Cloud Security Manage Services

PT Mitra Integrasi Informatika

Microsoft

Azure Sentinel

MITRA INTEGRASI INFORMATIKA

Four Security Priorities of Today

Protect
your people

Identity & access management

Secure and manage
your apps and devices

Unified endpoint management

Safeguard against
outside threats

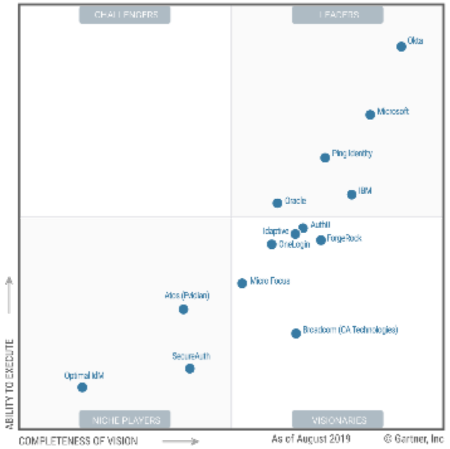
Advanced Threat protection

Keep your
data safe

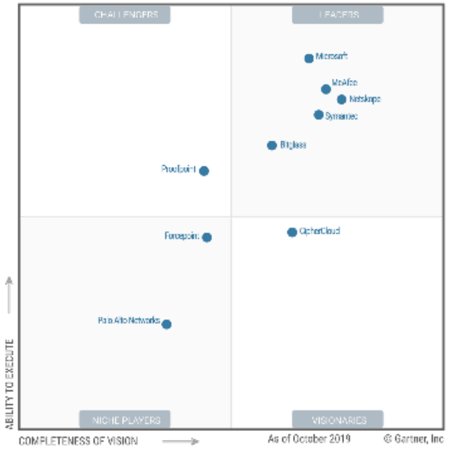
Information protection

Gartner®

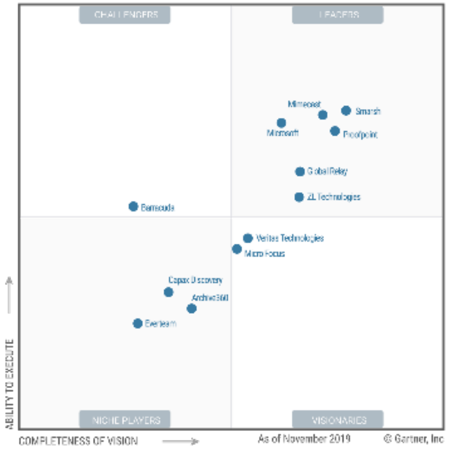
Microsoft—a Leader in 5 Gartner Magic Quadrant reports



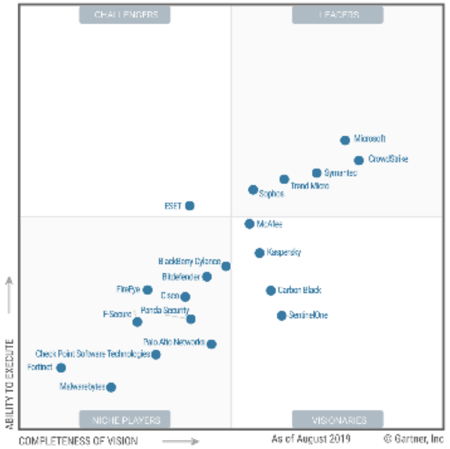
Access Management



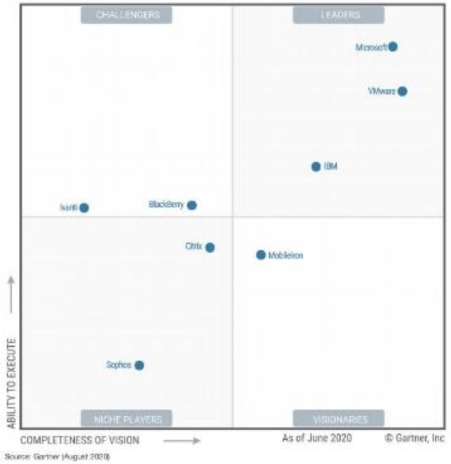
Cloud Access Security Brokers



Enterprise Information Archiving



Endpoint Protection Platforms



Unified Endpoint Management

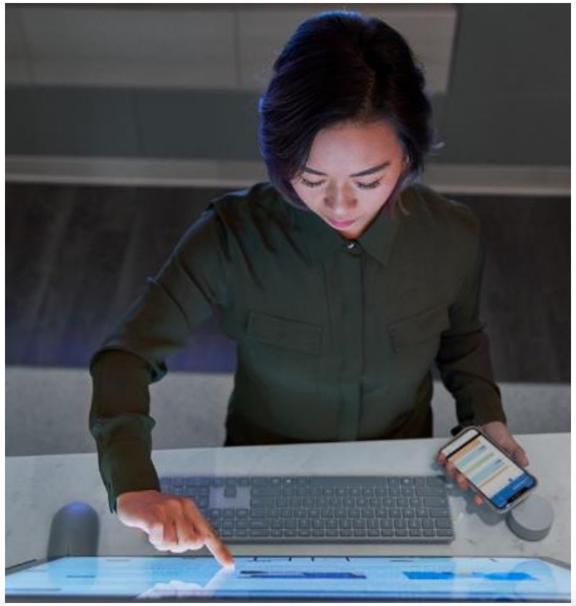
*Gartner "Magic Quadrant for Access Management," by Michael Kelley, Abhyuday Data, Henrique, Teixeira, August 2019
*Gartner "Magic Quadrant for Cloud Access Security Brokers," by Steve Riley, Craig Lawson, October 2019
*Gartner "Magic Quadrant for Enterprise Information Archiving," by Julian Tirsu, Michael Hoech, November 2019
*Gartner "Magic Quadrant for Endpoint Protection Platforms," by Peter Firstbrook, Dionisio Zumerle, Prateek Bhajanka, Lawrence Pingree, Paul Webber, August 2019
*Gartner "Magic Quadrant for Unified Endpoint Management ," by Dan Wilson, Rich Doheny, Rob Smith, Chris Silva, Manjunath Bhat, August 2020

These graphics were published by Gartner, Inc. as part of larger research documents and should be evaluated in the context of the entire documents. The Gartner documents are available upon request from Microsoft. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

