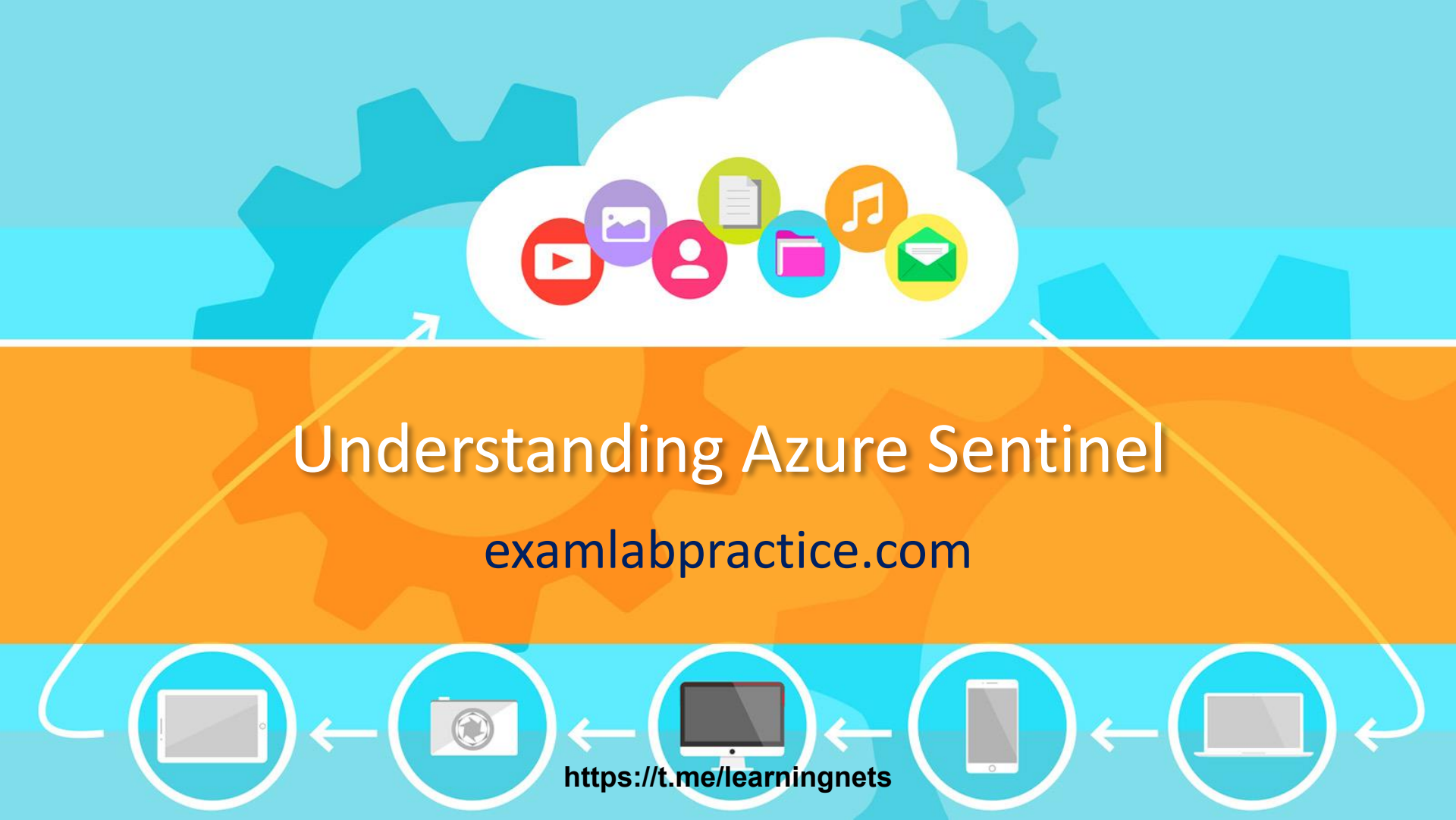


Understanding Azure Sentinel

examlabpractice.com

What is Azure Sentinel?

Azure Sentinel is a scalable, cloud based, security information event management (SIEM) and security orchestration automated response (SOAR) product. Sentinel delivers intelligent security analytics and threat intelligence solution, providing a centralized point for alert detection, threat visibility, proactive hunting, and threat response.

