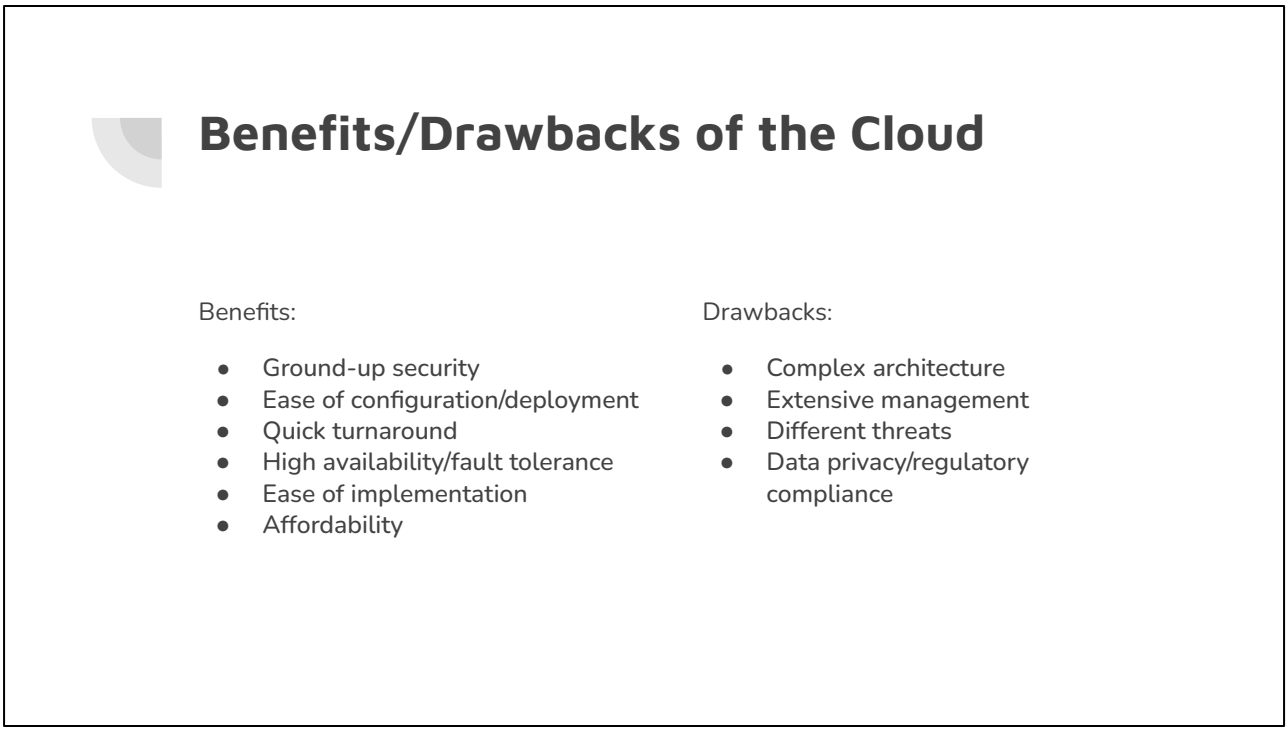
Microsoft Sentinel

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

By
Cory Wurtz

Table of Contents

Cloud Benefits/Drawbacks & Introduction to Microsoft Sentinel



Why is the cloud becoming so popular?

It has many benefits:

1. Ground-up security: From a security perspective, the cloud presents an opportunity to build a secure system from the beginning, as opposed to trying to implement new security measures on old systems.
2. Easy configuration: Instead of having to learn the many different tools that will be included on a network, an administrator can use the cloud service provider's website portal to create all necessary resources.
3. Quick turnaround: Compromised and insecure machines can be discarded and replaced quickly at no additional cost to the organization.
4. High availability and fault tolerance: Without their own physical data centers, engineers can focus on deploying their machines in multiple places, and the provider can maintain the data center. This way, cloud networks are more robust against power outages, DoS attacks and other threats, provided they are configured properly.
5. Easy Implementation: Security controls can be implemented more easily since they only require modifications to software configurations–no physical re-arrangements necessary.
6. Affordability: Organizations can use powerful machines that they would not otherwise be able to afford were they responsible for purchasing and maintaining them themselves. For example, GPU processing units, which are very expensive to buy and very expensive to lose to an attacker.