Microsoft security

Identity and access management

Secure access for a connected world



Threat protection

Stop attacks with integrated, automated SIEM and XDR

Information protection

Protect sensitive data and manage insider risks with intelligence

Cloud security

Safeguard your multi-cloud resources

Introducing Microsoft Azure Sentinel

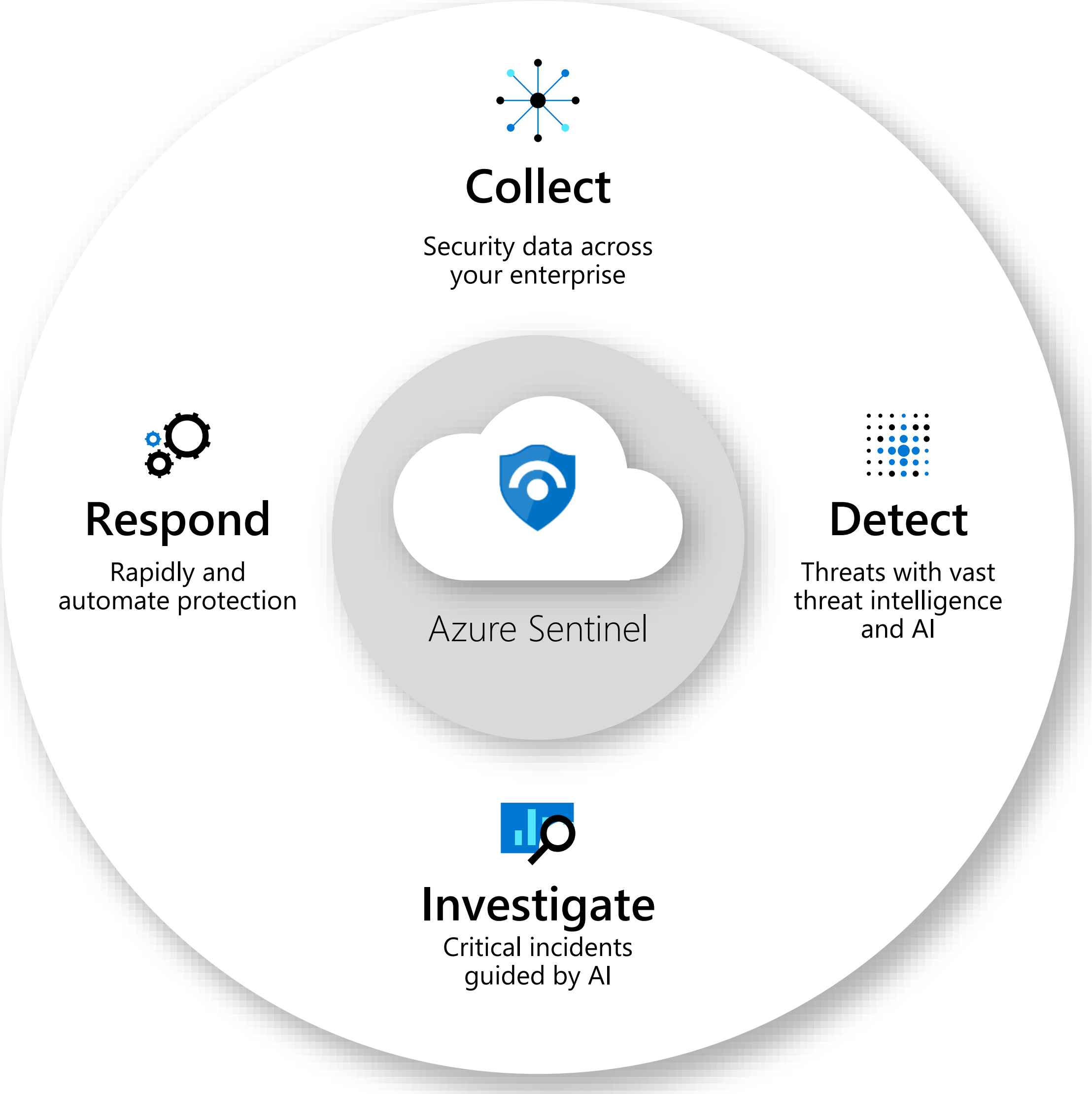
Cloud-native SIEM for intelligent security analytics for your entire enterprise

