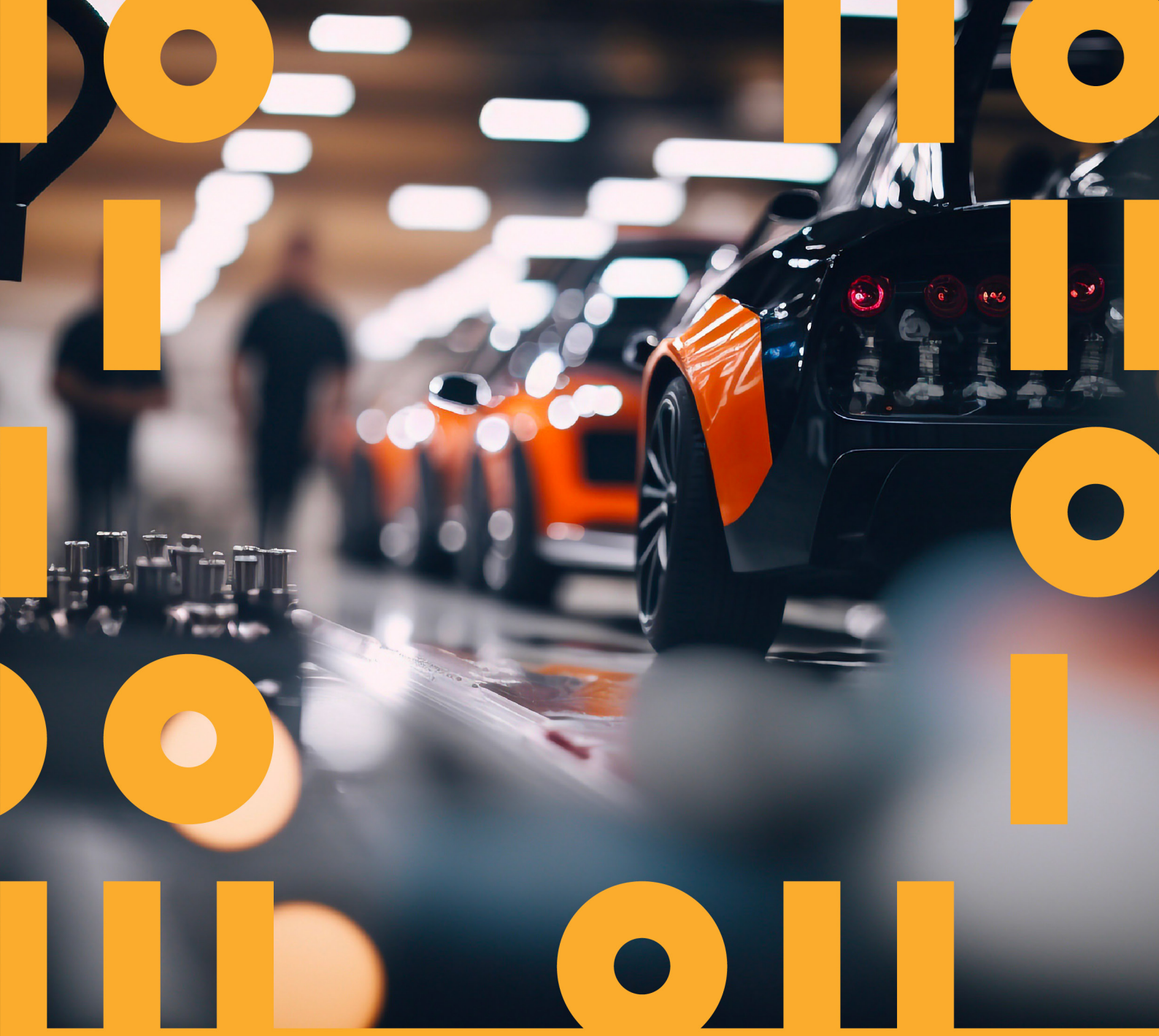

nomios

The cybersecurity challenges of operational technology (OT)

Viewpoint

The cybersecurity challenges of operational technology (OT)

Contents

Introduction

Industrial Control Systems (ICS) are used in almost all infrastructures handling physical processes. Applications range from energy production and distribution, gas and water supply to industrial automation, traffic control systems and facility management.

