

SIEM methodology and services



Tony D Pierce Senior Manager Ernst & Young LLP tony.d.pierce@ey.com +1 404 817 4419



Rupak Pandya Senior Manager **Ernst & Young LLP** rupak.pandya@ey.com +1 206 262 7197

EY SIEM service

Improve response time to better manage costs and drive the maximum value out of your security information and event management (SIEM) investment. EY SIEM service focuses on providing data visibility to the security infrastructure within organizations to help recognize and react to potential threats efficiently. To build a more mature SIEM capability, we help implement and support a variety of SIEM tools, reducing the cost of incidents by increasing the speed of detection and remediation.

Key challenges

Eighty percent of boards are not confident in their organization's cyber attack mitigation measures.1

Only 12% of organizations describe their analytics as "leading."²

Organizations struggle to optimize their security tools to maximize ROI

Methodology Assess . Design . Configure Operationalize . Enhance

around the globe

Health check Advance the health and scalability of your SIEM environment Review SIEM investment issues Develop baseline metrics and dashboards Propose recommendations to

Transformation

- Establish a framework to help identify
- maximize the capability
- Provide leading practices for enhanced future state

Evolve your current SIEM implementation

- 1. Understand the current SIEM implementation
- 2. Develop a strategy to enhance the current SIEM capability
- Configure changes to SIEM deployment
- Define use case maturity
- 5. Tune and automate alerting

Migration

Replace your current SIEM technology

1. Understand the enterprise technology

4. Normalize fields and implement data

5. Integrate with case management

2. Gather business and functional

Configure SIEM solution

environment

requirements

solution

Implement high return-on-investment use cases

Use case development

- 1. Review existing use case implementation
- 2. Map use case coverage to standard SIEM maturity framework
- Determine use cases to close gaps identified
- 4. Implement use cases
- 5. Tune use case logic

Why Ernst & Young LLP?

- Alliance and ecosystem relationships
- Proven methodology
- Improve cost management
- Sector-focused innovation
- Unique accelerators

Confirm your SIEM environment's stability and scalability

Identify gaps in your deployment to mature your SIEM and comply with industry standards

Identify an approach to remediate gaps in the current SIEM implementation

- Improve utilization of SIEM capabilities to maximize ROI
- Accelerate implementation of the new technology to streamline transition process
- Enhance deployment architecture to mitigate costs
- Mature the SIEM capability by enhancing processes and content
- Prioritize use case development based on standardized frameworks

Improve your SIEM capability by leveraging EY global experience and industry knowledge

Value provided

Qualified 65

Industry leading certification

Reduction in investigation time

ectors Retail Energy Insurance

Life Sciences Media and Entertainment

Financial Services Telecommunication EY use case library

1. "Cybersecurity: How firms can protect, optimize and enable," EY website, 22 November 2018.

2. "Why is the best digital strategy a human one?" EY website, 15 May 2018.

EY | Assurance | Tax | Strategy and Transactions | Consulting

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 bette 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