Limitless cloud speed and scale

Bring your **Office 365 data for Free**

Easy integration with your **existing tools**

Faster threat protection with **AI by your side**



Collect
Security data across your enterprise

Respond
Rapidly and automate protection

Azure Sentinel

Detect
Threats with vast threat intelligence and AI

Investigate
Critical incidents guided by AI

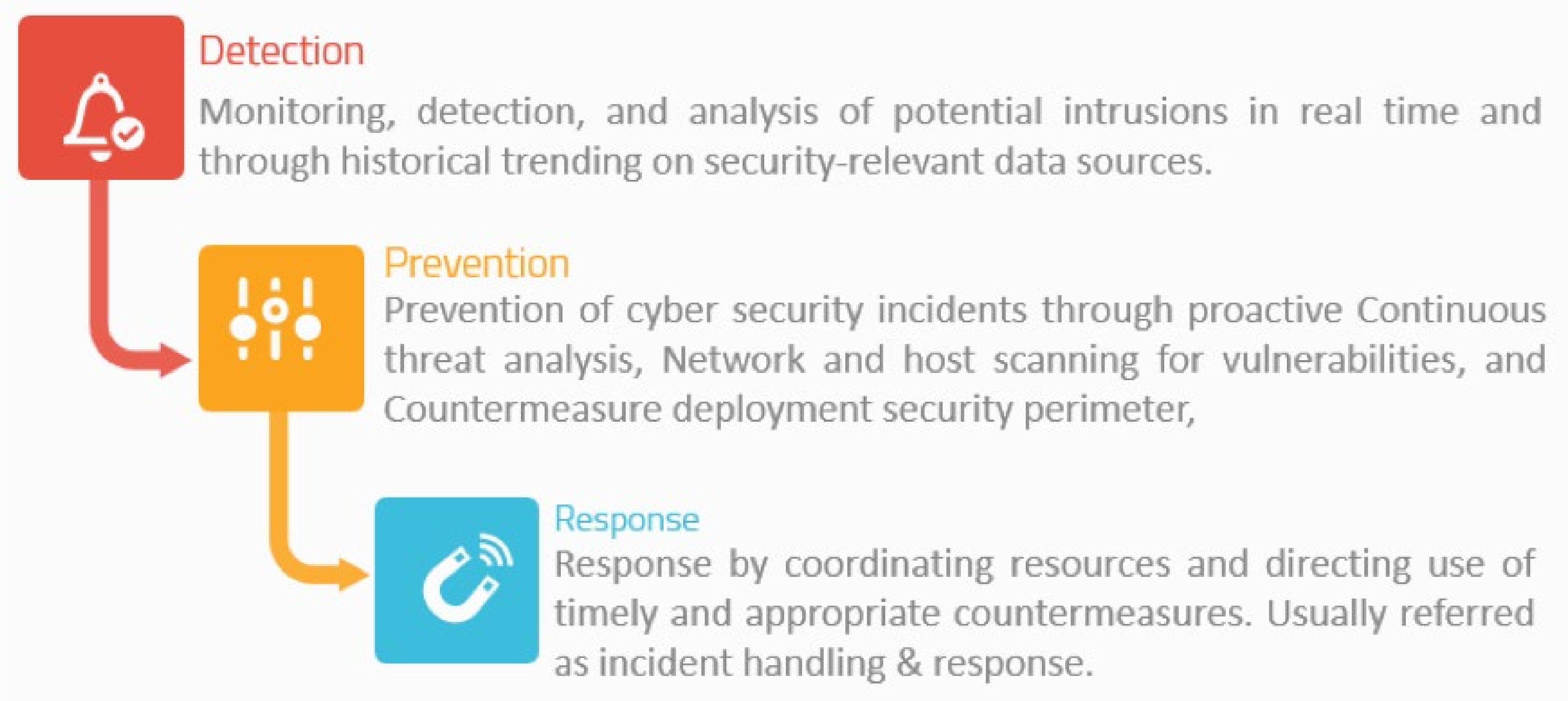
Security Operation Center

A SOC is a team primarily composed of security analysts organized to

- **Detect**
- **Prevent**
- **Respond**

Cyber Security Incidents

Security Operation Center Capability



Detection

Monitoring, detection, and analysis of potential intrusions in real time and through historical trending on security-relevant data sources.

Prevention

Prevention of cyber security incidents through proactive Continuous threat analysis, Network and host scanning for vulnerabilities, and Countermeasure deployment security perimeter,

Response

Response by coordinating resources and directing use of timely and appropriate countermeasures. Usually referred as incident handling & response.

Key Benefit of Managed Security Services

Cost Savings:

Cost saving on Technology / Applications (SIEM, Security Appliance, Ticketing System)
Cost saving on Security Analyst (Hiring, Training, Certification)
Cost saving on Security Operation Center Facilities

Knowledge and Expertise:

Accessing IT Security Expert from MSSP
Getting the latest security trend and issue
Up to date technology and information regarding security issue
Proactive Security Approach rather than Reactive Security Approach for Security Monitoring

Improve Performance:

Internal staff can focus on higher level
Focus on strengthen policy and procedure for company
Accelerate detection and response on every potential security threat

MSSP Main Features

24x7 (1 Years) Security Monitoring Services

Security Advisory Services

Regularly Vulnerability Assessment

Cutting Edge and Advanced Technology

Incident Response and Incident Handling

Digital Forensic

Key Benefit of MII MSSP Solution

Advance Threat Intel Feed

We Integrated Our Services third party threat intelligence feed

Threat Hunting Approach

MII SOC Using Proactive Security Monitoring Methodology To enhance security Analyst capability to Detect advance threat

