher suites

More Information

CompTIA Cloud+ (CV0-004): Security

Michael Brown

Thank you for your attention

@pwsh1996