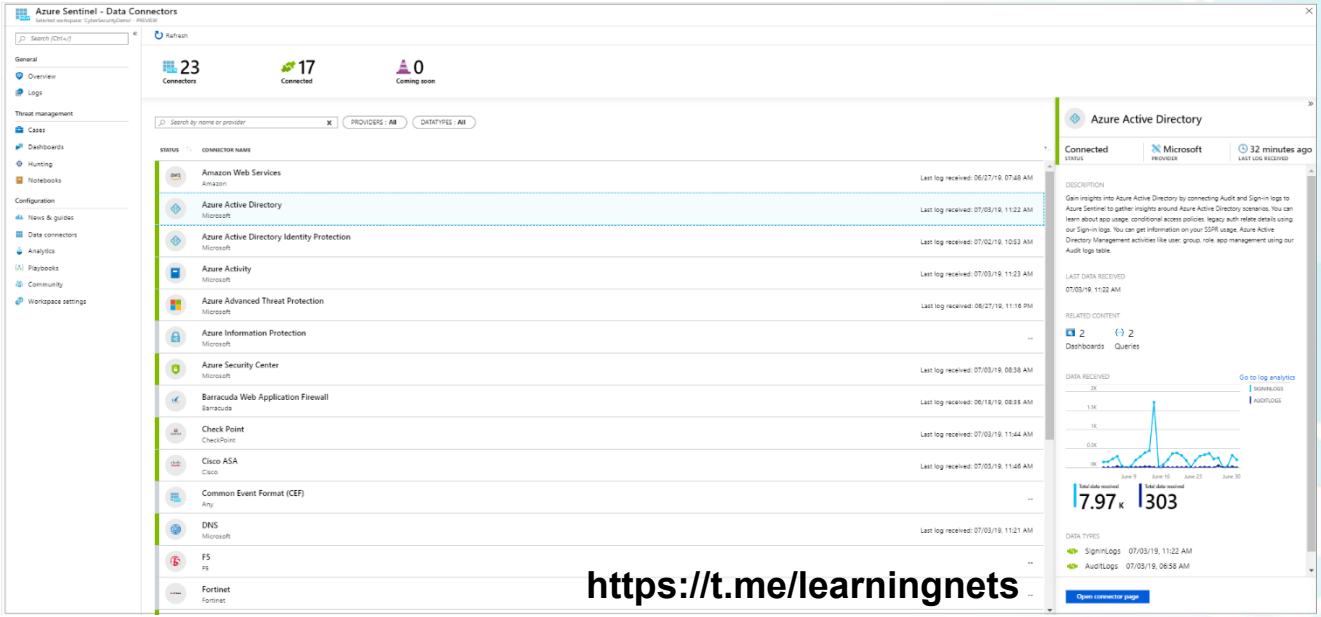
Purposes of Sentinel

Azure Sentinel is your eye in the sky for viewing across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution timeframes.

- Data collection at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in the cloud.
- Find previously undetected threats, and minimize false positives using Microsoft's analytics and threat intelligence.
- Investigate threats with artificial intelligence, and hunt for suspicious activities, tapping into years of cyber security work at Microsoft.
- Respond to incidents rapidly with built-in orchestration and automation of common tasks

