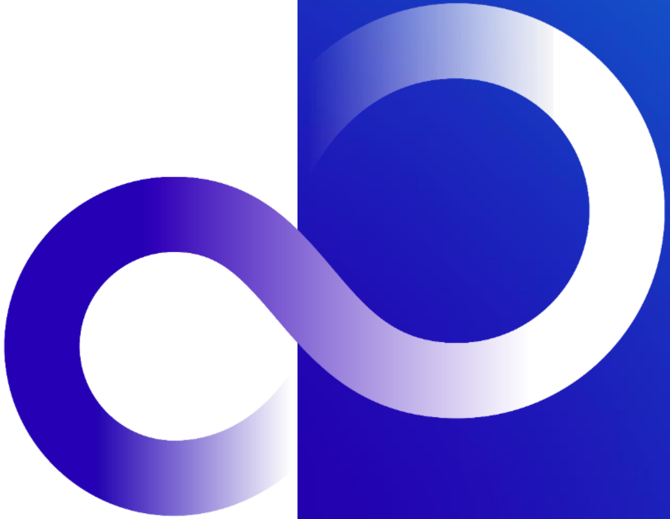
Uvance Hybrid IT
Security Services

Threat Monitoring Workshop



Agenda

Threat Monitoring Workshop

- Threat Monitoring Overview
- Introduction to the tool: Microsoft Sentinel
- Threat Monitoring Workshop Timeline
- Architecture and Future Development

Threat Monitoring Overview

What is it?

Security incident alerting

Sentinel management

Why we do it?

SIEM onboarding

MDR first steps

How do we do it?

Infrastructure as code

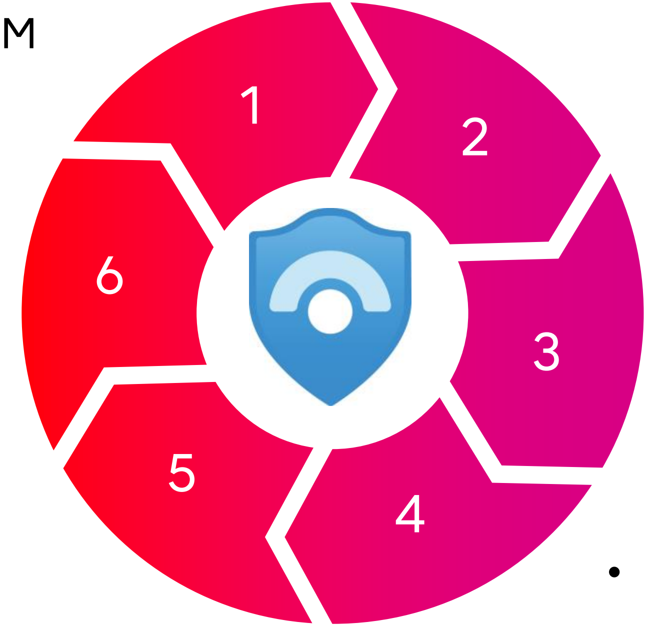
Curated content

What do we need?

Roles

Stakeholders

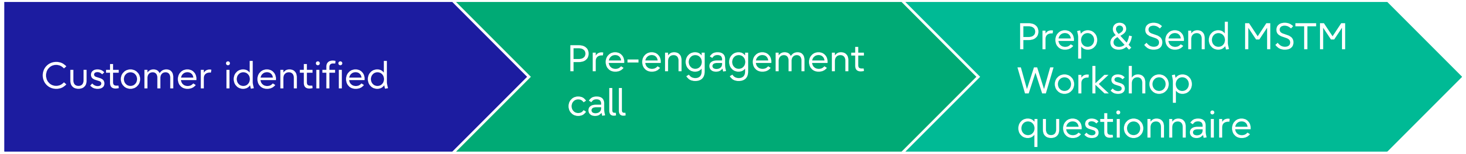
Microsoft Sentinel



- Gartner-leading cloud-based SIEM
- Collect data from security tools and infrastructure
- No fees for Microsoft related logs / connectors
- Modular deployments and ease of MSSP and customer collaboration
- Out-of-the-box connectors and templates
- Early detection of threats integrated with MS 365 products