Many attacks on Operational Technology (OT) systems seem to target older devices running unpatched software, indicating that OT networks are increasingly being targeted by IT-based legacy attacks that are no longer effective against IT networks. However, the industry as a whole is also tracking a disturbing rise in purpose-built OT attacks designed to target SCADA and ICS.

Malware targeted specifically at ICS and SCADA systems has been developed and deployed for over a decade. Attacks specifically designed for OT systems seem to be on the rise, with safety systems increasingly being a target. For those OT organisations responsible for critical infrastructure, any sort of compromise needs to be taken extremely seriously.

A lesson from history

One notable example of a cybersecurity attack on an OT network is the Stuxnet worm, which targeted Iranian nuclear facilities in 2010. Stuxnet is widely considered to be one of the first instances of a cyber weapon specifically designed to target industrial control systems and cause physical damage.

Stuxnet was a highly sophisticated, multi-stage malware that exploited multiple zero-day vulnerabilities in the Windows operating system and Siemens Step7 software. The worm was designed to spread via infected USB drives, making it possible to infiltrate air-gapped systems that were not connected to the internet.

Once inside the target network, Stuxnet sought out Siemens Programmable Logic Controllers (PLCs), which were used to control the centrifuges in Iranian nuclear enrichment facilities. The malware altered the PLCs' programming, causing the centrifuges to spin at dangerously high speeds while simultaneously displaying normal operating conditions to the facility's monitoring systems. This sabotage led to the destruction of a significant number of centrifuges, ultimately delaying Iran's nuclear program.

The Stuxnet attack demonstrated the potential for cyber attacks to cause physical damage and highlighted the vulnerability of OT networks and industrial control systems. This incident served as a wake-up call for governments and organisations worldwide, emphasising the need for robust cybersecurity measures to protect critical infrastructure and OT environments.

OT security challenges

In light of the increasing frequency of incidents and newly discovered vulnerabilities for ICS, asset owners need to address these issues urgently. Hence, they have to consider the risk and damage potential of untargeted malware as well as targeted, high-quality attacks against ICS infrastructures.

This applies to infrastructures directly connected to the internet as well as those that can be compromised by cyberattacks indirectly. Cybercriminals also target devices by focusing on the wide variety of OT protocols in place. While IT systems have been standardised TCP/IP, OT systems use a wide array of protocols—many of which are specific to functions, industries, and geographies. This can create a challenge as security managers have to create disparate systems to secure their environment, creating complexity from different vendor offerings and products. As with legacy IT-based malware attacks, these structural problems are exacerbated by poor security hygiene practices within many OT environments; often as a result of digital transformation efforts.

Some of the key cybersecurity risks associated with ICS and OT include:

- **Legacy systems:** Many ICS and OT components are built on older technology that lacks modern security features. Upgrading these systems can be expensive and time-consuming, leading to vulnerabilities and a higher risk of cyber attacks.
- **Insufficient network segmentation:** In some cases, IT and OT networks are not sufficiently segmented, allowing attackers to infiltrate the OT environment through vulnerabilities in the IT network. This can lead to devastating consequences, as attackers can gain control over critical industrial processes.
- **Inadequate security policies and practices:** Many organisations lack comprehensive security policies and practices specifically designed for their ICS and OT environments. This can result in insufficient protection, monitoring, and incident response capabilities, making it easier for attackers to breach these systems.
- **Lack of awareness and training:** Employees working in OT environments may not be aware of cybersecurity best practices, making them more susceptible to social engineering attacks or unintentional insider threats.
- **Supply chain risks:** ICS and OT components are often sourced from third-party vendors, which introduces supply chain risks. If a vendor's security is compromised, it could impact the end-user's ICS and OT environment.
- **Remote access vulnerabilities:** The increasing need for remote access and monitoring of ICS and OT environments has introduced new attack vectors. If remote access is not properly secured, attackers can exploit these channels to infiltrate the systems.

