



EXECUTIVE BRIEF

Integrating OT into IT/OT SOCs

In the new world of increased cyber risk, approaches that bridge the IT/OT divide are no longer optional – they're mission critical. Executive leadership expects CIOs and CISOs to anticipate and stay ahead of the enterprisewide threat landscape, including oversight of cyber risks related to industrial operations.

Integrating operational technology (OT) threat monitoring into security operations centers (SOCs) contributes greatly to achieving fast, comprehensive threat detection and response. This Executive Brief looks at the trends behind combined IT/OT SOCs and outlines a straightforward way to include industrial threat monitoring that meets the needs of both IT and OT.

Cyber Incidents Threaten Results and Reputation

Business executives and Boards of Directors are increasingly aware of the potential impact of cyber security incidents on results and reputation. High-profile attacks, such as the Equifax data breach and the NotPetya global attack, have demonstrated just how costly they can be, with worldwide NotPetya damage estimated at \$10 billion.¹

In the OT arena, cyberattacks on critical infrastructure and strategic industrial assets have dramatically increased. This includes attempts to disrupt operations and steal intellectual property. Governments are also intensifying regulatory oversight and breach reporting requirements.

As a result, OT cyber security is receiving unprecedented attention and transitioning away from siloed engineering supervision to management by collaborative IT/OT teams.

Industrial Cyberattacks – A Top Global Risk

Cyberattacks on critical infrastructure and strategic industrial assets are now one of the top five global risks.

World Economic Forum, Global Risk Report, 2018

Attackers Exploit IT/OT Defense Gaps

"Many industrial companies still view IT and OT cyber security as separate challenges. Different concerns and practices seem to justify siloed efforts and separation of responsibilities. However, attackers are already exploiting gaps between IT and OT defenses.

For example, spam phishing is commonly used to gain privileges and entry into OT systems. And hackers are using HVAC and other poorly defended OT systems as entry points into data centers and corporate IT networks."

ARC Advisory Group, IT-OT Cyber Security Convergence, Jul 2018

CIO/CISOs Need to Make Informed Choices

"Attacks and compromise are inevitable, and, by 2020, 60 percent of security budgets will be in support of detection and response capabilities."

Gartner, The IT Implications for I&O Leaders, Mar 2018

"Security tools deployed for OT security have to support the need for coordinated enterprisewide security activities, which comes from having IT and OT security handled with a joint governance process."

Gartner, Competitive Landscape: OT Security, Oct 2018

ENEL, THE #1 GLOBAL ELECTRIC UTILITY, CHOOSES NOZOMI NETWORKS

“With Nozomi Networks Guardian we can now detect and collect operational and cyber security issues in real-time, and take corrective actions before the threat can strike.”

GIAN LUIGI PUGNI
Head of Cyber Security Design, Enel

“Nozomi Networks Guardian is now a fundamental element of our network infrastructure and an essential tool for our daily activities.”

FEDERICO BELLIO
Head of Power Generation Remote Control System, Enel

The Driving Force Behind IT/OT SOC's

The Reality of Risks Facing OT Systems

In the past, industrial systems were not considered to have high cyber risk because they were isolated (air gapped), without connectivity to enterprise systems or the internet. They were also protected by obscure proprietary technology and considered of low interest to hackers or attackers.

Now, industrial cyber risk is much higher due to:

- More connectivity and exposure – The increased use of common technology platforms and data sharing between IT and OT systems exposes industrial systems to more cyber threats. This includes the migration to the Industrial Internet, where physical assets and IT infrastructure are closely integrated.
- The transition to virtual systems – Shifting industrial system architectures away from local monitoring and data processing to cloud-based applications and analytics increases cyber risk exposure.
- More sophisticated attacks – A new era of industrial threat actors, such as hackers, criminal organizations and nation states, focus on disrupting industrial systems for financial or political gain.
- Easier access to resources – A marketplace of tools, example malware frameworks and vulnerability exploits makes it faster and easier to execute industrial cyberattacks.

As a result of these trends, the majority of IT and industrial control systems (ICS) security practitioners across a variety of industries believe the threat level to OT systems is high or critical.²

Why the IT/OT SOC?

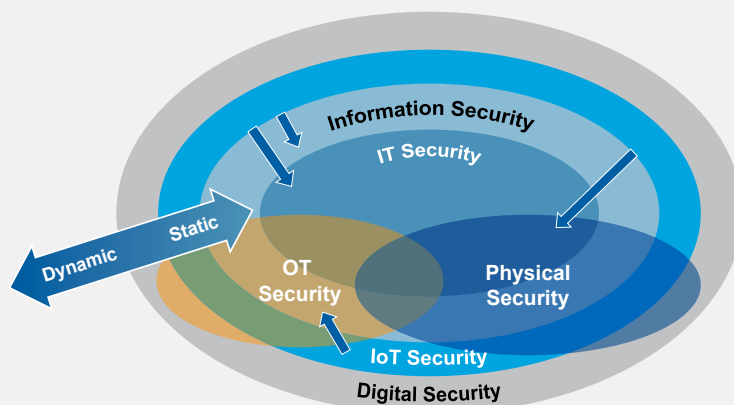
SOCs are generally tasked with preventing, detecting and responding to cyber security threats and incidents. Often, they also assess and fulfill regulatory requirements. Typically, their mandates do not cover industrial systems – though it is possible to leverage the investment in SOC's to include OT.

