Microsoft Sentinel

Deploying a Cloud-Native SIEM/SOAR Solution to Monitor a Virtual Lab Environment Within Microsoft Azure

By
Cory Wurtz

Table of Contents

Introduction to Microsoft Sentinel and Azure

What is Microsoft Azure?

- Microsoft Azure is a cloud computing platform and service provided by Microsoft that allows individuals and organizations to build, deploy, and manage applications and services through a global network of Microsoft-managed data centers. Azure provides a wide range of cloud services, including virtual machines, storage, databases, analytics, networking, and much more.
- Within Azure, users can choose from a range of deployment options, including public, private, and hybrid clouds, and can scale their applications and services to meet changing business needs. Additionally, Azure offers a range of tools and services to help users manage, monitor, and optimize their applications and services, including Azure Monitor, Microsoft Defender for Cloud/Endpoint/365, and Azure Advisor, amongst many others.

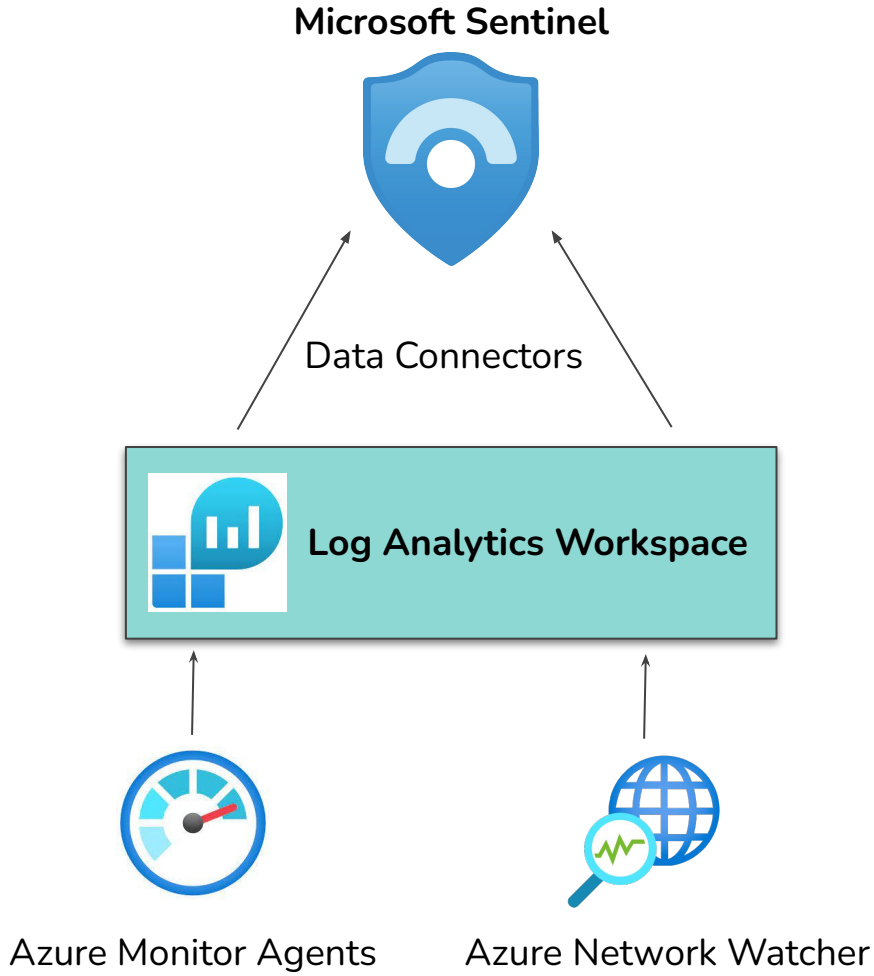
What is Microsoft Sentinel?

- Microsoft Sentinel is a cloud-native SIEM (Security Information and Event Management) solution offered by Microsoft within its Azure cloud platform.
- Sentinel collects data from various sources, including endpoints, servers, applications, and network devices, and provides a centralized location to store, analyze, and respond to security events.
- Its automated response feature can be configured to automatically perform actions to mitigate a threat or stop an activity. As an example, it could automatically block the IP address of a detected malicious actor.
- Its ability to automate responses to threats and activities also classifies Microsoft Sentinel as a SOAR (Security Orchestration, Automation, and Response) tool.

