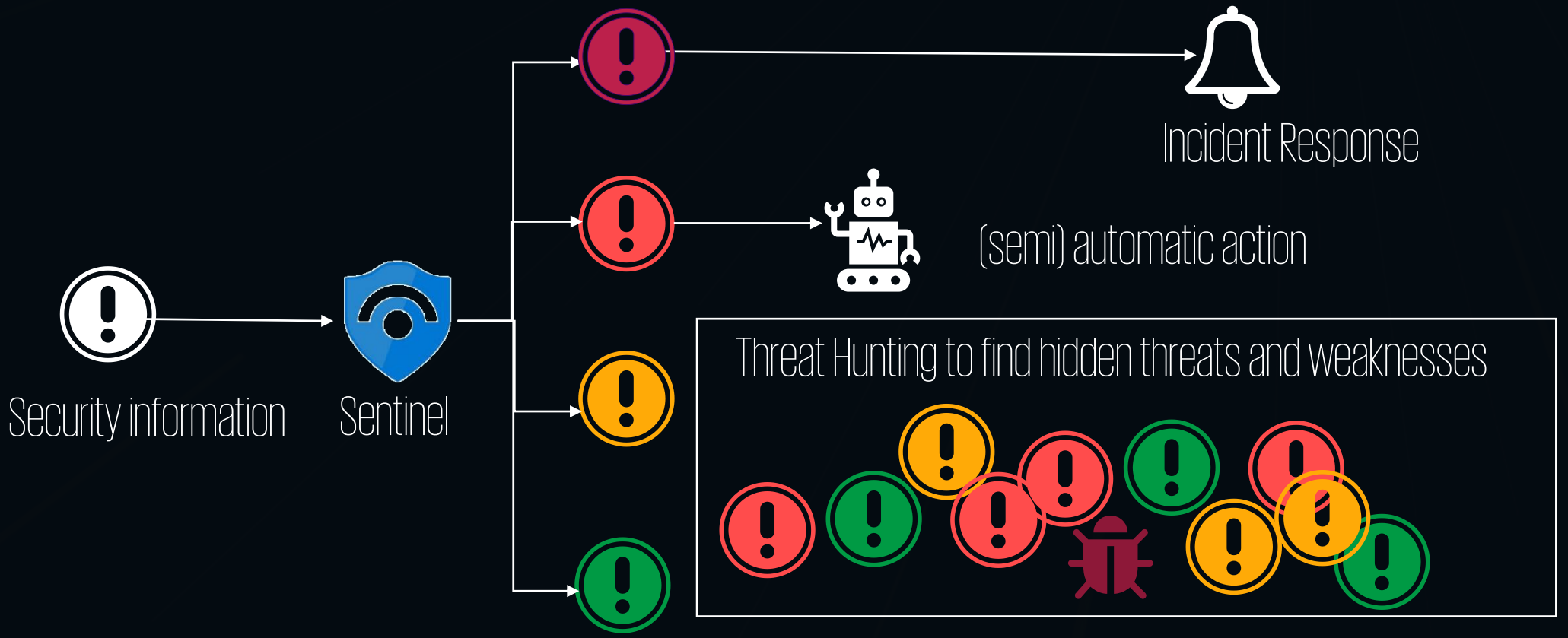
KPMG

Simplifying Security Ops on Azure Sentinel - Managed Threat Hunting

Managed Threat Hunting on Azure Sentinel at a glance...



Managed Threat Hunting vs Traditional SOC

	Managed Threat Hunting KPMG	Traditional SOC MSSP
Real-time alert triage	Review alerts in bulk during threat hunt (from weekly to yearly)	Review alerts within stipulated SLA on 24/7 basis
Automatic high risk alert handling on 24/7 basis	Yes, supported through full-fledged incident response services – based on previous defense tuning	Depending on range of incident response services
Response to incidents	Yes	Depending on range of incident response services
Detection of threats that have evaded front line defenses	Yes	Depending on range of threat detection services
Alerts reviewed by senior analysts	Yes	Most alerts reviewed by level 1 analysts

This is how we do it on Azure Sentinel...

Transforming the security operations ecosystem with Azure Sentinel and KPMG services

ASSESS

- Review of existing implementation
- Purple team/red team in the cloud

DESIGN

Develop the SecOps Transformation program, including

- Simplified architecture
- Migration from legacy security tooling
- Requirements (log sources, use cases)
- Integration with existing legacy security tooling

BUILD

- Ready to go playbooks for common use cases (O365, Phishing, Defender)
- Create custom playbooks
- Integration with ticketing systems
- Integration with other solutions
- AI/ML queries/models to detect
- Creation of connectors
- Integration of automated process
- Integrate into legacy SOC processes and procedures

OPERATE

- Training to use the solution
- On-call incident response
- Tuning of alerts to a point only L3 required
- Managed operations
- Managed threat hunting

KPMG

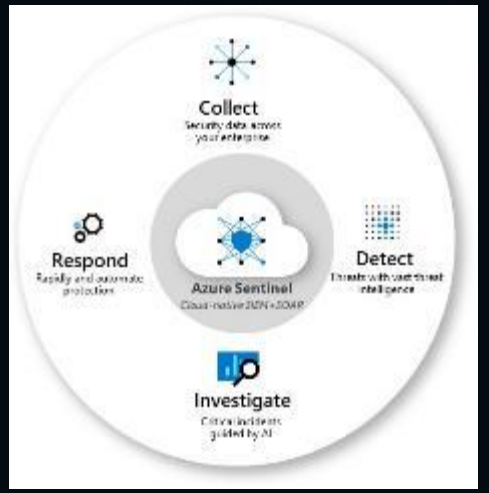
Cyber Defense Framework

The framework focuses on the key security operations capabilities within Identify, Protect, Detect, Respond and Recover to provide an understanding of the current and desired maturity level using identified gaps to establish a program towards mature and advanced Cyber Defense.