Threat Monitoring Workshop Timeline

Week 1: Pre-engagement

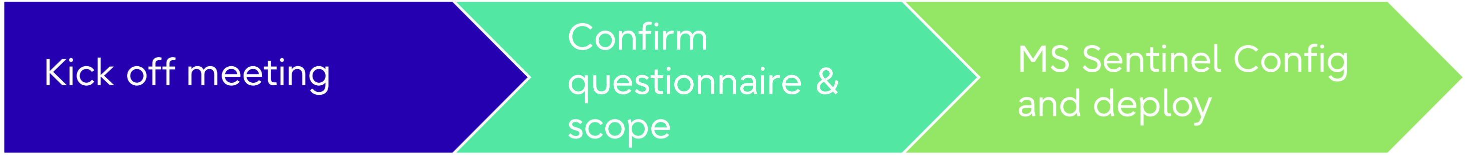


Customer identified

Pre-engagement call

Prep & Send MSTM Workshop questionnaire

Week 2: Engagement and setup



Kick off meeting

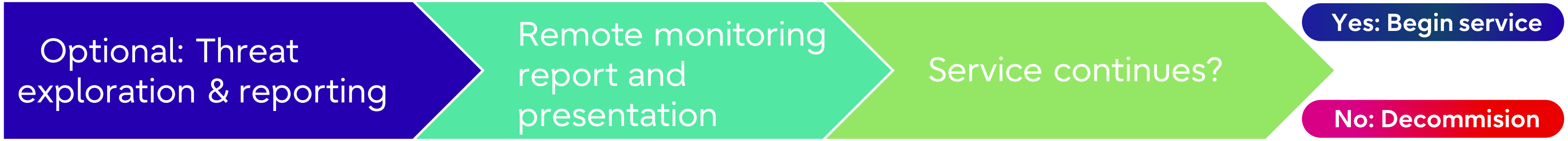
Confirm questionnaire & scope

MS Sentinel Config and deploy

Week 3:Data collection and monitoring

Remote monitoring as per service

Week 4: Wrap up



Optional: Threat exploration & reporting

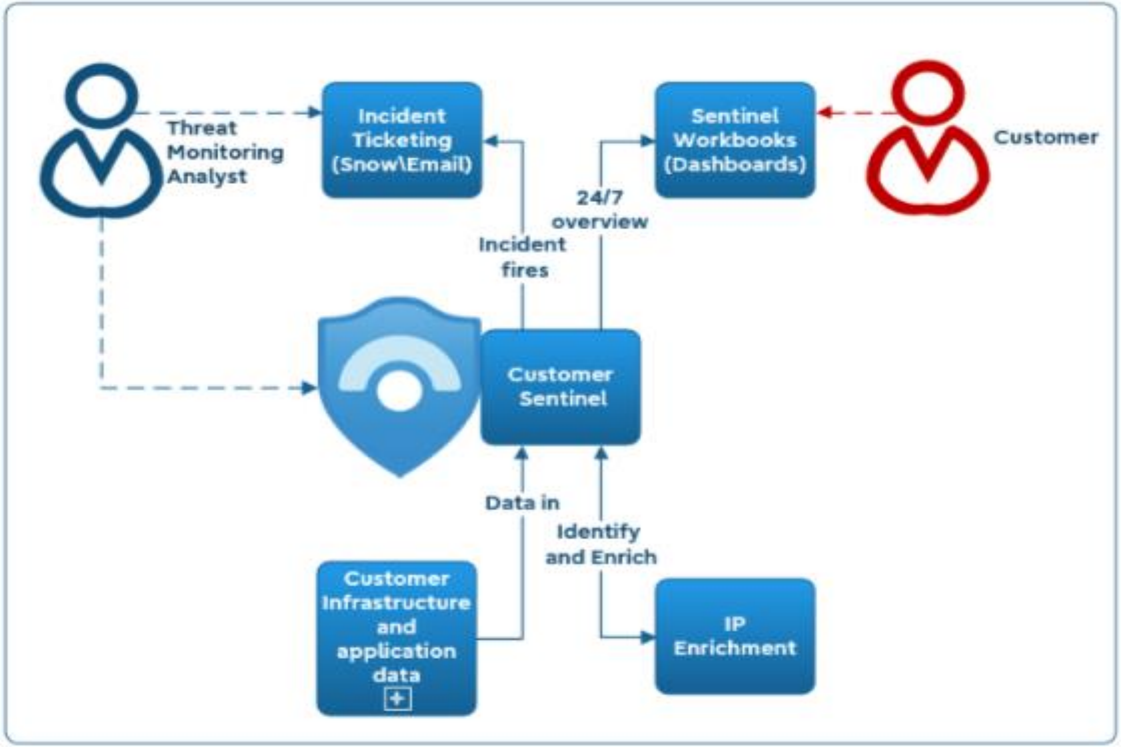
Remote monitoring report and presentation

Service continues?

