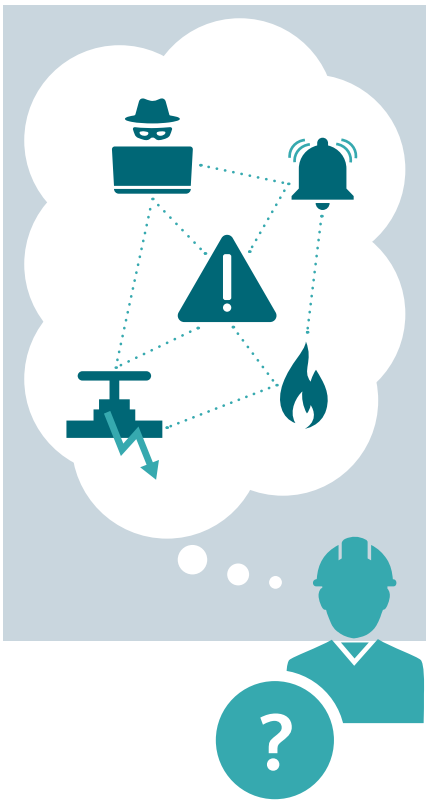
SIEMENS
Ingenuity for life

# Plant Security Monitoring

siemens.com/energy



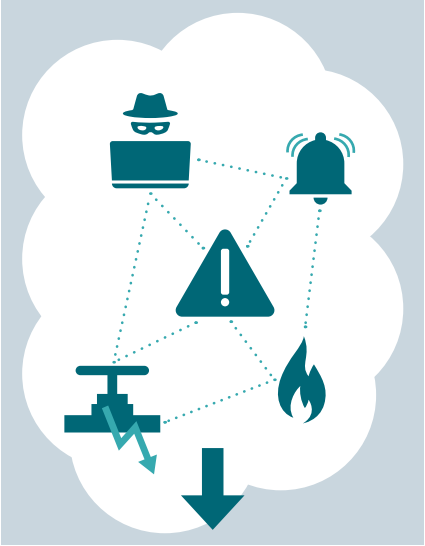

## Customer Challenge

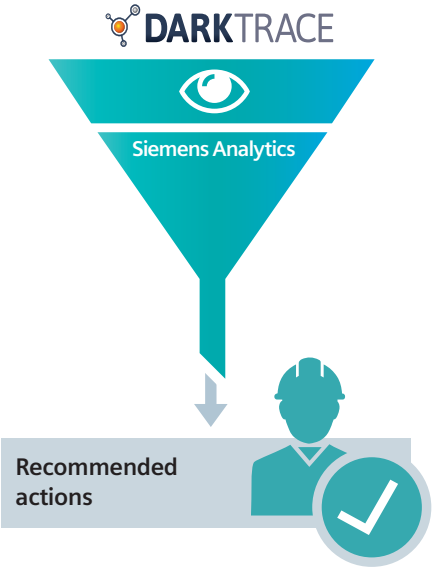
Hundreds of industrial devices are **connected together to keep a plant up** and running. These devices continuously share information to reach operational goals. A company's ability to serve its customers depends on the **reliability of these systems**. Customers face two persistent challenges in this area:

1. They **lack real-time visibility** into their operating technology and networks
2. They are **overwhelmed by "noisy" alerts**, and struggle to translate these alerts into actionable recommendations for the operating environment

While **signature-based methods** can be effective in detecting known threats, they are ineffective against sophisticated threats like **zero days and advance persistent threats**. This means that these tools are potentially missing many sophisticated attacks. And the longer a threat sits on an organization's network, the greater the potential of impact (interruption, etc). Many organizations understand the challenge they face: they know they are unable to quickly, effectively detect cyber breaches.

Most security teams lack the ability to sift through thousands of **cyber security alerts,** understand the **root cause of events,** identify the **highest priority issues** and take **corrective action.**






# Solution

Siemens, along with its technology partner Darktrace brings **real-time anomaly detection** to the industrial OT environment. Siemens Plant Security Monitoring service provides the continuous visibility required to make **smarter, faster decisions.**

By leveraging Siemens' knowhow and expertise, organizations receive **fewer, smarter alerts alongside clear and actionable recommendations** on how to address them.

The technology applies **unsupervised machine learning** to automatically detect cyber-threats within all types of networks, including physical, industrial control, cloud and virtualized networks.

## The solution...

- **Continuously learns and models network** activity by leveraging unsupervised machine learning algorithms
- **Reducing false positives** and producing fewer, smarter alerts
- **Identifies** advanced threats passively in real time
- **Provides operational context** to anomalous network events

Siemens provides the technical design, deployment and installation of the Darktrace software. OT experts assess the unique network topology and optimize Darktrace's deployment to **maximize its visibility into assets' network activity**, while ensuring zero risk to on-going operations. Along with the delivery and deployment of the appliance, the technical support component of this solution includes:

1. **Collection of network data**
2. **Analysis** of reported security events and anomalous operations
3. **Applied operational context** to identified events to improve understanding of impact
4. Filtering and periodic **reporting of relevant findings**, along with recommended actions to secure operational technologies from cyber threats


# Benefits

Siemens Plant Security Monitoring undertakes investigations to provide clear operational context and insights that help manage and prioritize alerts.

- Enables resource constrained organizations to f**ocus only on most critical alerts**, backed by Siemens expertise
- Offers unmatched insights into OT: **Empowers organizations** to make smarter, faster security decisions
- **Works across all networks and OT devices**, regardless of vendors
- Detects both insider and sophisticated external threats
- Solution can be provided on a single facility or across a fleet

## Part of a comprehensive solution set...

Plant Security Monitoring is a key part of Siemens cyber solutions offerings that include **Asset Management** and **Vulnerability Management**. Alone, Plant Security Monitoring provides network visibility into potential attackers. However when matched with Asset Management and Vulnerability Management, customers **gain deeper understanding of how an attack is forming, when an exploit is taking place, and what an attacker is changing on a particular OT device**. Combining Siemens expertise with these services provides a complete picture across the OT environment and optimizes your **ability to prevent, detect, and respond to attacks.**

**siemens.com/energy**