Construction of Microsoft Sentinel/Classification

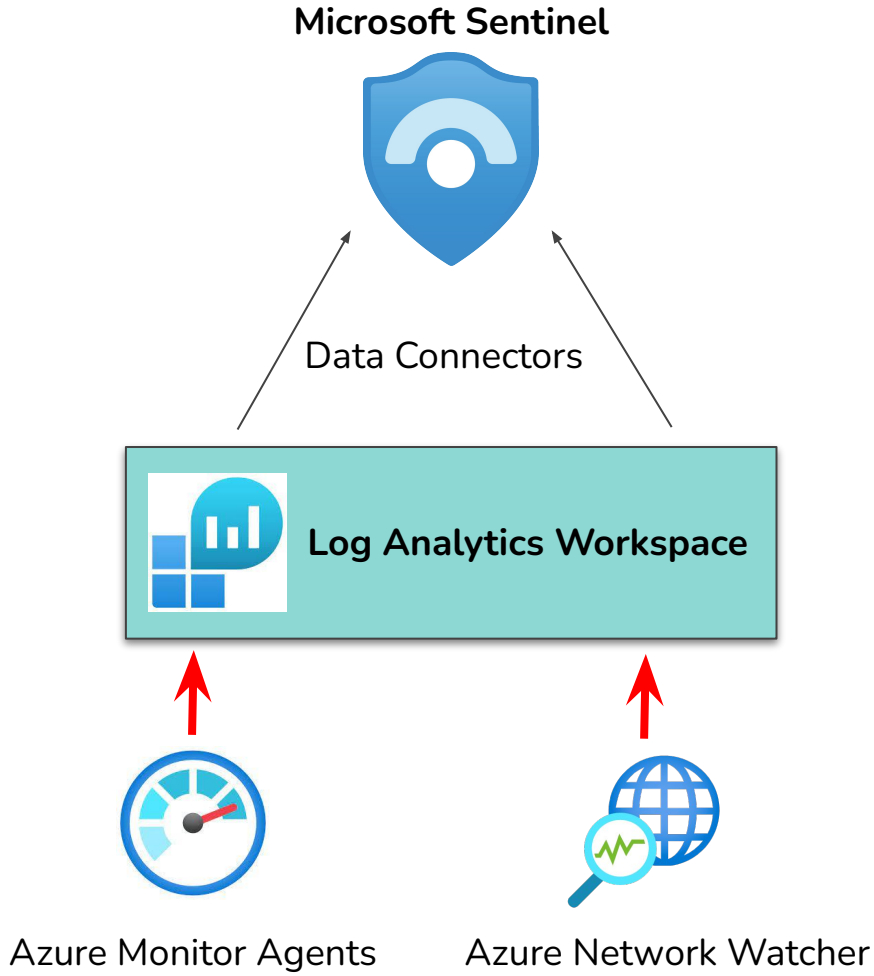
How Is It Constructed?

- Like any SIEM solution, Microsoft Sentinel is built upon data ingestion. Our data ingestion model primarily includes the agents Azure Monitor and Azure Network Watcher, but can include other sources such as Microsoft Defender for Cloud/Endpoint.
- Sources of data can also be ingested from tools and resources outside of Microsoft Azure, including Amazon Web Services, Fortinet, and many others.



