EY Application Threat Detection and Response Service (TDR) for SAP

The next-gen security operations services of EY

Building a better working world

Cybercriminals are becoming more persistent and are deploying sophisticated attack strategies to target "crown jewel" applications like: SAP

- As one of the leading solution providers for applications that manage business processes, SAP is the custodian of massive amounts of sensitive business-critical data in many of the biggest organizations in the world. However, protecting these systems is notoriously challenging.
- Therefore, it is imperative that security operations centers (SOCs) keep pace by focusing on priority threats and leveraging the detection and response capabilities available to them to protect SAP applications.
- The complex nature of SAP ecosystems means threats can emerge across multiple systems and applications, requiring ongoing monitoring, advanced threat detection and cross-correlation capabilities.
- However, since these ecosystems are so unique and complex, it's crucial to monitor SAP effectively for threats and incorporate as part of ongoing security operations.

EY Application TDR Service for SAP solution benefits:

- Visibility: Quickly gain visibility over your SAP ecosystem, and combine with integrated, on-premises data sources to achieve a holistic view
- Advanced capability: Apply the capabilities of Microsoft's cloud-scale security analytics to adopt a threat-centric approach to detection and response for SAP ecosystems
- Tight native security information and event management (SIEM) integration: Cut through the complexity of SAP landscape to provide continuous threat detection and analytics for SAP systems hosted on Azure, other clouds, or on-premises
- Deep SAP insights: Gain deep insights into SAP transactional activities, databases, interfaces, infrastructure through the rich SAP data sources, i.e., security audit log, job log, spool log, Internet Communication Manager (ICM) log, change documents and more
- Correlation of SAP activity with other signals: Accurately detect SAP threats by cross-correlating across all your data sources
- Customization as per needs: Build your own detections to monitor your critical SAP business data

EY Application TDR Service for SAP supported by Microsoft

EY Application TDR Service for SAP is an advanced cyber intelligence and automation platform for innovation that can assist you to automatically discover "advanced-attack patterns" and proactively strengthen your protection capability. This will include being able to utilize our security professionals who will not only monitor your SAP environment for security threats 24x7, but also will work with your team to customize and improvize the Microsoft Sentinel platform continuously to best fit your SAP environment and use cases.
This customization includes, integrating and onboarding standard and customized logs, designing and creating customized dashboards or workbooks, and tuning customized alerts or rules or analytics to help your company manage SAP cyber risks.

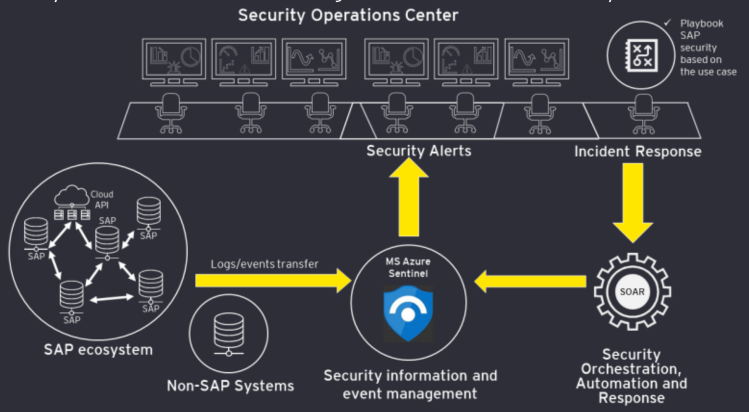
Service offerings:

- Deliver broad 24x7 Microsoft Sentinel monitoring and Uplift-as-a-Service for SAP in a mix of both off-shore and on-shore modes
- Provide skilled platform and threat professionals (including SAP) who will be dedicated to your business
- Provide Incident Response (IR) professionals with capabilities to bring in IR and forensics expertise globally
- Offer expertise in SAP Security that is related to monitoring of threats and vulnerability in SAP environments

Key functionality !

