EY point of view

SOC-in-the-box

Building a better working world

EY's SOC-in-the-box provides a centralized, robust and simple way to quickly gather, analyze and secure massive amounts of data from multiple sources to confirm security and business resiliency.

Security Operations Centers (SOCs) have various technologies that cause tool fatigue impacting decision-making, increasing the mean time to defend (MTTD) and mean time to response (MTTR). With the EY SOC-in-the-box, tools can be consolidated across enterprises and redundancies can be minimized. With all the information available in one dashboard, operational efficiency and mitigating expenses can be increased.

Key client challenges

Decentralization	Compliance	Cyber threat
Increased volume of alerts due to disparate technology stack results in the higher time to detection and time to mitigation.	As legal and regulatory are frequently updated, Management's controls can fall behind, posing a potential security threats and regulation fees.	When threats are detected and manual triaging is performed, there is an increased opportunity for the threat to spread throughout the company. There is also a potential for human error, correlating across disparate data sources to build a risk-based framework to define risk scoring.

SOC-in-the-box industry offerings and use cases

Splunk

Security monitoring

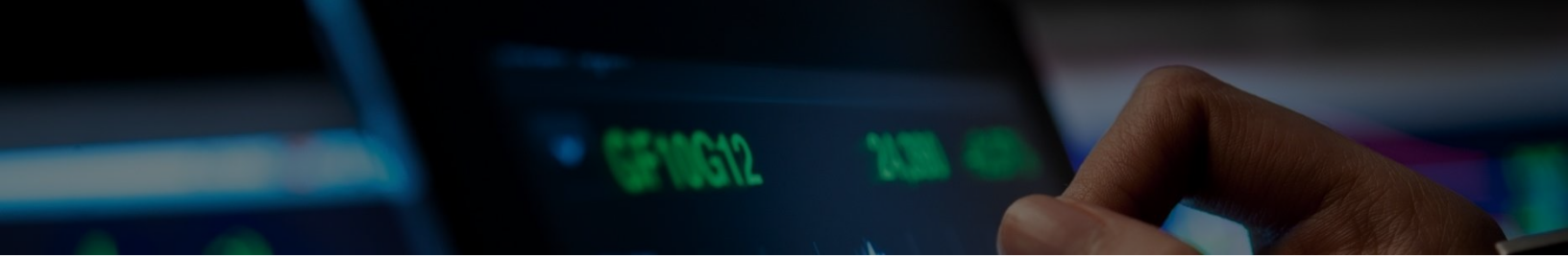
- Integrations and monitoring with all available threat feeds
- Real-time data aggregation
- Views for SOC manager, Chief Information Security Officer (CISO), SOC analyst and more
- Holistic overview of security posture

Compliance

- Compliance reporting (Payment Card Industry (PCI), National Institute of Standards and Technology (NIST) and MITRE)
- Single point of view for monitoring compliance in real time

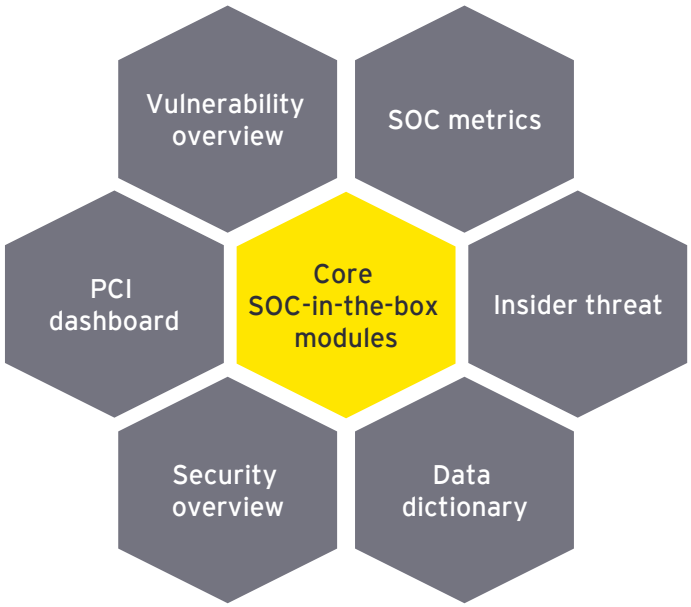
Threat detection

- Advance threat and insider threats proactively identified
- Complete Security Information and Event Management (SIEM) management
- Threat assessment and planning
- Advanced intelligence gathering
- Cloud monitoring



How does SOC-in-the-box solve challenges organizations face?

EY SOC-in-the-box aims to minimize redundancies and provide a consolidated view of the organization's cyber risk posture across the cyber verticals. Deploying EY's SOC-in-the-box can help quickly identify gaps to prioritize development needs, improving maturity by enabling data-driven decision-making.



Additional capabilities

1. Risk-based monitoring
2. Enrich alerts using external intel feeds
3. Track the path of the packet
4. Automate the threat intel process

Implementation approach

Design	Configure	Enhance
1. Perform current-state analysis. 2. Gather and prioritize requirements. 3. Develop a roadmap for deployment.	1. Align data sources to correlation searches. 2. Enable dashboards and searches.	1. Tune searches to improve efficacy. 2. Map to the standardized framework. 3. Identify gaps in coverage for development.

Ernst and Young LLP contacts

Suzanne Hall
Principal
Technology Consulting
suzanne.hall@ey.com

Kanitha Sar
Senior Manager
Cyber Alliance Business Development Lead
kanitha.sar@ey.com

Tony Pierce
Senior Manager
Americas SIEM Lead
tony.d.pierce@ey.com

Robb Mayeski
Senior Manager
US SOAR Delivery Lead
robb.b.mayeski@ey.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.

SOCRE no. 008860-21Gbl
ED None