Yes: Begin service

No: Decommision

Architecture and Future Development



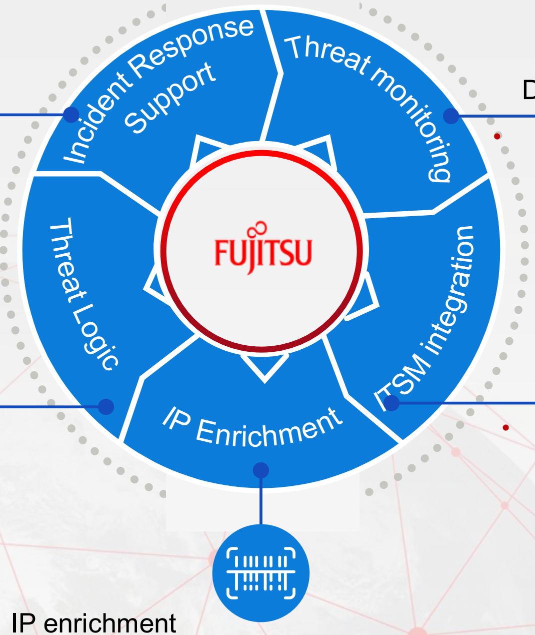
Threat Monitoring Analyst
Incident Ticketing (Snow\Email)
Sentinel Workbooks (Dashboards)
Customer
24/7 overview
Incident fires
Customer Sentinel
Data in
Identify and Enrich
Customer Infrastructure and application data
IP Enrichment

Threat Monitoring

FUJITSU

Threat Monitoring

- Out of the box analytic rules and detection packs
- Improved visibility
- Proactive threat detection
- IP enrichment against external IP addresses
- Integrated services across Microsoft security, network and cloud environments
- Service Desk integration



Incident Response Support

- Engagement with customer Incident Response team, logging of incidents in ITSM and provision of logs, where applicable to support investigations

Daily threat monitoring

- Analysing and responding to incidents observed in the Sentinel platform and incidents raised to the customer via ITSM

Out of the box rules

Static rules available through the Sentinel platform for monitoring of potential threats

- Implementation and monitoring of detection packs

ITSM integration

- Integration with Fujitsu Service Now instance for logging of incidents and customised view into customer ITSM for visibiity

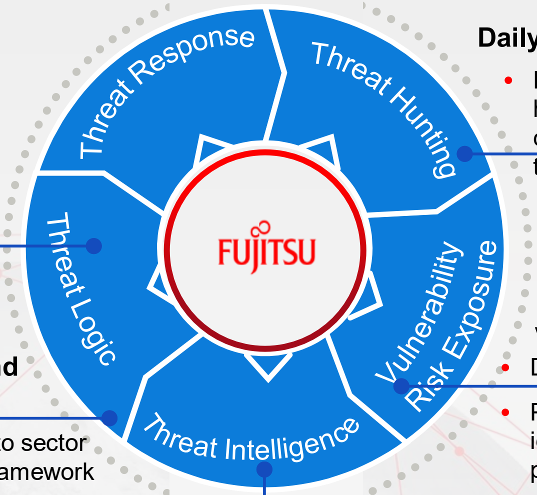
IP enrichment

Intelligence enrichment against external IPs

MDR

MDR

- Customized, dynamic rules, playbooks and detection packs
- Reduced MTTR
- Measurements against risk controls
- Proactive threat detection
- Increased User and Entity Behavior controls & analysis
- Integrated service across customer toolsets outside of Microsoft



Threat Response

- End to End incident response with collaboration via Teams Incident War Room

Daily threat hunting

- Hypothesis-based threat hunting and analysis and continuous learning and tuning

Customizable rules and alerts

- Dynamic rules aligned to sector and MITRE ATT&CK framework
- Customizable rules created from threat intelligence

Vulnerability Risk Exposure

- Daily analysis of vulnerabilities
- Playbook-driven approach to identification of devices for priority patching

Threat Intelligence

- Horizon scanning for latest threats related to the customer and sector
- Enrichment of playbooks and customized tags for IOC management and analysis

Thank you