EY Cyber Managed Service:

- Skilled SAP Security/Basis resource as member of the SOC/IR team


Security Operations Center
✓ Playbook SAP security based on the use case
Security Alerts
Incident Response
Cloud API
SAP
SAP
SAP
SAP
SAP
SAP ecosystem
Logs/events transfer
Non-SAP Systems
MS Azure Sentinel
Security information and event management
SOAR
Security Orchestration, Automation and Response

EY Application TDR Service for SAP

Collection	Detection	Investigation	Response
• NetWeaver data connector • SAP infrastructure data connector • In-built connectors • REST API, Syslog • Common event format (CEF) integration	• Built-in detections • Artificial intelligence (AI) and Machine Learning (ML) analytics • Threat modeling • Custom queries • Threat intelligence • Threat hunting	• Unified view • Incident alerting • Investigation UI • Custom workbooks	• Orchestration • Automation • Logic Apps • Service integration

EY Application TDR Service for SAP solution in action

A leading global hearing-aid equipment manufacturing and healthcare services organization headquartered in Singapore, engaged EY teams to design, build and run a next-generation SOC.

- EY team deployed, expanded, customized and managed a Microsoft Sentinel instance that was tailored to the business' specific needs.
- The solution demonstrated the seamless integration across the full Microsoft portfolio, including Microsoft Defender for Endpoint (MDE), Microsoft Office 365 and others.
- The solution included customized workbooks based on critical assets, users and high-risk watchlists.

Client challenges

- The client was struggling to detect and respond to advanced threats across the IT environment, spread across geographies.
- The client's lack of visibility on 'crown jewels' was leading to several security incidents.
- Recent mergers of companies also increased regulatory rigor which in turn was adding to governance complexity.
- The client wanted a 24x7 managed services along with a flexible, cost-effective, scalable and customizable solution that could integrate with the existing technology ecosystems which are Microsoft platform-based and other controls deployed.

Client benefits

- Demonstrate an efficient SIEM with 24x7 threat monitoring and proactive threat hunting services
- Show that the investment made in the Microsoft suite can be leveraged to provide scalable leading-edge security at a reasonable cost and quick time-to-value via right sizing and simple cost structure

EY and Microsoft: Work Better. Achieve More.

Every day, throughout the world, businesses, governments, and capital markets rely on EY business ingenuity and the power of Microsoft technology to solve the most challenging global issues.

EY and Microsoft bring a compelling formula to spark the potential of the cloud and unlock the power of data. We solve our clients' most challenging issues by blending trusted industry expertise with innovative cloud technology. Our strategic relationship draws on decades of success developing visionary solutions that provide lasting value.

Together, we empower organizations to create exceptional experiences that help the world work better and achieve more.

For more information, visit: ey.com/Microsoft.

EY Microsoft Confidential- Not for external use

For more information, please contact:

EY contact:

Darren Simpson

Partner
EY Cybersecurity
Ernst & Young APAC
darren.simpson@au.ey.com

Krishna Balakrishnan

Partner
EY Cybersecurity
Ernst & Young APAC
krishna.balakrishnan@sg.ey.com

Nadine Mueller

Partner
EY Cybersecurity
Ernst & Young Germany
nadine.mueller@de.ey.com

Eric YK Lam

Partner
EY Cybersecurity
Ernst & Young APAC
eric.yk.lam@sg.ey.com

Chang Boon Tee

Client Executive Director
EY Cybersecurity
Ernst & Young Singapore
boon.tee.chang@sg.ey.com

Microsoft contact:

Sachin Rathi

Director, Partner Management - Security Solutions & Strategic Initiatives
Microsoft Corporation
sachin.rathi@microsoft.com

Jodi Lustgarten

Microsoft Alliance Director
Microsoft Corporation
jodise@microsoft.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data, and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

US SCORE no.
Document reference no.

EYG no. 007127-22Gbl

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com