Azure Sentinel Deployment

Service Description

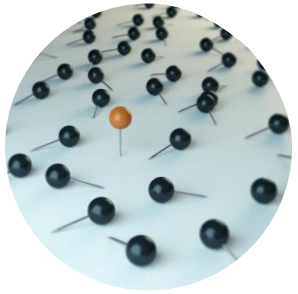
SULAVA

Azure Sentinel

Cloud-native Security Information and Event Management system (SIEM)

Collect Data

At cloud scale across all users, devices, applications and infrastructure, both on-premises and in multiple clouds

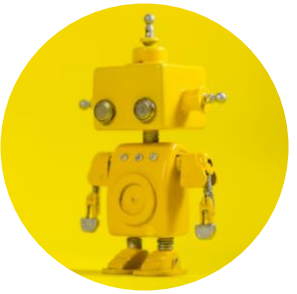


Detect

Previously uncovered threats and minimize false positives using analytics and unparallelled threat intelligence from Microsoft

Investigate

Threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.



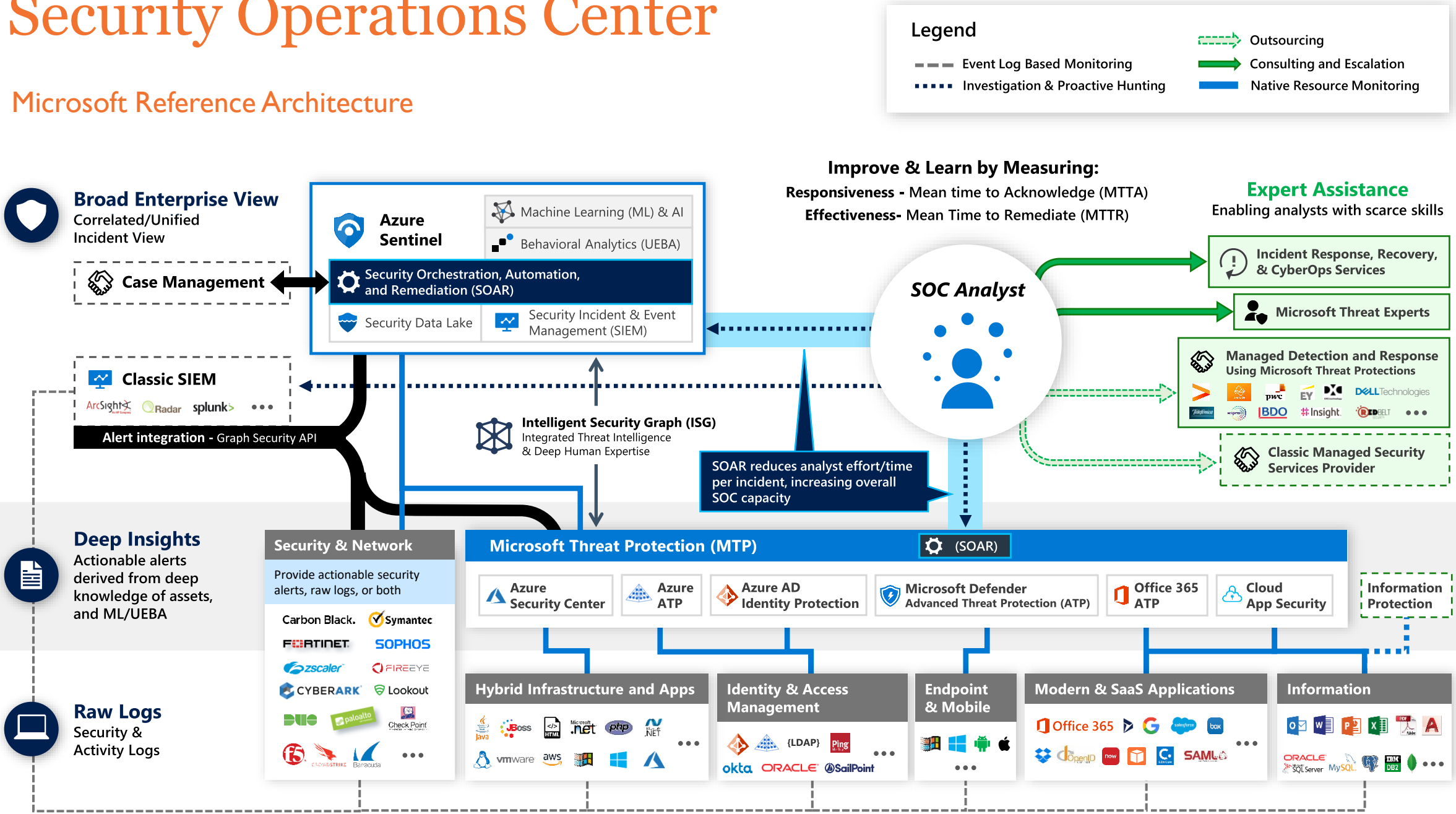
Respond

To incidents rapidly with built-in orchestration and automation of common tasks

SULAVA

Security Operations Center

Microsoft Reference Architecture



Azure Sentinel – WHY?

1. **Zero Footprint SIEM** – provisioned instantly from cloud
2. **Secure long-term retention** of O365 & Azure logs
3. **Ability to investigate security** issues by cross-refencing logs from various sources
4. **Truly pay-what-you use** based on gigabytes ingested – typical pricing 2-200€/month depending on the organization size
   - *For example, according to new IDG research among 300 IT and security leaders, the top outcomes respondents expect by switching to cloud-based SIEM include:*
     - *Forty percent—lower staffing costs.*
     - *Forty percent—lower operational expenses (OpEx).*
     - *Thirty-four percent—lower capital expenses (CapEx).*
     - *(Source)*

Azure Sentinel – WHAT?

