



# Industrial Cybersecurity Services

To protect Operational Technology (OT) Assets in the Energy Sector

GE's industrial cybersecurity solutions are designed to meet international standards & regulations. Together with its technology partners, GE provides customised end-to-end solutions that can be integrated into any existing cyber (IT&OT) defense plan.

Regardless if your Industrial Control System (ICS) is connected to the Internet or air-gapped, malicious attacks on ICS and Supervisory Control And Data Acquisition systems (SCADA) have increased significantly in recent years. New vulnerabilities are discovered, new attack methodologies are being developed. The majority of these attacks can be easily avoided with a robust Cybersecurity plan.

## Operational resilience in three steps

GE follows the defense-in-depth concept and can help you to plan, design and implement operational resilience into your processes and technology and train your people.



Figure 1: GE's 3 stages of cyber defense services



### Stage 1 - Assess

Identify immediate security concerns that can impact operations even if the environment is thought to be air-gapped.



### Stage 2 - Protect

Implement monitoring and defensive layers to comply with standards and strengthen the security posture of a facility or system.



### Stage 3 - Respond and Recover

Pursue proactive and predictive security measures such as have a response plan & trained personnel to execute it during or after cyber events.

In-line with local and global regulations and standards, GE help you to increase overall protection of your installations: up-to-date activities, faster recovery, better monitoring against threats.

Each service is performed in a secure environment, protecting your critical installations and systems, and executed by our certified experts.



Figure 2: GE's industrial cybersecurity solutions meet International Standards.

## Products and Services

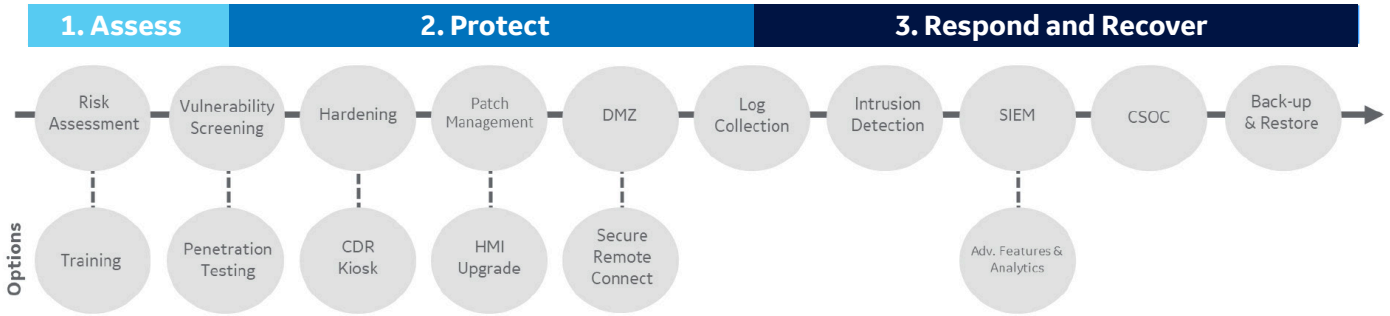


Figure 3: End-to-end cybersecurity solutions.

### Benefits

GE’s portfolio of industrial cybersecurity solutions provide in-dept cyber defense layers with the following benefits:

- Risk mitigation against cyber threats
- Support business continuity
- Full end-to-end cyber solutions and maintenance
- One partner for the entire portfolio, Integrating future-ready technologies
- In-line with international standards and local regulations
- Flexible and adaptable customized solutions and services

### References

GE has successfully installed cybersecurity solutions globally in more than 15 countries on a wide range of installed and new Power Plants, including:

- 1 x 121 MW, Concentrated Solar Power Plant, Israel .
- 1 x 650 MW, Combined Cycle Power Plant, Israel .
- 3 x 1300 MW, Nuclear Power Plant, Belgium.
- 1 x 30 MW, Industrial Plant , Indonesia.
- 1 x 344 MW, Hydro Power Plant , Israel.

### Applicability

The industrial cybersecurity solutions can be applied to all critical Operational Technology assets in the power industry and energy sector. Solutions are available for new assets and operational assets in amongst others renewable power plants (e.g. Hydro, Concentrated Solar Power), fossil and nuclear power plants and industrial plants.

### GE Partners

GE collaborates with selected technology partners such as Thales, Fortinet and Nozomi Networks who provide leading products and services for the ICS cybersecurity market.

THALES

FORTINET

NOZOMI NETWORKS

Figure 4: GE’s technology partners supporting end-to-end cybersecurity services portfolio

For more information please [contact](#) your local GE representative or visit us at:

[www.ge.com/steam-power/services/automation-controls/cyber](http://www.ge.com/steam-power/services/automation-controls/cyber)