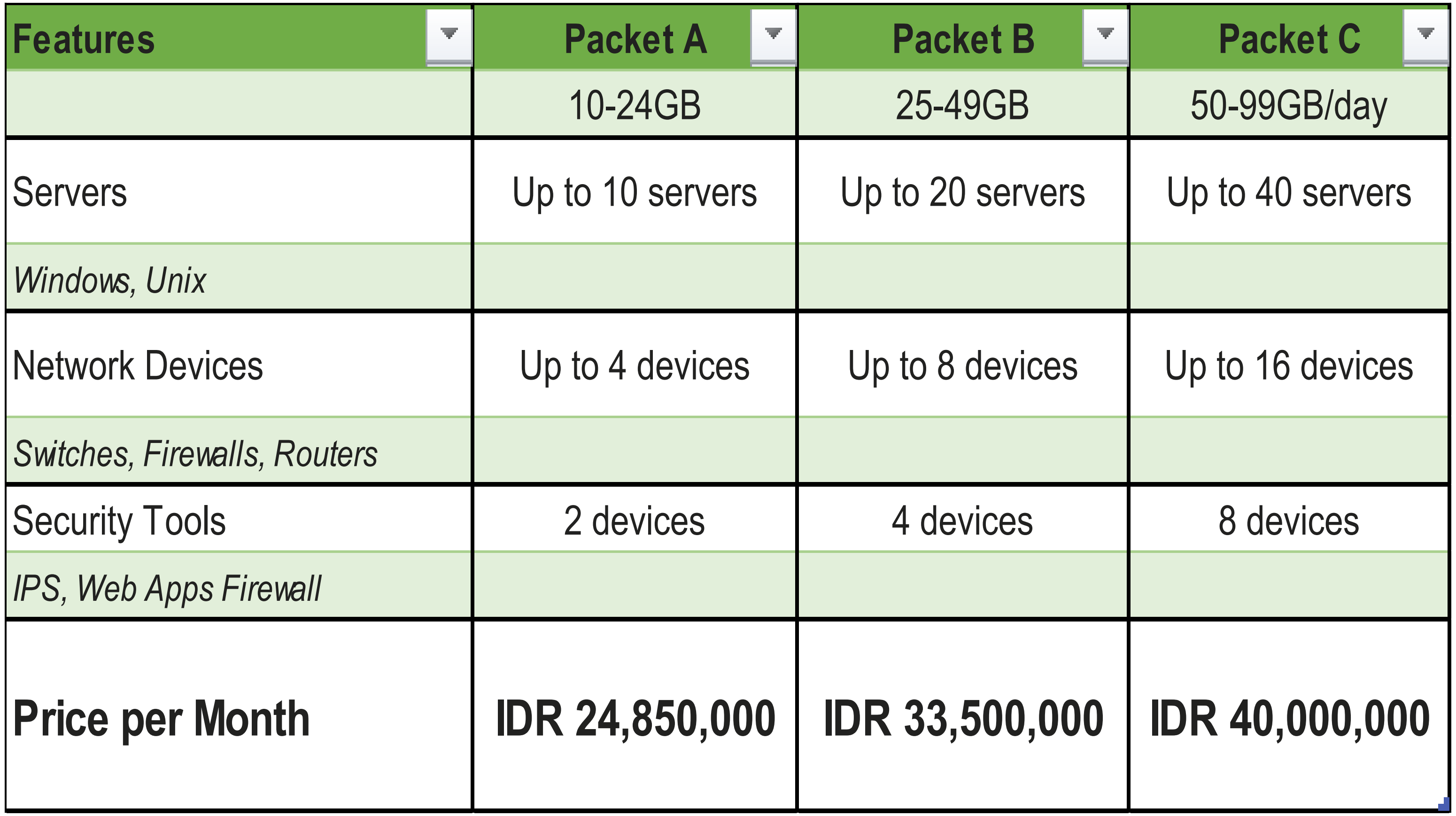
Bundled Security Services

Complete your security Visibility using our Bundled Security Service

Complete Security Policy and Procedure

We have pre-built in Security Policy And Procedure for Day-to-Day Activity

Packages include deployment



Features	Packet A	Packet B	Packet C
	10-24GB	25-49GB	50-99GB/day
Servers	Up to 10 servers	Up to 20 servers	Up to 40 servers
Windows, Unix			
Network Devices	Up to 4 devices	Up to 8 devices	Up to 16 devices
Switches, Firewalls, Routers			
Security Tools	2 devices	4 devices	8 devices
IPS, Web Apps Firewall			
Price per Month	**IDR 24,850,000**	**IDR 33,500,000**	**IDR 40,000,000**

All packages include:

- Provision Sentinel Services
- Configure Sentinel to ingest log (MII will configure on the sentinel part, customer configure from the device/server part)
- Configure out of the box rules from Sentinel
- Transfer knowledge - 1 day training
- Minimum 12-month contract
- **Exclude Azure Credit Subscription**

Scope of Work Service

MSSP Scope of Work

Deploy SIEM forwarder on Customer network to collect logs from Customer assets and provision Azure Sentinel Services

It should be noted that the data sources (logs) are always **stored on the Log Management Server located in Customer Data Centre, and never in our SOC facilities.**

Monitor, analyse, and detect potential security attack on **security devices, network devices, server, and workstation** that are configured as data sources to SIEM

Even though only 8x5 Office Hour Security Monitoring Services, our team will create rule to detect potential security attack, and automatically send to ticketing system, once the ticket generated, and the potential security attack is high and critical severity, our team can help to solve the problem immediately

Analyse network traffic going from/to the customer device(s).

- ✓ 24x7x365 Security Monitoring Services
- ✓ Vulnerability management Services
- ✓ Security Advisory Services
- ✓ Cutting Edge and Advance Technology
- ✓ Incident Response and Digital Forensic

MSSP Scope of Work

1. **Managed Security Monitoring**

   - **24x7x365 days Security Events Monitoring Service**
     - Deploy Forwarder on customer network to collect logs from customer assets.
     - It should be noted that the data sources (logs) are always **stored on the Log Collector Server located in Customer Data Centre, and never in our SOC facilities.**
     - MII will monitor, analyse, and detect potential security attack on **security devices, network devices, server, and workstation** that are configured as data sources to SIEM
     - Analyse network traffic going from/to the customer device(s).

MSSP Scope of Work

- Upon the detection of potential security incident (i.e. alarms), our SOC team will:
  - Perform a preliminary assessment on the situation,
  - Create an entry in the SOC ticketing system, and
  - Send notification to customer PIC via email or through our ticketing system .
- SOC team will then continue to investigate the potential incident, and send a full analysis along with the recommended action.
- Our ticketing system is used to track potential incident can be customized to fulfill specific customer format requirement. Customer can track ticket history from web interfaces ticketing system or customer can respond to each security ticket via email. Customer's email will be automatically stored in ticketing system as part of security ticket.

MSSP Scope of Work

2. Vulnerability Management Services

- Regular vulnerability assessment checking against customer’ s infrastructure, using industry standard tools with manual verification to reduce the rate of false-positives.
- Vulnerability Assessment will be conducted in **quarterly** and will be reported separately from MSS SOC Report

MSSP Scope of Work

3. Security Advisory Services

- Security advisory gives the latest security threat information regarding customer assets based on our threat intelligence database.
- The Security Analyst will provide recommendation and best practice actionable plan to mitigate or reduce risk

MSSP Scope of Work

4. Cutting Edge and Advanced Technology

- Azure Sentinel – cloud native SIEM technology
- Threat Intelligence Feed to Detect and Respond Immediately from latest information security threat
- Rich Correlation Rules from Vendor driven and fully customized by customer needs
- Adoption to Threat Hunting approach for advanced security analysis

MSSP Scope of Work

5. Incident Response and Digital Forensic Services

- **On Demand Services**

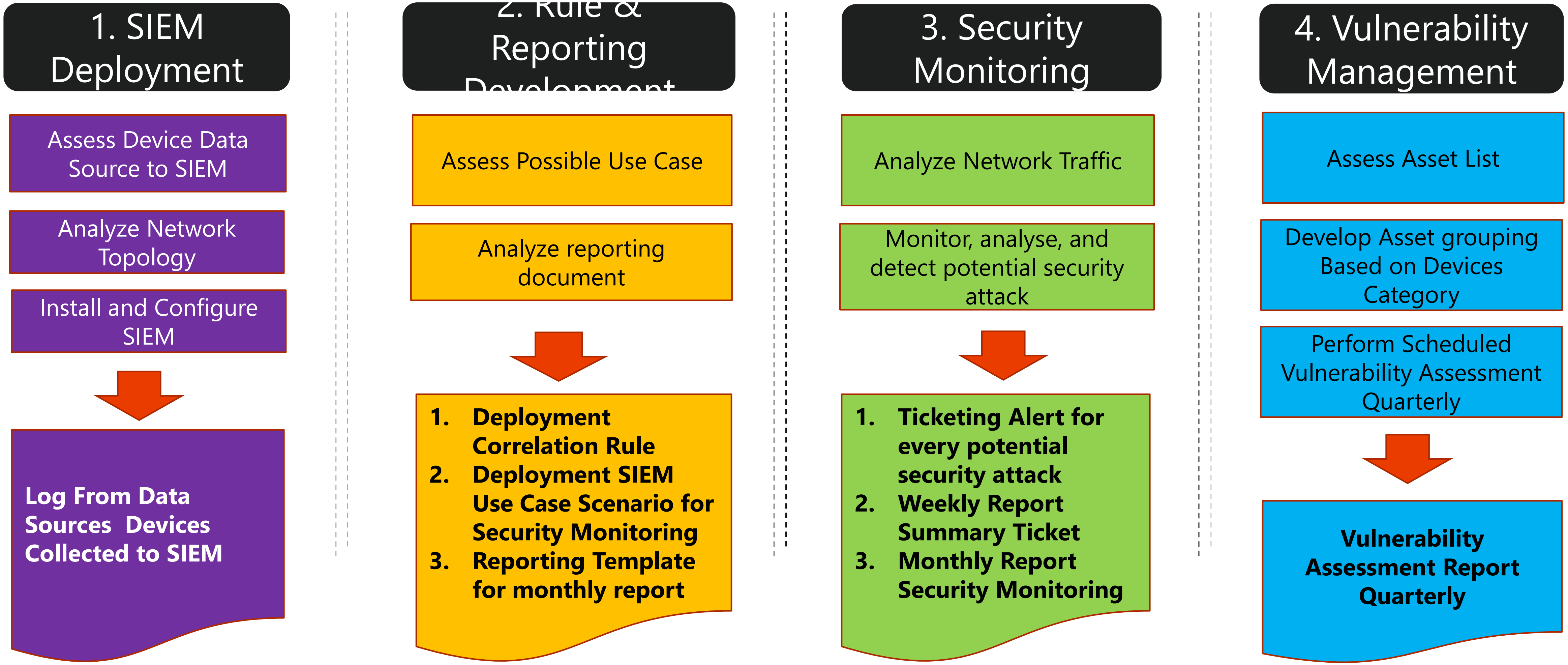
❖ Dedicated expert on incident responses to assist immediate respond and mitigation on security breach.

