Cyber innovation and engineering SOC-in-the-box

Innovations to enable a single pane of glass view for security operations through a security by design approach

Key message

Security Operation Centers have various technologies that cause tool fatigue impacting decision-making and resulting in increased MTTD and MTTR. Consolidate the tools across the enterprise via the EY SOC-in-the-Box to minimize redundancies and deliver a single pane of glass, improving operational efficiency and mitigating expenses.

Challenges

Volume of security alerts

Increased volume of alerts due to disparate technology stack result in higher time to detection and time to mitigation

Tool fatigue

Gathering relevant information requires analysts to pivot across various security tools

Legal and regulatory compliance

Legal and regulatory requirement compliance limits the time the SOC team has for mitigating potential security threats

Lack of contextual intelligence

Analysts need to gather threat details due to the lack of contextual information in alerts

Process inefficiencies

Manually triaging security threats increases inefficiencies and potential for human error

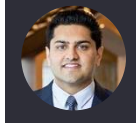
SOC-in-the-Box - Features

- Reduce alert fatigue and improve the time to detection and the time to mitigation through a single pane of glass view
- Ensure every role is mapped to a specific view using data as a differentiator providing essential compliance and risk exposure information across the cyber terrain
- Provide contextual information to increase analyst efficiency by enriching alerts using external intel feeds
- Empower executives to fast track audit completions by providing real-time tracking of compliance
- Focus on the path of the packet in the network layer to reduce inefficiencies and potential errors during the remediation process across your threat landscape
- Automate the threat intel process by integrating external threat intelligence enriching the events and enabling data driven decision-making to remediate threats

Ernst & Young LLP cybersecurity contacts

Kaushal J Patel
Managing Director
Technology Consulting

Tony Pierce
Senior Manager
Innovation Lead



Rupak Pandya
Senior Manager
US SIEM Delivery Lead

Robb B Mayeski
Senior Manager
US SOAR Delivery Lead

Implementation approach

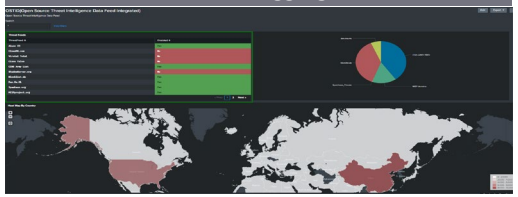
Design	Configure	Automate
1. Determine requirements	1. Enrich data feeds	1. Streamline process
2. Analyze data sets	2. Enable detections	2. Implement automation

Value provided

Executive overview

Incident management

Threat intel aggregation



EY | Assurance | Tax | Strategy and Transactions | Consulting