Preparation call

- Define full scope & align expectations
- Schedule the work & plan attendees
- Technical pre-requisites check

Workshop day 1 (3 hours, remote):

- Planning the role of Azure Sentinel in customer's current security architecture & pricing review
- Provisioning Azure Sentinel in customer's Azure environment
- Connecting available Microsoft cloud log sources
- Defining log retention policy
- Defining admin access to logs

Workshop day 2 (3 hours, remote):

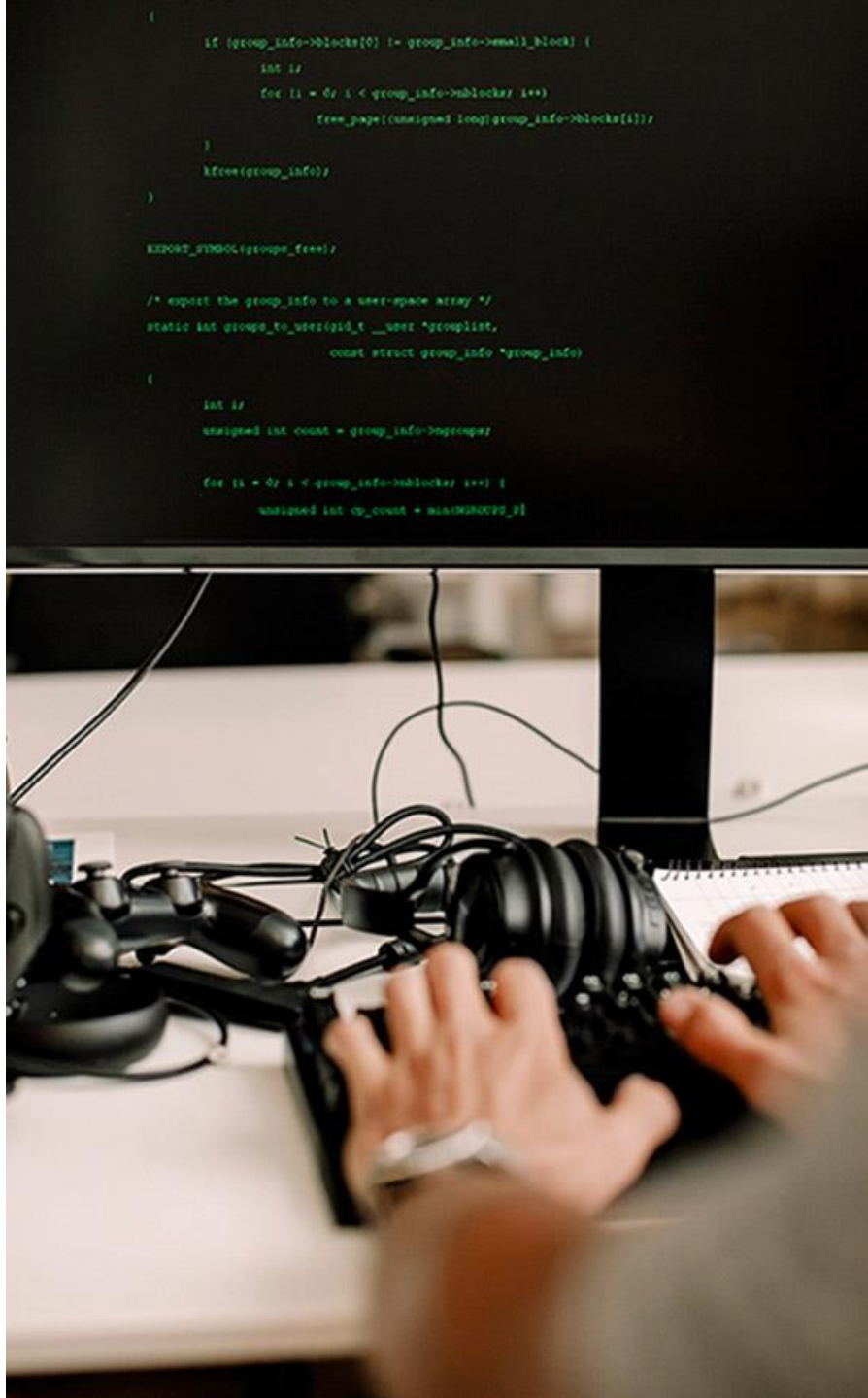
- Configuring sample alerts in Sentinel Analytics
- Walkthrough of utilizing detect / investigate / respond functionality
- Creating a plan for connecting additional sources: on-premises servers, firewalls, 3rd party services etc. & improving detection & response capability

SULAVA

Azure Sentinel

Deliverables and pricing:

- Sentinel workspace provisioned
- Long-term storage for Microsoft cloud log sources
- Understanding for Sentinels basic operations
- Capability for detecting & investigating anomalies
- A plan & roadmap for integrating other log sources and improving detect & response capabilities



Out of scope and customer responsibilites

Out of scope

- Connecting additional log sources
- Forensics services or deep analysis of found threats

Customer's responsibilities

- Access to appropriate Azure subscription & owner permission to provision new resources
- Global Admin access to M365 & Azure log sources (Sulava instructs customer or does the actual configuration)
- Participation in preparation call and workshops

SULAVA

Thank you!