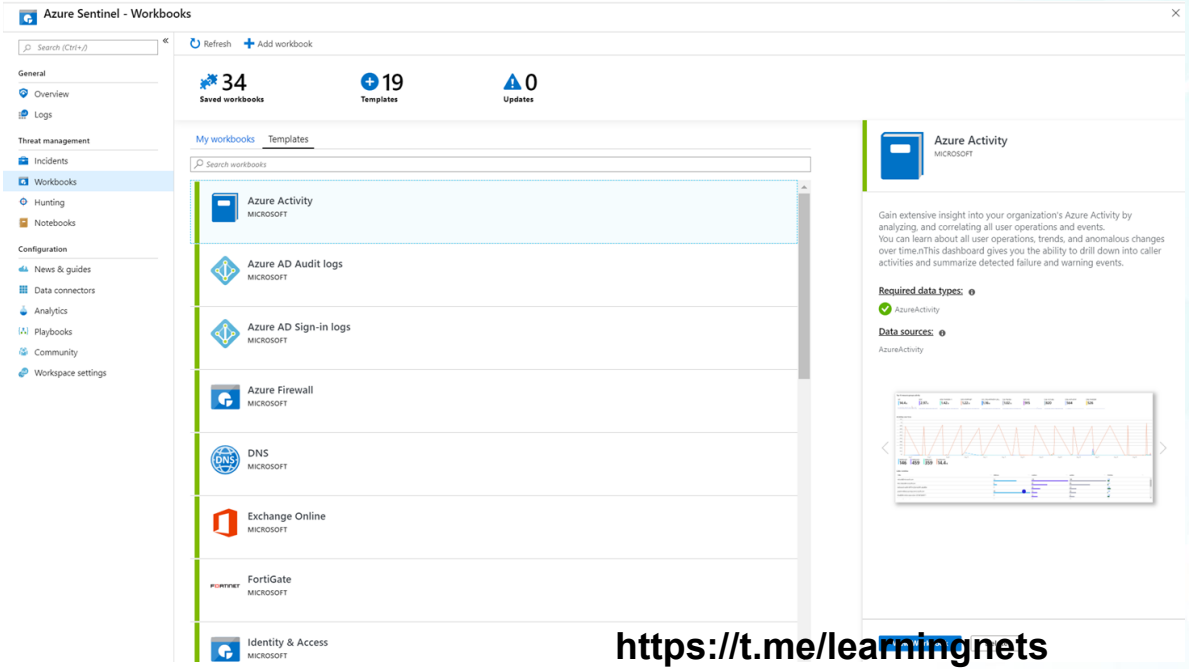
Connect With All Of Your Data

Azure Sentinel comes with a number of connectors for Microsoft solutions, available out of the box and providing real-time integration, including Microsoft Threat Protection solutions, and Microsoft 365 sources, including Office 365, Azure AD, Azure ATP, and Microsoft Cloud App Security, and more.



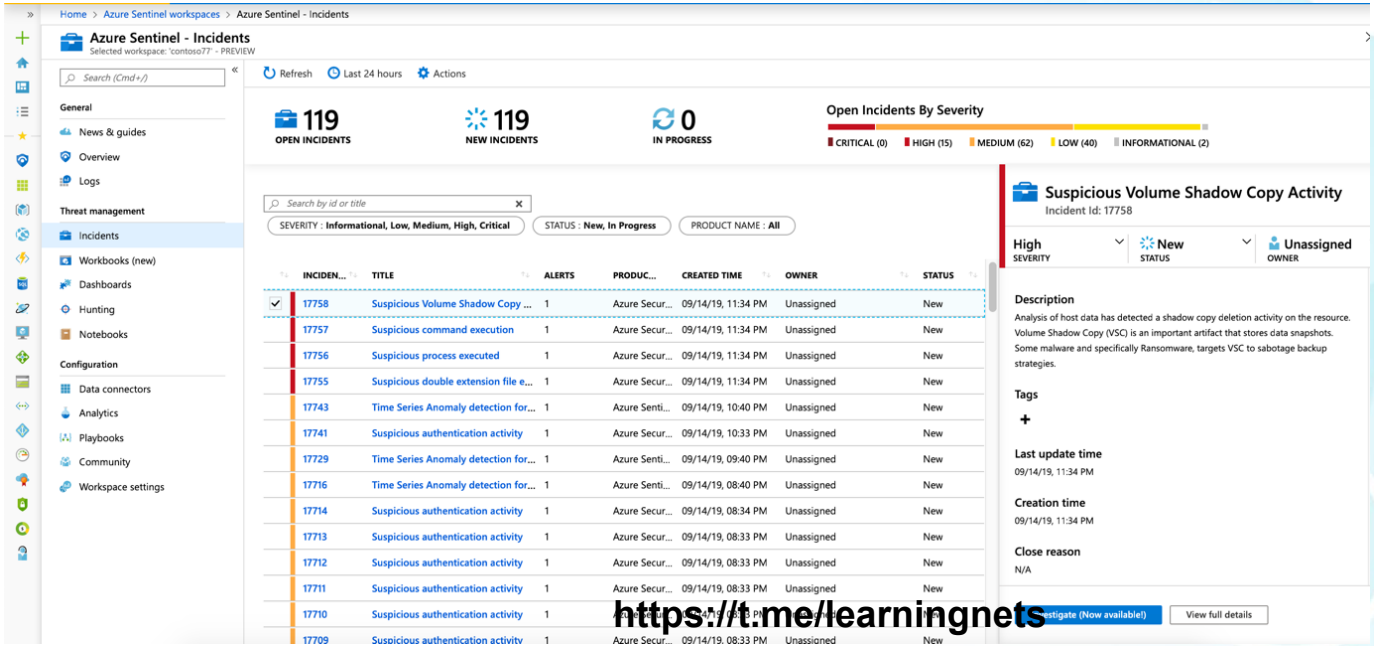
Workbooks

Azure Sentinel, you can monitor the data using the Azure Sentinel integration with Azure Monitor Workbooks, which provides versatility in creating custom workbooks.