❖ Just-in-time expert assistance to minimise the impact of security breach

❖ Handle the situation in a way that limits damage and reduces recovery time

❖ Prevent future attacks/incidents by remediation process and **finding** the root cause for every incidents which occur in customer site.

Deliverables (1)



1. SIEM Deployment

Assess Device Data Source to SIEM

Analyze Network Topology

Install and Configure SIEM

Log From Data Sources Devices Collected to SIEM

2. Rule & Reporting Development

Assess Possible Use Case

Analyze reporting document

1. **Deployment Correlation Rule**
2. **Deployment SIEM Use Case Scenario for Security Monitoring**
3. **Reporting Template for monthly report**

3. Security Monitoring

Analyze Network Traffic

Monitor, analyse, and detect potential security attack

1. **Ticketing Alert for every potential security attack**
2. **Weekly Report Summary Ticket**
3. **Monthly Report Security Monitoring**

4. Vulnerability Management

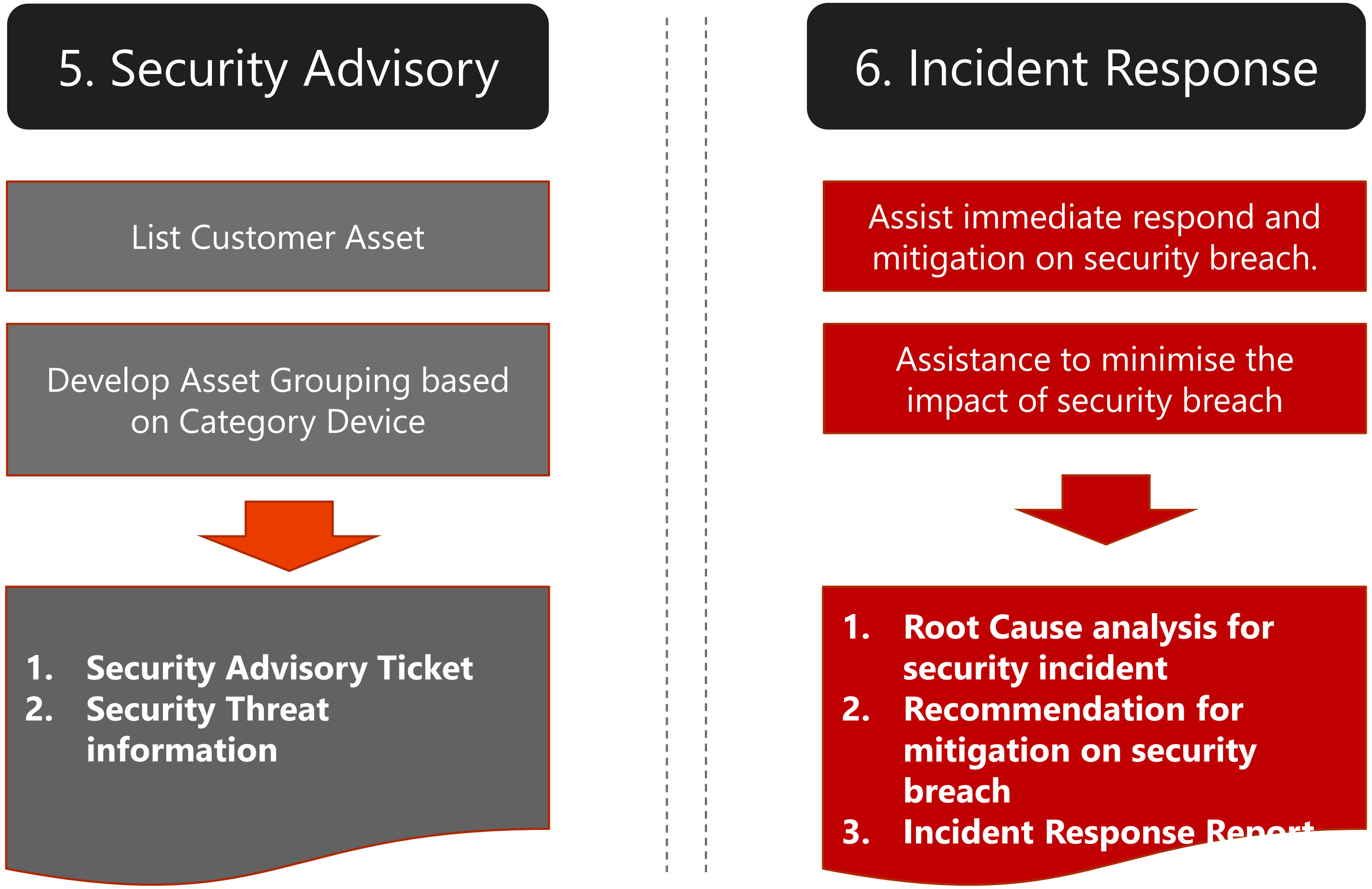
Assess Asset List

Develop Asset grouping Based on Devices Category

Perform Scheduled Vulnerability Assessment Quarterly

Vulnerability Assessment Report Quarterly

Deliverables (2)