While the benefits generally far exceed the potential drawbacks, those drawbacks are still worth considering.

1. Complex architecture: Systems must be built to both ensure basic security, and allow infrastructure personnel to securely monitor, reconfigure, and redeploy machines as necessary. This is typically easier to do securely with on-premises machines, since these are not exposed to public networks unless it is necessary. Since all access to cloud resources is through a public network to begin with, careful steps must be taken to ensure that they are only exposed to the relevant parties.
2. Extensive management: While ease of configuration and deployment is generally advantageous, without a proper method of tracking changes and management, a network of cloud resources can quickly become disorganized, complex, and inefficient.
3. Different threats: Cloud providers handle certain aspects of security for an organization, which means security professionals have new and different things they must pay attention to. Malicious actors will execute escalation and lateral movement tactics differently on the cloud than on-premises.
4. Data privacy/regulatory compliance: Depending on the nature of the data being stored in the cloud, compliance with industry-specific regulations and laws regarding data privacy may be a challenge. While cloud providers typically have good practices in place for ensuring their clients don't have to worry about this, in the event that the cloud provider does not meet compliance standards for a certain industry, liability for the fault in compliance would fall on the client, not the cloud provider (depending on the terms of service). Therefore, it is important that an organization looking into cloud services research what compliance standards a potential provider meets.

What is Microsoft Sentinel?

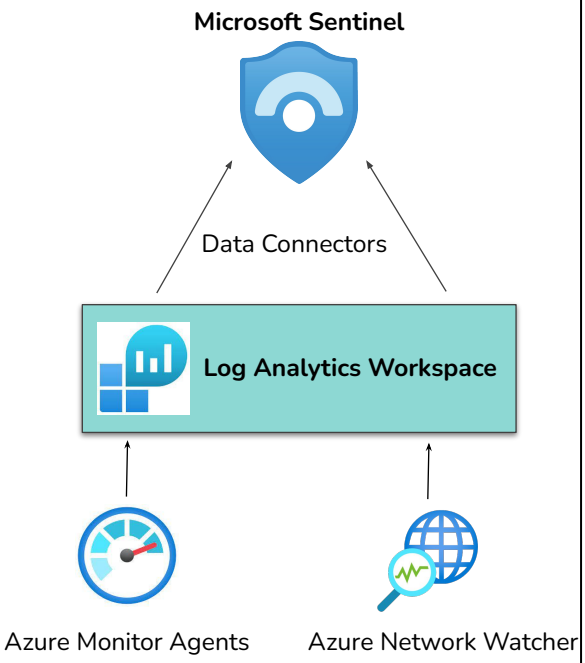
- Cloud-native SIEM (Security Information and Event Management) solution
- Uses the Kusto Query Language (KQL)
- Automated response feature
- SOAR (Security Orchestration, Automation, and Response) solution

- Microsoft Sentinel is a cloud-native SIEM (Security Information and Event Management) solution offered by Microsoft within its Azure cloud platform.
- Sentinel and the Log Analytics Workspace it is built upon utilize the Kusto Query Language (KQL) for log queries and analytic rule creation.
- 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.

Deployment of Microsoft Sentinel

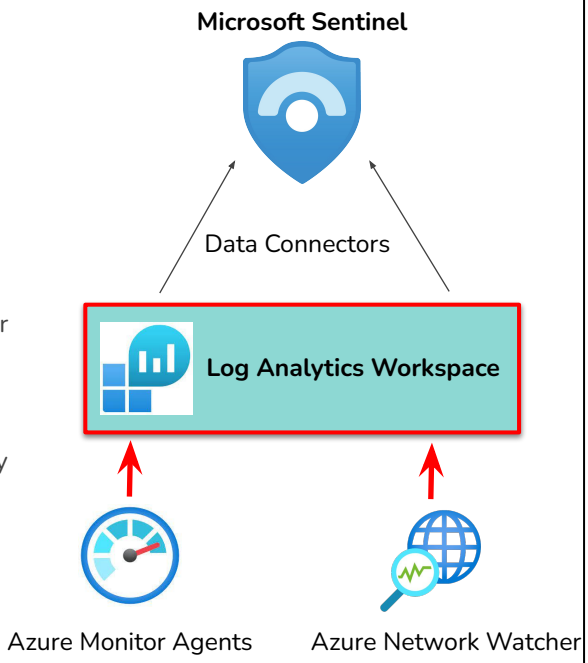
How Is It Constructed?