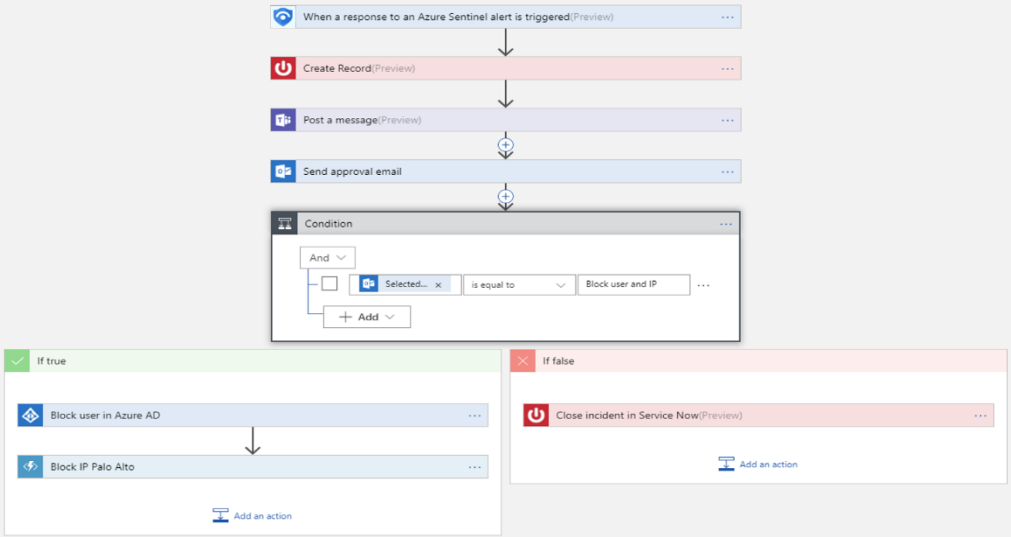
Analytics

To help you reduce noise and minimize the number of alerts you have to review and investigate, Azure Sentinel uses analytics to correlate alerts into incidents. Incidents are groups of related alerts that together create an actionable possible-threat that you can investigate and resolve.