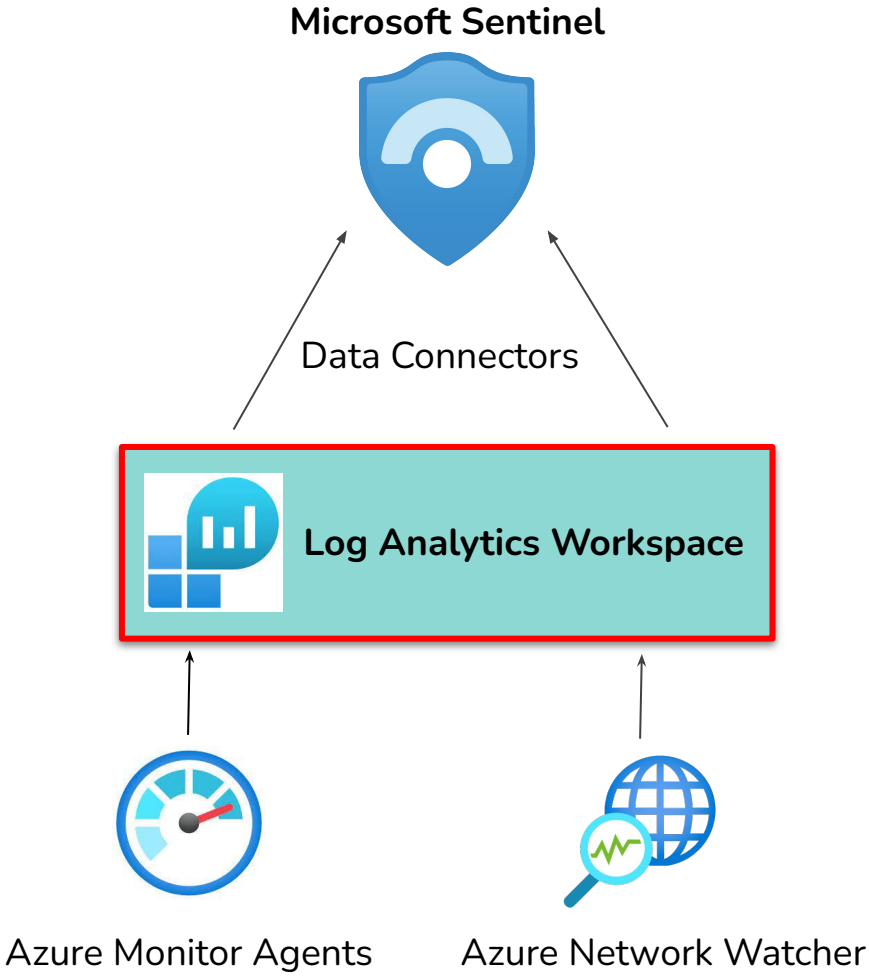
Our Data Flow -Agents

- Monitor agents are installed on the resources you wish to ingest logs from (VMs, containers, etc.), and Network Watcher is deployed as an agent for ingesting flow logs from our Network Security Group. Once configured and enabled, these logs transmit their data to our Log Analytics Workspace.