5. Security Advisory

List Customer Asset

Develop Asset Grouping based on Category Device

1. **Security Advisory Ticket**
2. **Security Threat information**

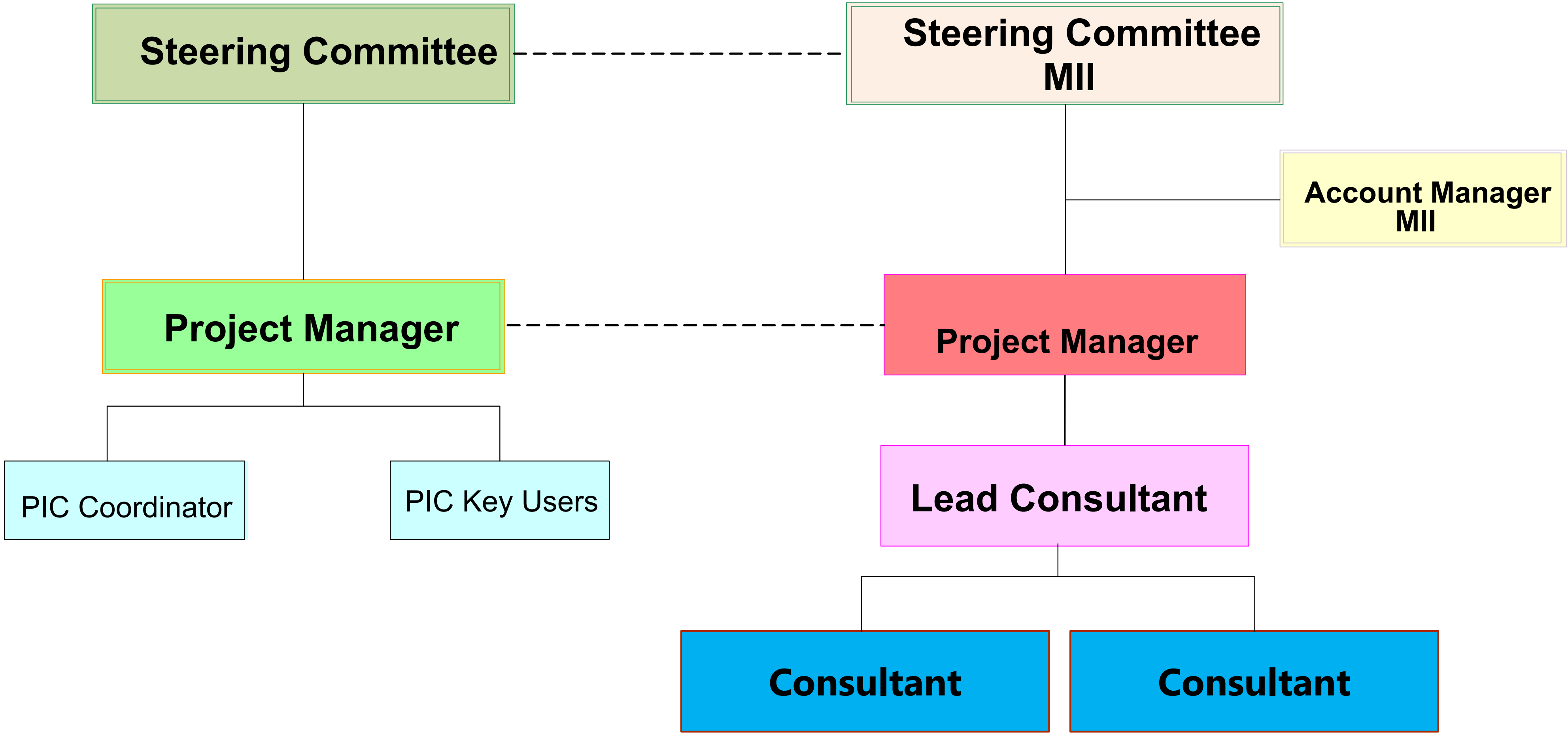
6. Incident Response

Assist immediate respond and mitigation on security breach.

Assistance to minimise the impact of security breach

1. **Root Cause analysis for security incident**
2. **Recommendation for mitigation on security breach**
3. **Incident Response Report**

Structure & Project Organization



Steering Committee

Steering Committee MII

Account Manager MII

Project Manager

Project Manager

PIC Coordinator

PIC Key Users

Lead Consultant

Consultant

Consultant

Winner
Microsoft Partner of the Year 2020

Indonesia

Thank You!

MITRA INTEGRASI INFORMATIKA

"World Class Business Technology Partner"

