Azure Sentinel
Use Cases

Ofer Shezaf, Principal Product Manager, Azure Sentinel
About module #2b: Use case discussion

**Overview**

- In this module you will learn where Azure Sentinel can be used.

**Pre-requisites**

- Azure Sentinel Overview module.
Sentinel use cases and value proposition
Sentinel use cases

- Log management
- Enabler (and compliance)
- Single pane of glass
- Shared responsibility with ticketing system
- Investigation & hunting
- Shared responsibility with expert detectors
- Response
- Detection
- Shared responsibility with expert detectors
- Alert handling
- Enrichment, Prioritization, Triaging
- Incident management
- Shared responsibility with ticketing system
- Automation
The great divide

Traditional SIEM
- Real time correlation
- Ingest time parsing

Search based SIEM
- Scheduled queries
- Query time parsing
Cloud SIEM

No brainer Advantages
- Auto-scales
- Easy collection from cloud sources
- Avoid sending cloud telemetry downstream
- Key log sources are free

But there is more!
- DevOps deployment and enforcement
- Distributed
- Cloud native-schema

Use
- The cloud security team

Requirements
- Side by side deployment with current SIEM
“Azure Sentinel works seamlessly with Office 365 and other Azure services and security tools. Compared to other SIEMS I have used, it’s much easier to connect our data sources to Azure Sentinel. There are built-in connectors not just for Microsoft but also for other major security vendors.”

Jay Vaidya
Senior Security Analyst, Brewin Dolphin
Serverless automation and integration

- **APIs**
  - Graph Security API
  - Management
  - Data ingest
  - Data query

- **Deployment**
  - ARM
  - DevOps integration
  - Azure policy

- **Serverless**
  - Logic Apps
  - Azure functions
  - Lambda functions....
Side by side

Upstream

Events

Alerts

Downstream
Sentinel and the Microsoft security suite

Cloud Native SIEM + SOAR - Azure Sentinel
Built on Azure Monitor, Logic Apps, and Microsoft’s UEBA/ML Technology

Microsoft Threat Protection

ENDPOINT
Windows Defender ATP
Endpoint Detection & Response (EDR)

IDENTITY
Azure ATP + Azure AD
Identity Protection

SaaS
Office 365 Advanced Threat Protection (ATP) + Cloud App Security

AZURE
Azure Security Center

Breadth
- Unified Alert Queue
- Customized Alerts

Depth
- High quality alerts
- End to end investigation and remediation

Event Log Data from Devices, Services, and Security Tools (3rd party and Microsoft)
Next Gen SIEM

Advantages
- Effortless infinite scale
- Ease of integration
- Effective and integrated SOAR
- Microsoft research and ML
- SIEM and data lake in one

Use
- SIEM replacement

Requirements
- On prem-collection
Microsoft Security Advantage

- $1B annual investment in cybersecurity
- 3500+ global security experts
- Trillions of diverse signals for unparalleled intelligence
Machine learning meets big data

300B
Identity

500B
O365

320B
Azure

28M
Identity

20M
O365

2M
Azure

320
Candidates

90
High Severity Incidents

Anomaly Detection

Graph-powered ML + Probabilistic Kill Chain

Additional ML
Innovative security operations
On-prem collection

Branch Office

CEF/Syslog connector

OS events, DNS, Windows FW, DHCP

CEF or Syslog connector

HTTPS

Logstash

Syslog (TLS, TCP, UDP)

CEF/Syslog connector

HTTPS

Custom Connectors

Sentinel REST API

OS events, DNS, Windows FW, DHCP

HTTPS

WEC

Sentinel REST API

HTTPS

Symantec

Barracuda

HTTPS

HTTPS

HTTPS

HTTPS

HTTPS

HTTPS

HTTPS

HTTPS
Cloud Collector

Advantages

• Easy collection from cloud sources.

*No* Opportunity

• Cost prohibitive.

Requirements

• Stream events to on-prem SIEM.
Pricing
**Annual ingress:**
$\text{GB/d} \times 365$

**Price per GB:**
$\$2.53 + \$0.1$

**Total annual cost:**
Annual ingress $\times$ Price per GB

**Small print:**
- East US prices
- > 500 GB/s volumes
Or use the calculator
Paying less

- An ASC license gives free ingest of 500MB/node/day of Windows Security Events.
- Some sources are free to ingest:
  - Office activity, azure activity, Microsoft alert sources.
  - Enables free use cases and evaluation
  - But not a major discount for a full deployment.
- Enterprise customers will pay less, sometime a lot less:
  - Enterprise agreement (EA) discount will apply
  - Azure commitment discounts (ACD) will apply
Sizing

- Never easy. The variant is high.
- Use the evaluation period.
- If you have an EPS estimate: 1000 EPS $\approx 50$GB/d
- We are building an estimation tool. Help us.