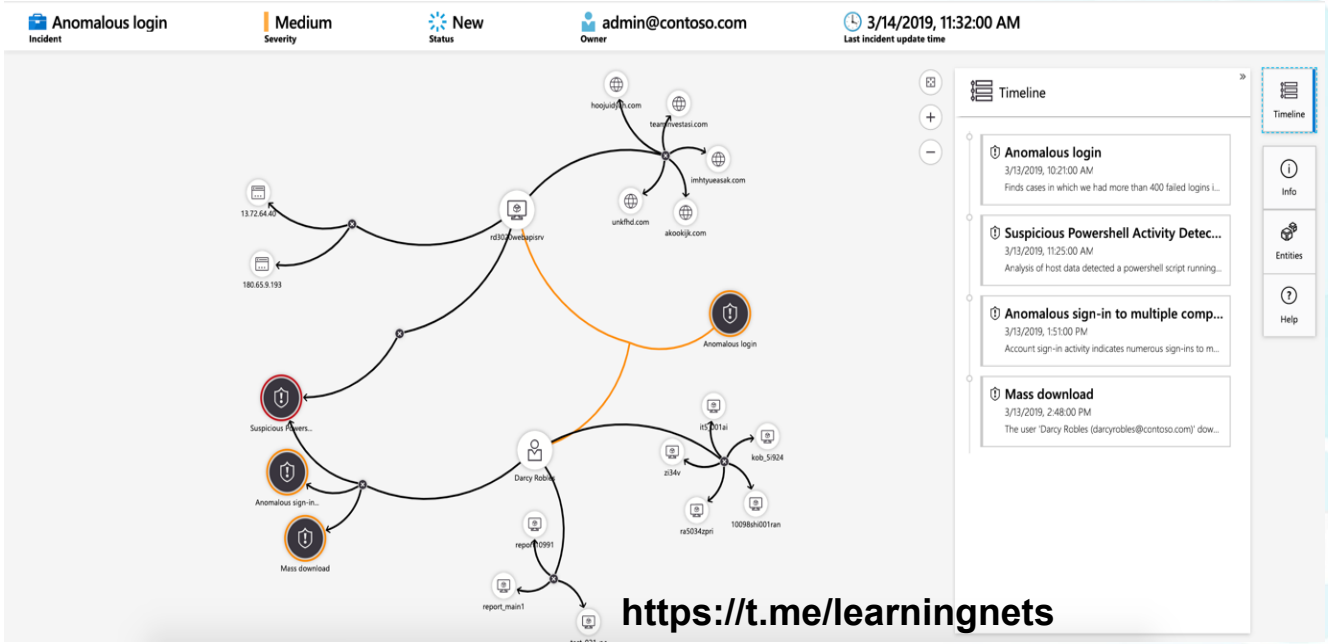
Security Automation & Orchestration

Automate your common tasks and simplify security orchestration with playbooks that integrate with Azure services as well as your existing tools. Built on the foundation of Azure Logic Apps, Azure Sentinel's automation and orchestration solution provides a highly-extensible architecture that enables scalable automation as new technologies and threats emerge.



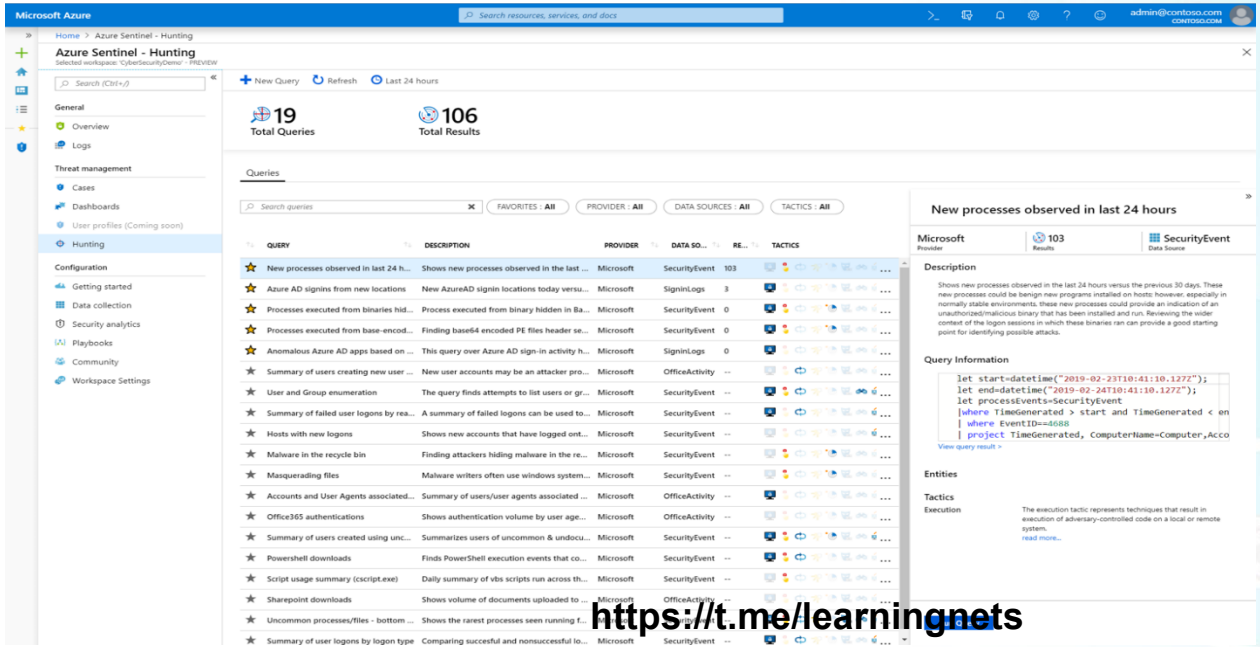
Investigation

Azure Sentinel deep investigation tools help you to understand the scope and find the root cause, of a potential security threat. You can choose an entity on the interactive graph to ask interesting questions for a specific entity, and drill down into that entity and its connections to get to the root cause of the threat.



Hunting

Use Azure Sentinel's powerful hunting search-and-query tools, based on the MITRE framework, which enable you to proactively hunt for security threats across your organization's data sources, before an alert is triggered.



Community

The Azure Sentinel community is a powerful resource for threat detection and automation. Our Microsoft security analysts constantly create and add new workbooks, playbooks, hunting queries, and more, posting them to the community for you to use in your environment.