Site Security Assessment from GE Digital
Develop an effective long-term strategy for improving security posture

Cyber attacks on ICS environments are on the rise

Cyber attacks on critical infrastructure are on the increase, and are a growing concern for system operators. In December 2014, it was revealed that a steel mill in Germany was the victim of a cyber attack, which gave the attackers access to the plant’s production network; a blast furnace was prevented from being properly shut down, causing massive damage. Earlier in the year, the U.S. Department of Homeland Security announced it would investigate the possibility that the Havex Trojan had targeted industrial control systems, compromising over 1,000 energy companies across Europe and North America. Attacks such as these severely impact service uptime, data integrity, compliance, and public safety.

It is imperative that companies that rely on computer networks for industrial control system (ICS) operations assess their current security posture, understand potential security risks, and develop effective risk mitigation strategies.

01 Business challenge
ICS networks are increasingly targeted for cyber attack, and system operators are experiencing cyber incidents at an ever-expanding rate. Operators need to understand their current security status and develop a plan to improve their security posture. They also require documentation and assistance to comply with industry regulations such as IEC 62443, ISA99, and other industry standards.

02 Solution
GE Digital’s Site Security Assessment is a comprehensive evaluation of an operating facility (such as oil refineries, electricity generation facilities, and others) that helps system operators reduce the risk of a network-based cyber attack. It helps them understand the security posture of their processes, architecture, and technology.

The assessment also provides findings to equip operators with the ability to identify security weaknesses, prioritize areas of improvement, and align security practices to industry standards.

The Site Security Assessment follows a proven, repeatable methodology specially developed to protect industrial control systems. Several security analysts come onsite to complete the full facility review. This comprehensive assessment enables operators to mitigate immediate risks, while developing an effective long-term strategy to improve their overall security posture.

03 Benefits
- Optimizes production and system reliability by identifying, prioritizing, and mitigating risks that impact critical production systems.
- Improves overall security by identifying weaknesses and mitigation strategies that address individual weaknesses in systems, assets, or data flows.
- Enables compliance efforts by helping to align with relevant industry standards, regulations, and best practices.
- Provides comprehensive reports and documentation to assist with regulatory compliance efforts and audits for IEC62443, ISA99, and more.

GE digital can help improve your security posture and succeed in today’s digital industrial landscape.

LEARN MORE
Site Security Assessment from GE Digital
Develop an effective long-term strategy for improving security posture

**Features**
- **Information gathering**
  Request relevant, customer documentation relating to people, architecture, and technology
- **Documentation review**
  Analyze at a high level the documents detailing network configuration, topology, policies, and other relevant aspects unique to each customer
- **Interviews and inspection**
  Meet on-site with subject matter experts (SMEs) to gain additional technical and contextual understanding not apparent from documentation reviews alone
- **Offline data analysis**
  Utilize GE Digital’s best practices methodology* to assess customer risks
- **Risk assessment**
  Identify sources of potential vulnerability and determine general security posture
- **Findings report**
  Share assessment findings observation

**Deliverables**
- **Actionable report**
  - Executive summary
  - Assessment methodology overview
  - Risk criteria and threat model
  - Risk assessment
  - Assessment observations (people, architecture, and technology)
  - Prioritized recommendations and mitigations
  - Security roadmap
- **Asset review workbook**
  - Security posture assessment, including all the collected raw data
  - Detailed analysis of potential cyber security risks for systems, including: system policies, account and password controls, installed security and software, patch versions, configuration settings, network information, and more
- **Results presentation**
  - Overview of the process and the results for management
  - High-level summary of the full report, including identified weaknesses and recommended mitigations

* GE Digital’s best practices methodology is based on many industry standards. Some of these standards include: ISA-99/IEC 62443, NIST 800-53, DHS-CSPL, ISO27001:2005