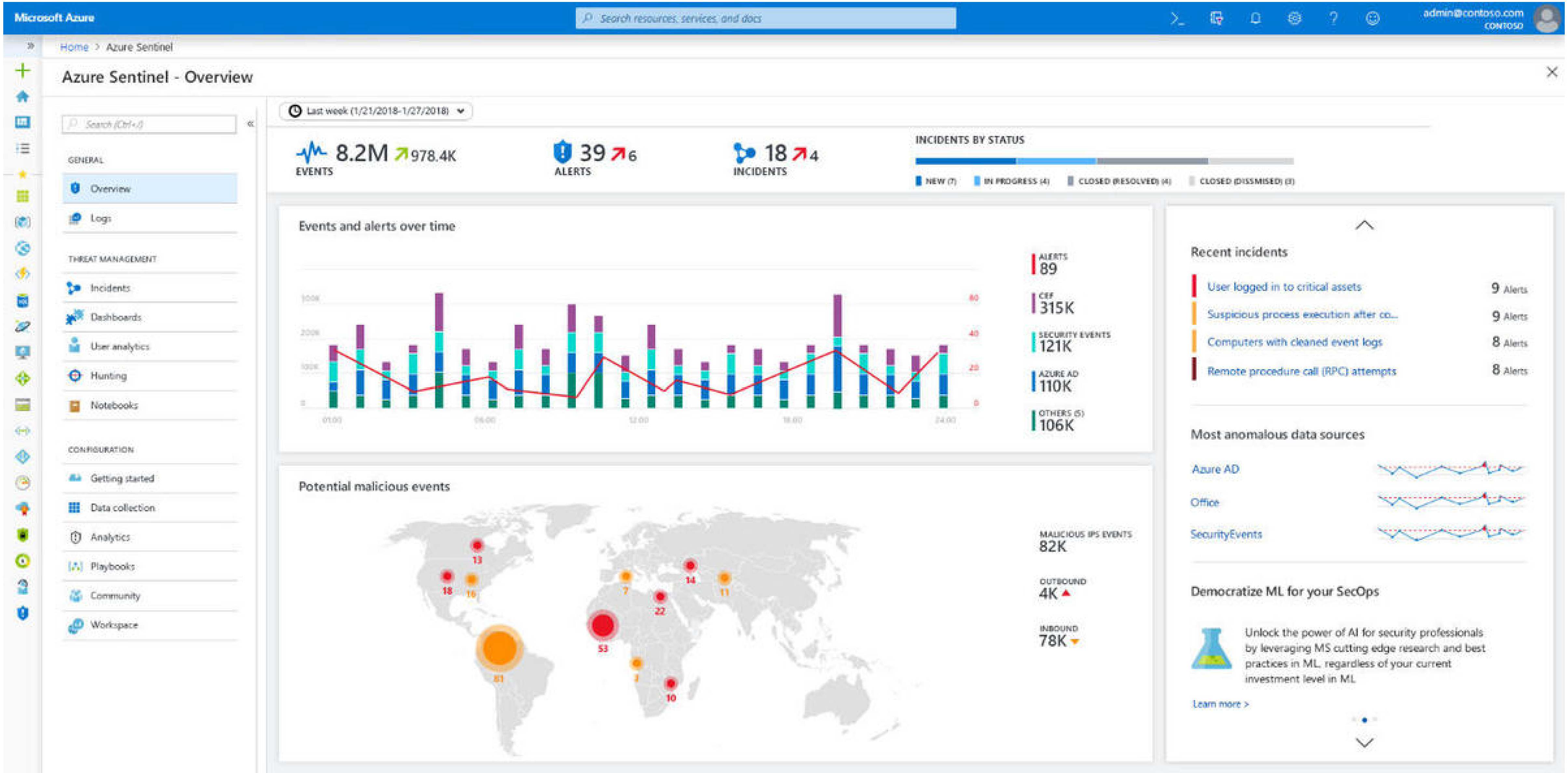
METRODATA

Member of METRODATA

www.mii.co.id

APL Tower 37th Fl.
Jl. Letjend. S. Parman Kav. 28, Jakarta 11470
Phone: (021) 2934 5777; Fax: (021) 2934 5700
Email: contact@mii.co.id

Intiland Tower Surabaya, 6th Floor, #2B
Jl. Panglima Sudirman Kav. 101-103, Surabaya 60271
Phone: (031) 5474217; Fax: (031) 5474 216
Email: MII.Surabaya@mii.co.id

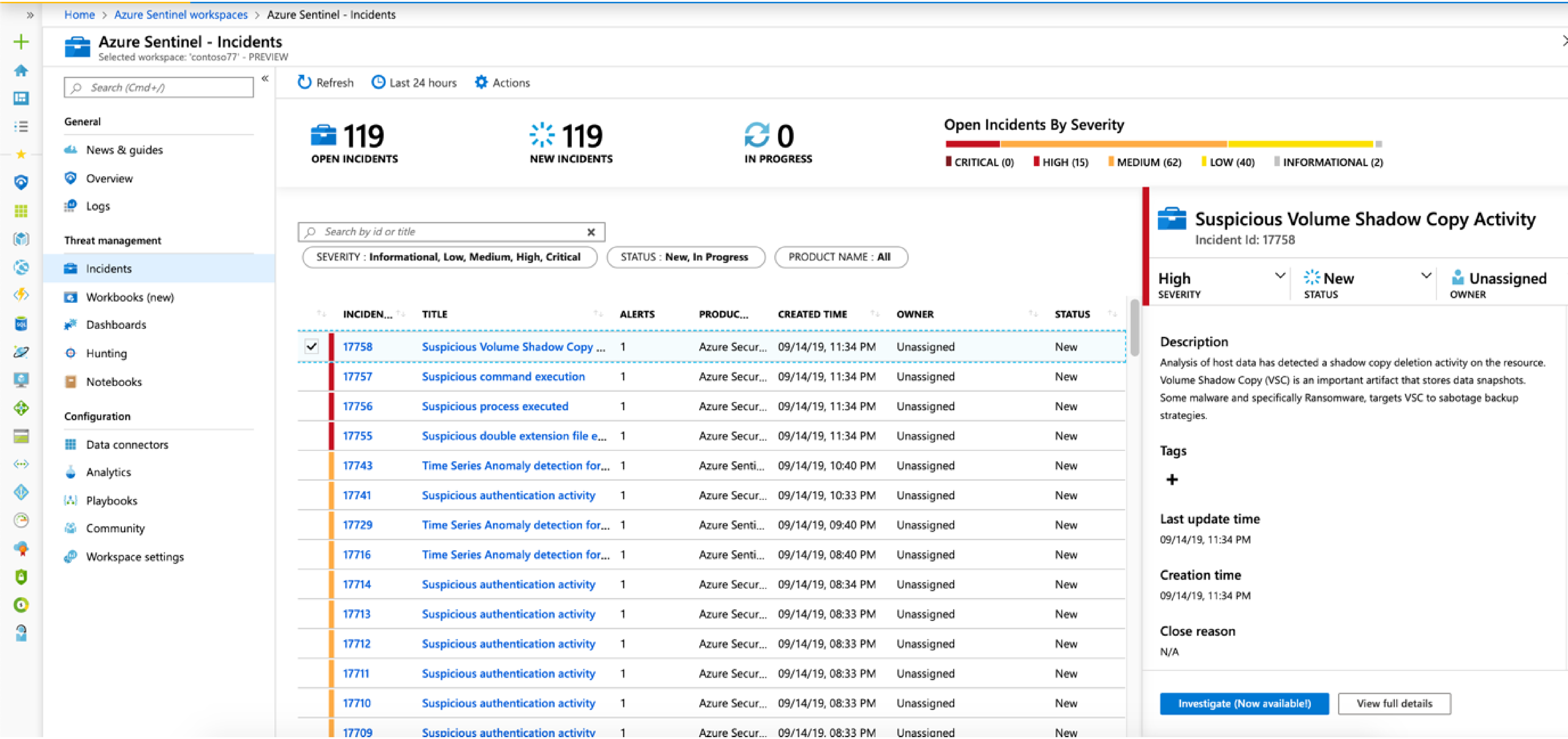


Recent incidents

User logged in to critical assets	9 Alerts
Suspicious process execution after co...	9 Alerts
Computers with cleaned event logs	8 Alerts
Remote procedure call (RPC) attempts	8 Alerts

Democratize ML for your SecOps

Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current investment level in ML



Home > Azure Sentinel workspaces > Azure Sentinel - Incidents

Azure Sentinel - Incidents

Selected workspace: 'contoso77' - PREVIEW

119 OPEN INCIDENTS

119 NEW INCIDENTS

0 IN PROGRESS

Open Incidents By Severity

CRITICAL (0) HIGH (15) MEDIUM (62) LOW (40) INFORMATIONAL (2)