Microsoft

Azure Sentinel

Azure Sentinel is a cloud-based SIEM-SOAR solution offering 'limitless cloud speed and scale' combined with AI and built in orchestration and automation of common tasks. Native integration with Microsoft products such as O365 as well as other cloud solutions and on premise logs.

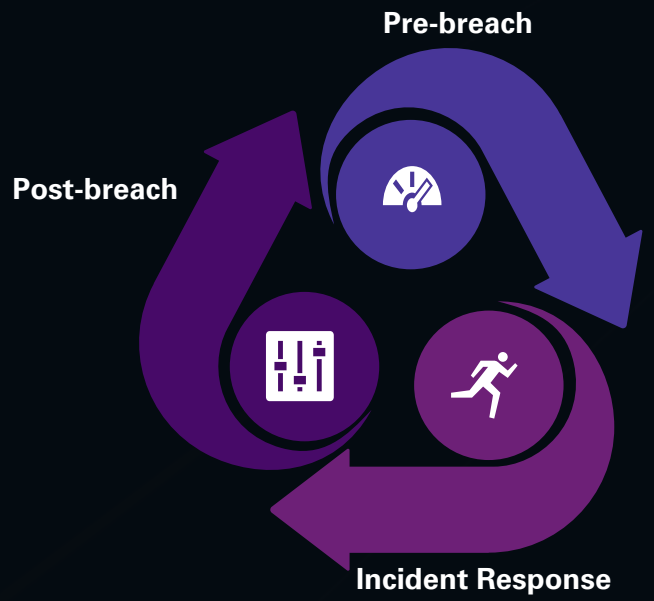


Our approach

	PREPARATION & DEPLOYMENT	DATA COLLECTION	MANAGED THREAT HUNTING	REPORTING	REMEDIATION
PHASES					
KEY STEPS	▪ Define the scope and threat hunting techniques (eg. KQL) ▪ Deploy and tailor the threat hunting rules	▪ Collect real time metadata from Azure Sentinel and analyse in real time ▪ Threat mapping with MITRE ATT&CK framework	▪ Undertake threat hunting, investigate high risk and anomalous activities ▪ Perform efficient correlation and analysis of events	▪ Perform reporting, alert on high risk findings and identify root causes	▪ Perform remediation and mitigation on incident ▪ Internal knowledge sharing for user awareness ▪ 24/7 cyber incident response plan

2 – 4 weeks

Giving peace of mind with 24/7 cyber response services



Pre-breach

- Discuss incident response requirements and approach
- Provide early insights and regular knowledge transfer

Incident response

- Identify scope and assess severity of the incident
- Contain the event and recovery to a known operational state

Post-breach

- Conclude investigation and present recommendations
- Identify areas of risk and provide roadmap for future mitigation

Leading Medical Device Manufacturer

Client situation

Experienced a cyber incident and KPMG was engaged as incident responders

- Existing LogRhythm Security Incident Event Management (SIEM) platform had performance and implementation issues - could not contain and eradicate the incident
- Too many unmanaged admin access accounts

How we have helped

- Configured Azure Sentinel to set rules/alerts and detect unusual admin access
- Provided a blueprint and technical assistance to move all critical data into Sentinel in 48hours
- Providing ongoing cyber response service
- Expanding conversations into other security hotspots with potential tech implementation

Other selected credentials

Financial Services

Performed threat hunting for 100 servers and endpoints to trace a data leakage that was reported to have been traded on the Darknet

Performed threat hunting to review 3rd party outsourcing risk for a system that contains client information and is managed by vendors

Oil, Gas & Energy

Performed threat hunting leveraging Azure Sentinel as Proof of Concept. We set up threat hunting queries, dashboard and alerts based on the MITRE ATT&CK matrix and tactics used by the attackers targeting clients in the same industry and provided recommendations based on agreed success metrics for future enhancements.

Implemented Azure Sentinel integrated with Defender for IoT and Azure Security Centre to provide client with the appropriate levels of visibility for potential security events on their IT and OT networks as Proof of Concept.


Here's our OOTB PoC offering...
Develop PoC project plan, data sources to be onboarded on Azure Sentinel and success metrics
Develop high-level solution architecture and acceptance criteria document
Activate Azure Sentinel service in client's Azure tenant
Configure log forwarders and activate built-in Sentinel security dashboards
Configure up to two additional, custom dashboards
Integrate Sentinel alerts with client's existing incident management system (if such exists)
Provide a one-off training
Conduct a one-off "system health check" after 30 days from implementation acceptance

Thank you!

Eddie Toh
M: 8112 0981
E: eddietoh@kpmg.com.sg

Sally Tao
M: 9636 7790
E: sallytao@kpmg.com.sg