**Comparison chart**

<table>
<thead>
<tr>
<th>Service Components</th>
<th>Site Security Assessment</th>
<th>Site Security Health Check</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Customer goal</strong></td>
<td>Comprehensive view of security posture</td>
<td>Rapidly gain high-level insight into current operational security posture</td>
</tr>
<tr>
<td><strong>Assessment methodology</strong></td>
<td>GE Digital proprietary*</td>
<td>GE Digital proprietary*</td>
</tr>
<tr>
<td><strong>Security gap analysis</strong></td>
<td>In-depth</td>
<td>Targeted</td>
</tr>
<tr>
<td><strong>Architectural review</strong></td>
<td>√</td>
<td>(Scaled)</td>
</tr>
<tr>
<td><strong>Findings report</strong></td>
<td>✓</td>
<td>(Scaled)</td>
</tr>
<tr>
<td><strong>Close-out presentation</strong></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Detailed asset review workbook</strong></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

**Process**
- **Information gathering**
  - √
  - (Scaled)
- **Documentation review**
  - √
  - (Scaled)
- **Interviews and onsite inspection**
  - Senior analyst, 2-days on-site
  - Analyst, 1 day on-site
- **Technical testing**
  - √
- ** Offline data analysis**
  - √
- **Risk assessment**
  - √
  - Scaled
- **Risk mitigation recommendations**
  - Prescriptive, detailed strategies
  - High-level general direction

* International standards-based

**Summary**

GE Digital’s Site Security Assessment helps system operators of industrial control systems understand their system security weaknesses, identify and prioritize areas of improvement, and align security policies to industry best practices. GE Digital site assessments are delivered by experienced industry experts who have completed 200+ assessments to enhance our customers’ security postures and align with industrial security best practices.
Site Security Assessment from GE Digital
Develop an effective long-term strategy for improving security posture

Services
In the world of Industrial Internet of Things (IIoT), organizations are able to optimize productivity, reduce costs, and achieve Operational Excellence. No matter where you are on your IIoT journey, GE Digital has the right services offering for you.

Advisory Services We can help you plan and start your IIoT journey in a way that aligns to your specific business outcomes.

Managed Services We can help you maintain your critical machines from one of our remote locations around the world using model-based predictive-analytic technology.

Implementation Services Our experienced global automation partners can implement a collaborative, multi-generational program that marries your existing investments to the right enhancements and technology.

Education Services We specialize in education services to ensure that you’re leveraging our solutions to the fullest extent with our training and certificate programs.

GlobalCare Support Services Let us help by ensuring that your business continues to operate at its highest efficiency, all while mitigating risks to your investments.

Cyber Security Services Our solutions provide industrial-grade security for a wide range of OT network and application topologies.

Related products
GE Digital’s OT cyber security suite helps protect industrial and healthcare companies against misconfigured devices and unplanned downtime due to cyber incidents. We can help you test, certify, and secure industrial connected devices, applications, and processes.

Achilles Test Platform
Build in product security. Achilles Test Platform discovers vulnerabilities and faults to be reproduced, isolated, identified, and resolved before product introduction.

OpShield
Designed to help protect critical infrastructure and controls network by defending the processes, communications, and assets that underpin your control strategy.

Predix
Innovate and transform your business with the cloud-based operating system for the Industrial Internet, purpose-built for industry.

Continue your IIoT journey
Transforming your business requires innovative foundational solutions that lay the groundwork for optimized performance.

Historian
Optimize asset and plant performance through time-series industrial data collection and aggregation, leveraging Predix IIoT connectivity.

iFIX
Gain visibility into your operations and secure agility for smarter decision making that drives results.

Asset Performance Management
Move from reactive to proactive maintenance to reduce unplanned downtime, minimize maintenance costs, improve efficiency, and extend asset life.

Contact
Americas: 1-855-YOUR1GE (1-855-968-7143)
gedigital@ge.com
www.ge.com/digital

About GE
GE (NYSE: GE) is the world’s Digital Industrial Company, transforming industry with software-defined machines and solutions that are connected, responsive and predictive. GE is organized around a global exchange of knowledge, the “GE Store,” through which each business shares and accesses the same technology, markets, structure and intellect. Each invention further fuels innovation and application across our industrial sectors. With people, services, technology and scale, GE delivers better outcomes for customers by speaking the language of industry.

©2017 General Electric. All rights reserved. *Trademark of General Electric. All other brands or names are property of their respective holders. Specifications are subject to change without notice. 05 2017