- 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, Google Cloud, or traditional IT structure.



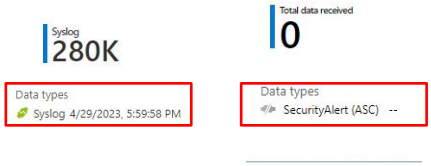
Log Analytics Workspace

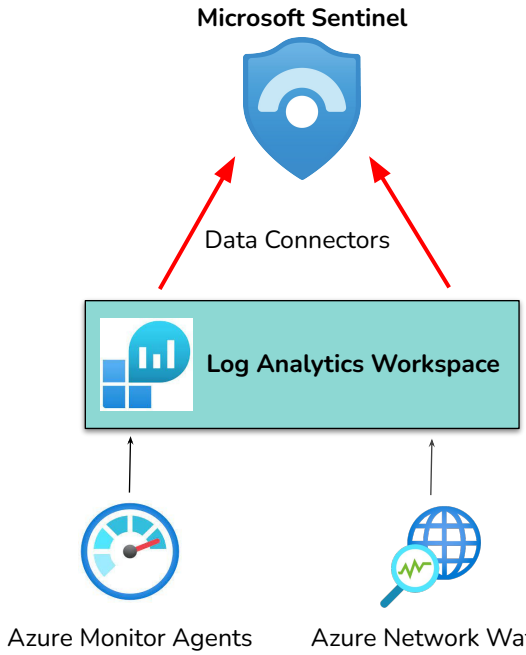
- Before we can install our monitoring agents, we first need a place to send the logs. Our Log Analytics Workspace will serve as our repository for all of our logs and telemetry data. Once our agents are configured and populating our Workspace, we can deploy Microsoft Sentinel on top of it and apply our data connectors.



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.