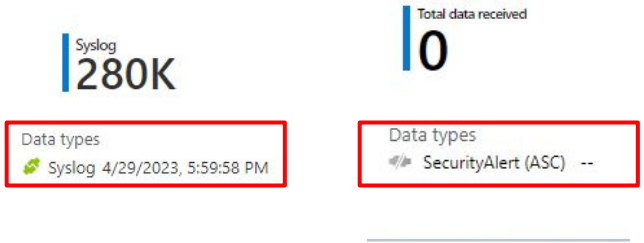
Our Data Flow -Log Analytics

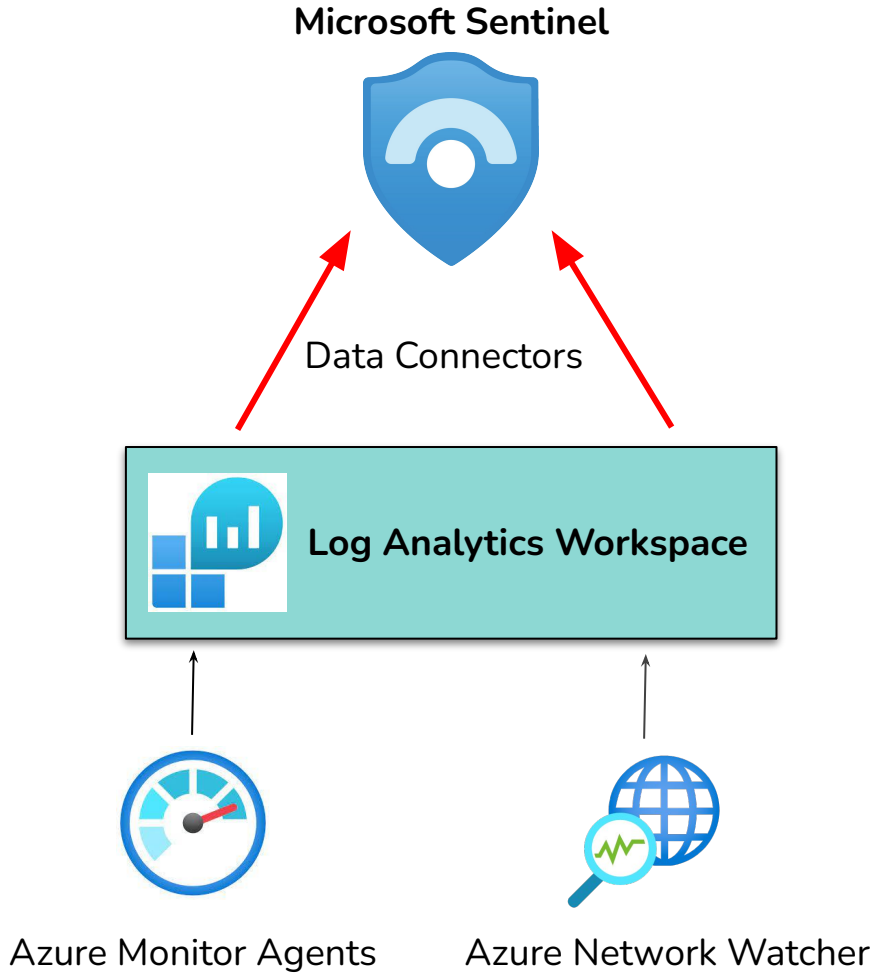
- We deploy our instance of Microsoft Sentinel on top of our Log Analytics Workspace. Our LAW serves as the repository for all of our logs and telemetry data, where they can be aggregated, queried, and later connected to Microsoft Sentinel for advanced threat detection and response. Sentinel utilizes a query language similar to SPL in Splunk, called Kusto Query Language (KQL).



Our Data Flow -Connectors

- Our data connectors within Microsoft Sentinel connect the data in our LAW and other Azure resources to Microsoft Sentinel, allowing us to visualize the data in dashboards known as workbooks. With some exceptions, these require data to be in our LAW before they can be connected in Sentinel; no data=no data connection.