SEVERITY : Informational, Low, Medium, High, Critical

STATUS : New, In Progress

PRODUCT NAME : All

	INCIDEN...	TITLE	ALERTS	PRODUC...	CREATED TIME	OWNER	STATUS
✓	17758	Suspicious Volume Shadow Copy ...	1	Azure Secur...	09/14/19, 11:34 PM	Unassigned	New
	17757	Suspicious command execution	1	Azure Secur...	09/14/19, 11:34 PM	Unassigned	New
	17756	Suspicious process executed	1	Azure Secur...	09/14/19, 11:34 PM	Unassigned	New
	17755	Suspicious double extension file e...	1	Azure Secur...	09/14/19, 11:34 PM	Unassigned	New
	17743	Time Series Anomaly detection for...	1	Azure Senti...	09/14/19, 10:40 PM	Unassigned	New
	17741	Suspicious authentication activity	1	Azure Secur...	09/14/19, 10:33 PM	Unassigned	New
	17729	Time Series Anomaly detection for...	1	Azure Senti...	09/14/19, 09:40 PM	Unassigned	New
	17716	Time Series Anomaly detection for...	1	Azure Senti...	09/14/19, 08:40 PM	Unassigned	New
	17714	Suspicious authentication activity	1	Azure Secur...	09/14/19, 08:34 PM	Unassigned	New
	17713	Suspicious authentication activity	1	Azure Secur...	09/14/19, 08:33 PM	Unassigned	New
	17712	Suspicious authentication activity	1	Azure Secur...	09/14/19, 08:33 PM	Unassigned	New
	17711	Suspicious authentication activity	1	Azure Secur...	09/14/19, 08:33 PM	Unassigned	New
	17710	Suspicious authentication activity	1	Azure Secur...	09/14/19, 08:33 PM	Unassigned	New
	17709	Suspicious authentication activity	1	Azure Secur...	09/14/19, 08:33 PM	Unassigned	New

Suspicious Volume Shadow Copy Activity

Incident Id: 17758

High SEVERITY | New STATUS | Unassigned OWNER

Description

Analysis of host data has detected a shadow copy deletion activity on the resource. Volume Shadow Copy (VSC) is an important artifact that stores data snapshots. Some malware and specifically Ransomware, targets VSC to sabotage backup strategies.

Tags

+

Last update time

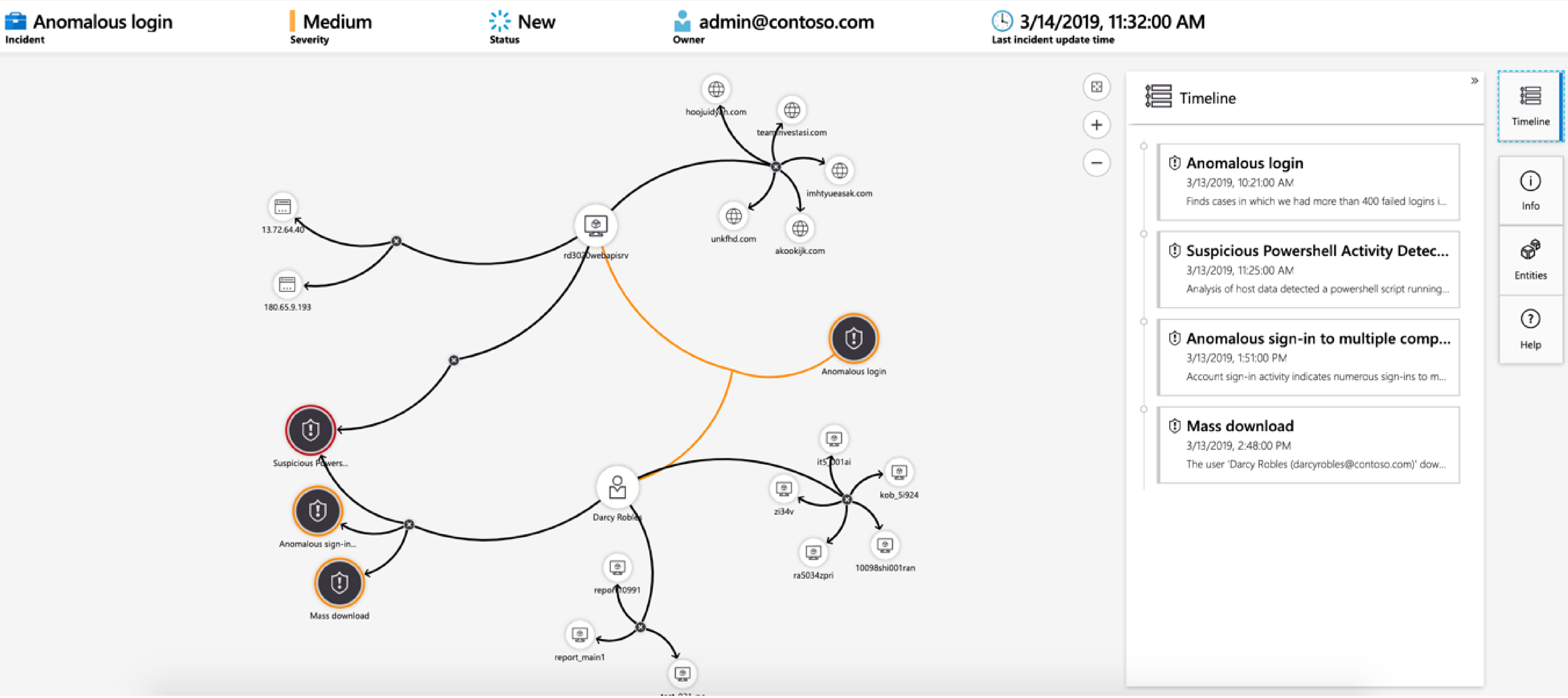
09/14/19, 11:34 PM

Creation time

09/14/19, 11:34 PM

Close reason

N/A



Anomalous login
Incident

Medium
Severity

New
Status

admin@contoso.com
Owner

3/14/2019, 11:32:00 AM
Last incident update time

Timeline

Anomalous login
3/13/2019, 10:21:00 AM
Finds cases in which we had more than 400 failed logins i...

Suspicious Powershell Activity Detec...
3/13/2019, 11:25:00 AM
Analysis of host data detected a powershell script running...

Anomalous sign-in to multiple comp...
3/13/2019, 1:51:00 PM
Account sign-in activity indicates numerous sign-ins to m...

Mass download
3/13/2019, 2:48:00 PM
The user 'Darcy Robles (darcyrobles@contoso.com)' dow...