

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

1. Determine requirements
2. Analyze data sets

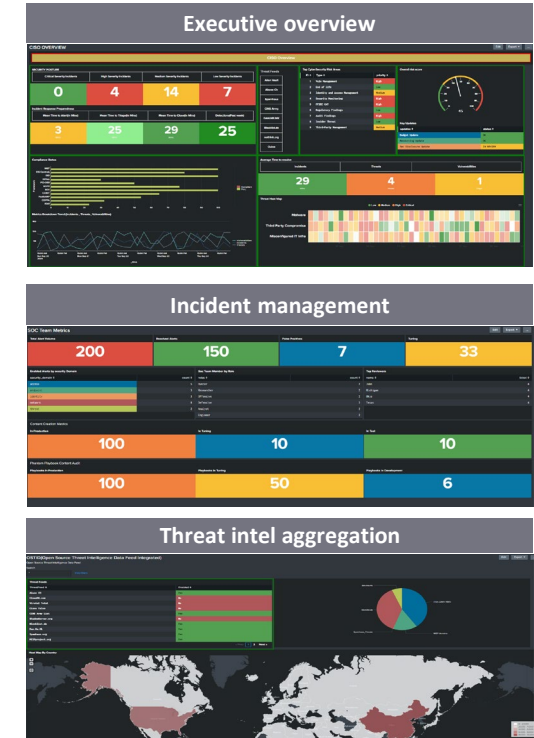
Configure

1. Enrich data feeds
2. Enable detections

Automate

1. Streamline process
2. Implement automation

Value provided



EY | Assurance | Tax | Strategy and Transactions | Consulting

About EY
EY is a global leader in assurance, tax, strategy, transaction and consulting services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

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. 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.

© 2020 Ernst & Young LLP.

All Rights Reserved.
US SCORE no. 10645-201US
2009-3596760
ey.com