

Information Technology (IT) and Operational Technology (OT) cybersecurity program



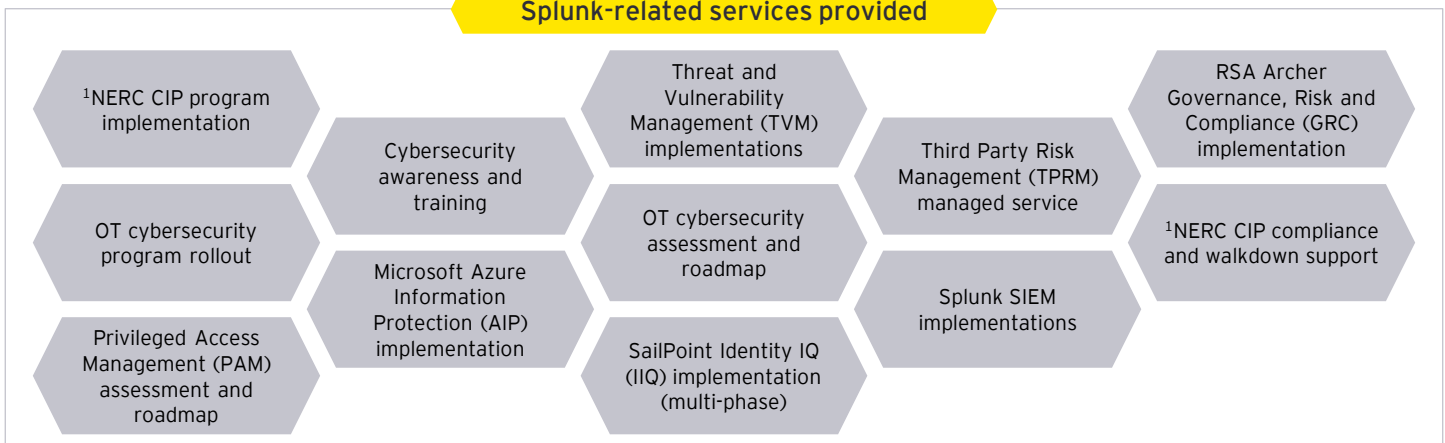
Our service focuses on building a secure, scalable, reliable and repeatable Security Information and Event Management (SIEM) architecture to enable companies to move fast, integrate efficiently and create a secure and sustainable Splunk platform. By creating a robust platform that enables contextual data in a proactive environment, we mature both the use cases and processes that support key critical systems across a company's environment.

Our approach begins with deploying a highly-skilled, experienced, knowledgeable and insightful core team to focus on and deliver the engagement. The core team is augmented by our partnership with Splunk, enabling a diverse group of subject matter experts capable of innovating and advancing the Internet of Things (IoT)-OT space. This allows our core team to be lean, effective and adaptable while having vast resources readily available to respond to threats and create innovative solutions to emerging ones. Our methodology and approach center on collaboration to achieve and maintain maximum availability and security of Client resources.

OT solutions allow us to enable and enhance our clients' Splunk capabilities.

- ▶ Safely collect OT machine data utilizing our OT Sandbox Testing approach.
- ▶ Deploy and implement proven data collection methodologies at scale.
- ▶ Efficiently onboard multiple data source simultaneously using pre-built guides and runbooks.
- ▶ Flatten the learning curve with custom, Common Information Model (CIM) compliant, OT vendor apps and add-ons.
- ▶ Support data-driven decisions with advanced toolsets like Machine Learning Toolkit (MLTK), IT Service Intelligence (ITSI), Phantom, etc.
- ▶ Decrease time-to-operation and acceptance via packaged training materials and job aids.

Splunk-related services provided



¹ North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)

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.



EY IT/OT advanced Splunk solutions

EY is utilizing advanced tools, technologies and procedures to assist our clients in making more quantifiable and actionable decisions based on a perspective driven by data insights.

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

MLTK example use cases

- ▶ Abnormally low resource availability for critical systems
- ▶ Abnormal protocol traffic traversing security perimeter
- ▶ Occurrences on fault patterns that exceed the baseline threshold
- ▶ Business process authentication violations to human-machine interface (HMI) systems
- ▶ Improbable configuration changes on serial port servers
- ▶ Prediction of future relay "trips" based on event correlation

ITSI example use cases

- ▶ Real-time fleet monitoring
- ▶ Service disruption and impact calculations based on size, scope and severity
- ▶ Root cause analysis of service degradation

OT Sandbox

- ▶ It is designed to model selected architecture and technologies representing the business area technologies, to enable functional testing of equipment and software before it is deployed into operations.
- ▶ This is a Sandbox environment that can be used for patch testing, updates and other operational changes of equipment to ensure capability before applying changes on critical infrastructure. The lab can also simulate cybersecurity events and conduct known Common Vulnerabilities and Exposures (CVE) testing on equipment in a secure manner.

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.

© 2021 EYGM Limited.
All Rights Reserved.

SCORE no. 008860-21Gb
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com