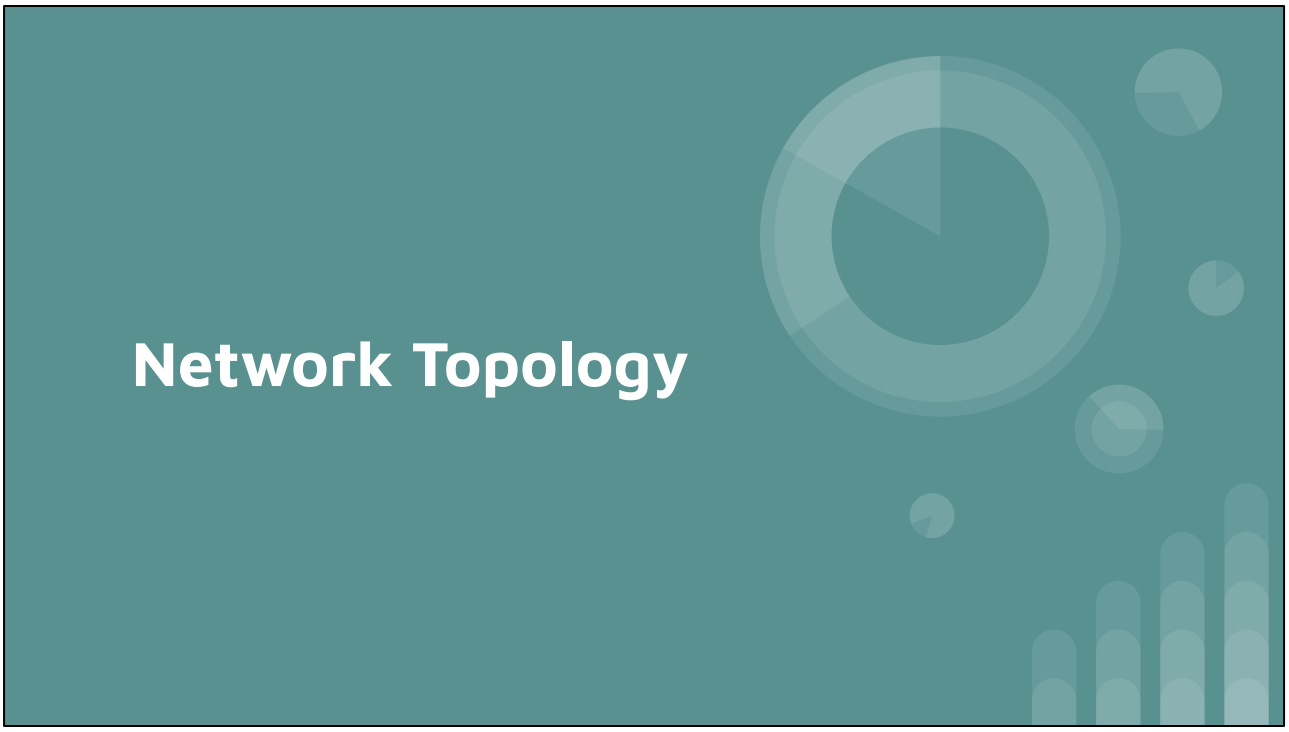
Classifying Our Environment

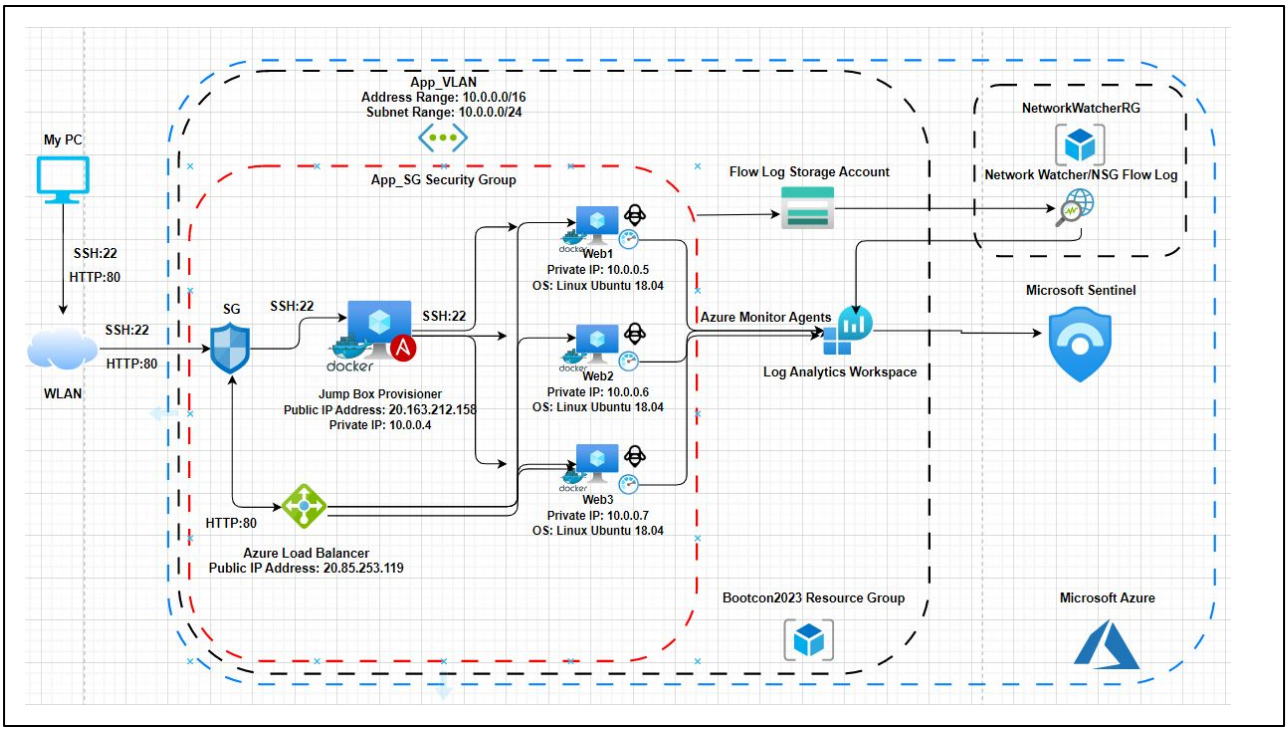
- Hybrid Environment
- Lab: IaaS
- Sentinel: PaaS

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.

- 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.

Network Topology





Some quick notes:

- We can see all of our resources, aside from my personal computer, are deployed within Microsoft Azure.
- Our log analytics workspace is deployed within our Bootcon resource group, and receives logs directly from our Azure Monitor agents.
- Our flow logs from our Network Security Group must first be exported to a storage account, then to our Network Watcher deployed in its own resource group, before it heads to our Analytics Workspace.
- Once our logs are in our Analytics Workspace, we then apply our data connectors in Sentinel.

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!