EY point of view

## Splunk for healthcare

EY
Building a better working world

EY's SIEM service addresses our clients' cyber security challenges and concerns by providing the experienced and knowledgeable subject matter resources (SMRs) and technical capabilities that our clients need.

The healthcare industry is experiencing challenges in normalizing data and meeting compliance requirements as patient needs change, and data volume exponentially increases scale. The EY solution provides a more personalized patient experience and helps healthcare organizations reduce overall costs and operational inefficiencies with a data-driven approach.

By leveraging the EY solution to use data to make informed decisions, organizations will not only meet compliance requirements but also improve their overall operational efficiency.

Business challenges faced in the healthcare industry

1 Provide centralized log collection and retention based on compliance and security requirements.

2 Provide the ability for analysts to search and analyze events of interest to identify issues in the environment and report suspicious activity.

3 Provide rule-based real-time event correlation to detect potential threats more quickly.
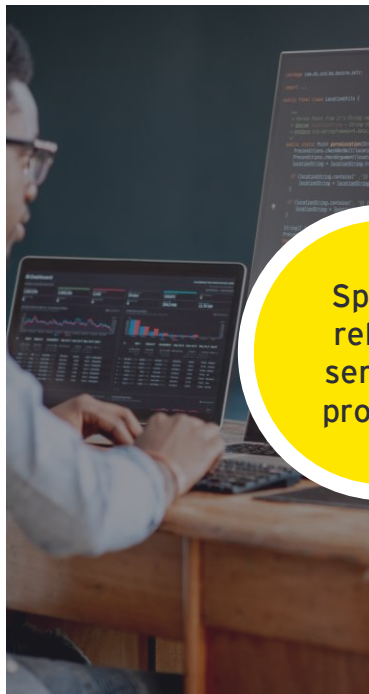
Splunk-related services provided

- Remote patient management
- Cloud migration
- Infrastructure performance monitoring

Methodology

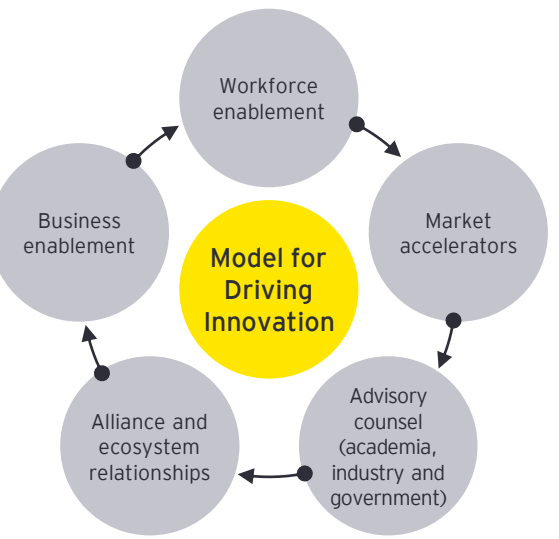| Assess	Design	Configure	Operationalize	Enhance
Understand the current state.	Develop an implementation approach.	Implement and configure technology.	Enable Security Operations Center (SOC) teams to respond to alerts.	Improve efficiency and performance.

Remote Patient Management	Infrastructure Performance Monitoring	Cloud Migration
Enable healthcare professionals and IT admins alike to monitor healthcare IOT devices.	Leverage the adaptability of cloud environment to maintain leaner operations.	Monitor the organization's environment in one platform while identifying areas for increased efficiency .
1. Understand the technology platform and data availability 2. Design an implementation strategy with healthcare privacy in mind. 3. Onboard the data from in-scope devices. 4. Configure dashboards and alerts to notify both healthcare professionals and IT admins of critical activity 5. Enable the organization to leverage device data to make informed patient decisions	1. Gather requirements based on the current implementation 2. Design an implementation approach based on data volume and performance requirements 3. Configure Splunk components and migrate data 4. Enable access and design updated processes based on cloud environment 5. Monitor the environment to adjust deployment to operational efficiency while reducing costs	1. Assess the current state of the IT environment 2. Design a data normalization strategy to monitor for operational inefficiencies. 3. Onboard data based on CIM compliance and configure required use cases 4. Operationalize alerting to enable IT admins and the SOC teams to respond 5. Automate response to reduce mean time to respond (MTR) and improve operational efficiency

Value Provided

▸ Respond more quickly to changes in a patient's health ▸ Provide individualized approach to personal healthcare	▸ Decrease infrastructure overhead and management costs ▸ Focus on development efforts to improve maturity	▸ Improve the performance of IT infrastructure by leveraging data to drive decisions ▸ Minimize impact to the business by responding more quickly to IT infrastructure related issues

Impacted audience

IT Admins	SOC Analysts	Healthcare Professionals

Model for Driving Innovation

- Workforce enablement
- Business enablement
- Market accelerators
- Alliance and ecosystem relationships
- Advisory counsel (academia, industry and government)

Why Ernst & Young LLP?

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

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.

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. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.