As threats to OT systems intensify, there are several reasons to include OT in an enterprise-level SOC. With a combined approach, companies can:

- **Stop threats faster** – Most cyberattacks on OT systems originate on the IT network and involve multiple steps in an elaborate cyber kill chain process. High profile examples include an attack on a German steel mill, disruption to Ukraine's power grid in 2015 and 2016, and the shutdown of a gas facility in Saudi Arabia in 2017. Thus, to protect OT systems, threats need to be stopped in their early stages, often while they are present in IT systems.
- **Speed up response times** – Monitoring OT systems separately from IT systems runs the risk of breakdowns in communication and dropped incident handling between multiple teams.
- **Keep costs down** – It's more cost effective to include OT threat monitoring within one comprehensive SOC than to have multiple SOC's.
- **Leverage teams' strengths** – Protecting OT systems requires a blend of IT and OT skills. For many organizations, it is easier to close the skills gap by training IT people on OT sensitivities than training OT people on IT cyber security skills.

IT/OT Convergence

"To reduce risk, security and risk management leaders should eliminate IT and OT silos by creating a single digital security and risk management function. This function should report into IT but should have responsibility for all IT and OT security."



ID: 347847

© 2018 Gartner Inc.

Building an IT/OT SOC

The Challenges of Securing OT Systems

Adding OT security into the mandate of SOCs is not a simple matter of extending IT security solutions and staff responsibilities to include industrial networks.

OT networks are often large, complex and include a wide range of assets that are unknown to IT, including legacy equipment that can be sensitive to many types of network traffic.

They also use insecure and often proprietary protocols whose communications cannot be properly evaluated by IT security tools.

Finally, the central mission of the people managing industrial networks is to maintain high safety, availability and production efficiency. This focus must be embraced when integrating OT network monitoring into an SOC.

Key Considerations for an SOC Transition

All these unique challenges mean that companies will need to consider the following as they create an IT/OT SOC:

- **Technology**—Solutions need to meet all the specific requirements for OT, but also integrate seamlessly with IT SOC systems and infrastructure.
- **People Resources**—Enterprise SOCs require the inclusion of industrial cyber security specialists in core SOC resourcing, or as part of a virtual or extended team. To keep costs down and reduce the need for scarce cyber security skills, companies should consider concentrating the SOC team in one location and providing cross-training on critical skills.
- **Accountability**—Business leaders must create an environment that aligns IT and OT under one common culture and reporting structure. As the teams merge,

they should work to understand the others' priorities and challenges, and achieve the common goals set by the executive responsible for companywide cyber risk.

Selecting the Right OT Technology

To embrace the inevitable convergence of IT and OT teams and achieve a high-functioning, cost-effective enterprisewide SOC, companies need better visibility of OT infrastructure and threats.

When selecting an OT cyber security and visibility solution, make sure it:

- Delivers superior real-time OT threat monitoring that shortens the mean time to detection and response.
- Provides comprehensive OT network visualization and asset inventory, without risk to the industrial process.
- Empowers security analysts to rapidly remediate threats with OT-specific alert aggregation, dashboards and forensic tools.
- Integrates seamlessly with IT infrastructure, easily sharing data with existing applications and assets.
- Includes pre-built integrations with SOC tools, such as SIEMs.
- Deploys quickly and easily with mature technology that is ISO 9001 certified.
- Consolidates information from multiple industrial sites and scales to meet the needs of very large distributed organizations.

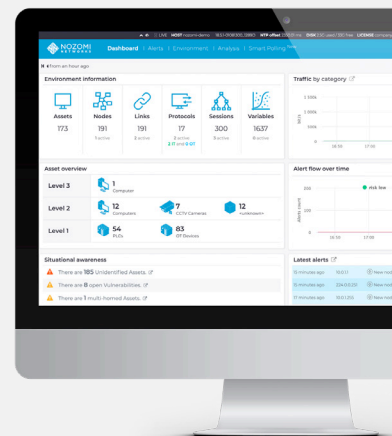
Companies with an IT/OT SOC will experience better threat detection and response metrics, improved cyber resiliency and an overall decrease in cyber risk.

Improving Enterprisewide Cyber Security

While increasing cyber threats dominate the news, there is reason to be optimistic. New technology, such as the Nozomi Networks solution, is easy and safe to deploy, dramatically improves OT cyber security and integrates seamlessly with IT infrastructure.

To see OT cyber security and visibility in action, and experience how easy it is to work with Nozomi Networks, have your team contact us:

www.nozominetworks.com/contact



Nozomi Networks - The Leader in Industrial Cyber Security

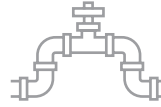
ENGAGED WITH GLOBAL INDUSTRY LEADERS



Electric Utilities



Automotive Manufacturing



Oil & Gas



Pharmaceuticals



Mining



Chemicals



Food & Consumer Goods



Water/Wastewater

STRATEGIC PARTNERS



...and more!

References

- Wired.com: "[The Untold Story of NotPetya, the Most Devastating Cyberattack in History](#)," Andy Greenberg, Sep 22, 2018
- Sans.org: "[Securing Industrial Control Systems – 2017](#)," Bengt Gregory-Crown, Doug Wylie, Jun 2017

About Nozomi Networks

Nozomi Networks is accelerating the pace of digital transformation by pioneering innovation for industrial cyber security and operational control. Leading the industry, we make it possible to tackle escalating cyber risks to operational networks. In a single solution, Nozomi Networks delivers OT visibility, threat detection and insight to thousands of the largest critical infrastructure, energy, manufacturing, mining, transportation and other industrial sites around the world.



www.nozominetworks.com

@nozominetworks

© 2019 Nozomi Networks, Inc.

All Rights Reserved.

EB-IT-OT-SOC-A4-003