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.

Why Ernst & Young LLP?

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

Methodology

1. **Assess**
2. **Design**
3. **Configure**
4. **Operationalize**
5. **Enhance**

100+

Splunk **trained technicians** around the globe

Health check	Transformation	Migration	Use case development
Advance the health and scalability of your SIEM environment	Evolve your current SIEM implementation	Replace your current SIEM technology	Implement high return-on-investment use cases
1. Review SIEM investment 2. Establish a framework to help identify issues 3. Develop baseline metrics and dashboards 4. Propose recommendations to maximize the capability 5. Provide leading practices for enhanced future state	1. Understand the current SIEM implementation 2. Develop a strategy to enhance the current SIEM capability 3. Configure changes to SIEM deployment 4. Define use case maturity 5. Tune and automate alerting	1. Understand the enterprise technology environment 2. Gather business and functional requirements 3. Configure SIEM solution 4. Normalize fields and implement data models 5. Integrate with case management solution	1. Review existing use case implementation 2. Map use case coverage to standard SIEM maturity framework 3. Determine use cases to close gaps identified 4. Implement use cases 5. Tune use case logic
Value provided			
• 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

Qualified **65** Industry leading certification

70%-90% Reduction in investigation time

Sectors
Retail
Energy
Insurance
Life Sciences
Media and Entertainment
Financial Services
Telecommunication

300+ 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