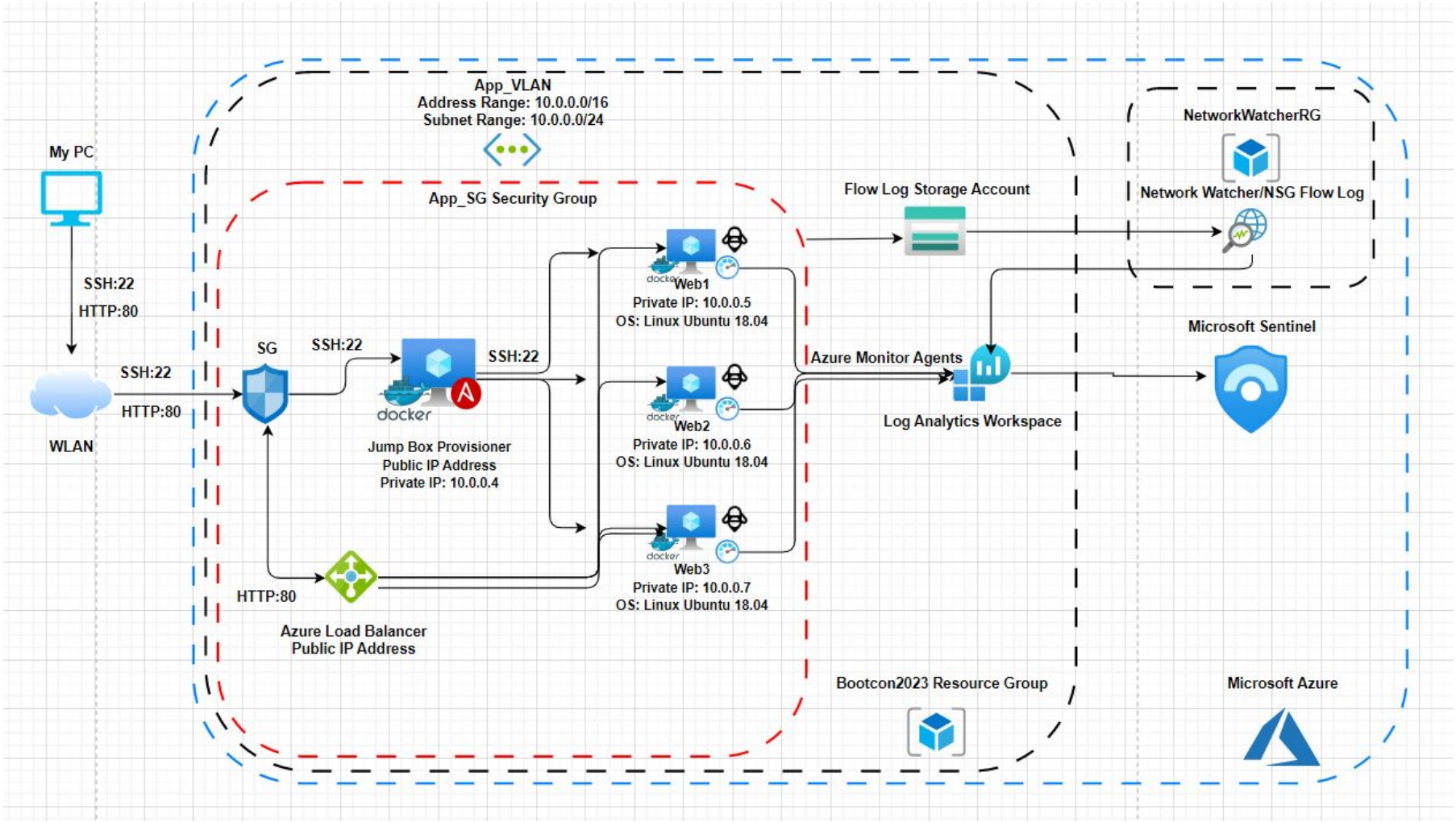


Classifying Our Environment

- The environment we have configured Sentinel to monitor is a recreation of the pentesting lab environment from the cloud security unit earlier in the course. This environment would be classified as “Infrastructure as a Service”, with Azure providing infrastructure such as VMs with us managing and providing the software and applications within it (Docker/Ansible, etc.).
- Our deployment of Sentinel falls under Platform as a Service, with Azure providing their SIEM/SOAR as a platform for security monitoring and with us simply utilizing and configuring it.

Infrastructure as a Service (IaaS)	Provides physical/virtualized infrastructure and networking only; client controls deployment of application, data, and software.
Platform as a Service (PaaS)	Cloud provider supplies all infrastructure/virtualization, software, and networking as well as runtime and middleware; client only configures and delivers pre-built applications.
Software as a Service (SaaS)	All infrastructure/virtualization, software, applications, runtime, and middleware supplied by cloud provider; client only needs web browser or API.

Network Topology


App_VLAN
Address Range: 10.0.0.0/16
Subnet Range: 10.0.0.0/24
App_SG Security Group
NetworkWatcherRG
Network Watcher/NSG Flow Log
Flow Log Storage Account
My PC
SSH:22
HTTP:80
WLAN
SG
SSH:22
HTTP:80
SSH:22
SSH:22
docker
Jump Box Provisioner
Public IP Address
Private IP: 10.0.0.4
Web1
Private IP: 10.0.0.5
OS: Linux Ubuntu 18.04
Web2
Private IP: 10.0.0.6
OS: Linux Ubuntu 18.04
Web3
Private IP: 10.0.0.7
OS: Linux Ubuntu 18.04
HTTP:80
Azure Load Balancer
Public IP Address
Azure Monitor Agents
Log Analytics Workspace
Microsoft Sentinel
Bootcon2023 Resource Group
Microsoft Azure

Brief Tour/Demonstration Within Azure

To Summarize

- We constructed a virtual lab environment within Microsoft Azure.
- We configured the resources within that environment to feed telemetry data to a central repository for aggregation and analysis.
- We deployed a cloud-native SIEM/SOAR solution to connect with that data, created dashboards known as workbooks for data visualization, and analytic rules for generating alerts and incidents that a SOC team can then investigate and respond to.
- Automation of those responses would be the next step up in your environment's maturity model.

Fin

Thank you for listening to my presentation! Any questions/comments/suggestions are very welcome!