In this section we will dig a little bit deeper and provide an overview of the most critical and the most common top five threats to Operational Technology.

1. Malware infiltration via external hardware and removable media

Used in the office and at ICS networks, removable media such as external hardware and USB flash drives are frequently used at home as well. Notebooks, for example, carrying external data and maintenance software, are likely to be used at different (public) locations and organisations. Traditionally, ICS security awareness is mainly focused on availability and physical security, such as access restrictions, safety and protection from external influences. This is why cybersecurity awareness about the effects of malware and techniques used by cybercriminals to infiltrate systems, is often low among employees.

There are multiple examples of malware (and ransom-ware) that have caused financial, operational and reputational damage to industries. Potential threat scenarios can be executable files and applications containing malicious code, resulting in data leakage and malware infection. When accessing office networks or infrastructure, an infected notebook computer could quickly infect systems and components with malicious code, once the notebook is being operated in the ICS network.

Having strong organisational policies in place, offering virus protection and running security awareness campaigns on the use of external devices such as USB flash drives and notebooks is not enough. To prevent malware infections from causing extensive damage, OT security solutions should at least provide IT teams with user access management tools, policy enforcement and endpoint security controls, as well as full encryption capabilities.

2. Human error

Employees and external personnel such as maintenance or construction workers, working in an ICS environment, often pose challenges for security.

Systems can be compromised by unauthorised or incorrectly configured software and hardware. Employees can (unwillingly) install malware through emails, games, or by inserting USB devices into their notebooks for example. Often they are unaware of the risks that are being posed by such actions.

IT teams are also regularly being challenged by the amount of next-generation firewalls that have to be managed and updated or that have to be configured regularly. Having an unverified update or patch installed on networking or security components could cause them to run into functional and even critical problems. Allowing unauthorised access via mobile endpoints, for example, is a common result of someone who has added incorrect rules to the firewalls.

Of course, security can never be guaranteed by technical controls alone. Organisational regulations are required, as well as running qualifications and cybersecurity awareness training programmes. Organisations should introduce policies for critical processes in the ICS network such as standards concerning security and configuration management, regulating the involvement of security

experts and other relevant roles. This ensures that changes or updates are implemented only after they have been consulted. In this context, it is important to document all agreements backed up by additional arrangements such as using the four-eyes principle.

The majority of OT attacks tend to target the weakest parts of OT networks. Many of these attacks often take advantage of the complexities caused by a lack of protocol standardisation, and a sort of implicit trust strategy that seems to permeate many OT environments. This trend is not limited to specific locales or sectors. Exploits are increasing in volume and prevalence for almost every ICS/SCADA vendor.

3. DDoS attacks and IoT-botnets

Firms increasingly have different kinds of IoT technologies connected to their network, including passive RFID, real-time location tracking (active RFID, ultra-wideband, ultrasound, etc.), GPS tracking, security sensors, grid sensors, and condition sensors. These devices also use a wide range of communications protocols, including Wi-Fi, cellular systems such as CDMA/GPRS/4G, mesh networks, telematics, and near-field communications (NFC). Each of these technologies not only introduces its own unique security challenges, but they are compounded by many of the security issues inherent in IoT devices that have been built using poor code, that have backdoors and passwords built directly into their firmware, or that operate as headless devices, preventing even basic updating and patching.

IoT-botnets became a well-known cyber threat during the Mirai attack. Botnets are controlled by Command and Control (C&C) networks. The hacker runs these C&C networks, which can be used to launch Distributed Denial of Service (DDoS) attacks.

With IoT device usage rapidly increasing in today's connected world, so does the threat of botnet DDoS attacks. Because many IoT devices lack built-in security measures, they are being 'recruited' into botnets and used to initiate DDoS attacks.

If connections between ICS components are interrupted, transmitting and measuring control data, for example, is not possible. A common tactic used to cause outages of components and systems is to overload a component with a very high number of queries making it impossible to deliver a timely answer. In some cases, these DDoS attacks are distributed over several threat agents.

With more and more IoT devices out there, the new generation of botnet DDoS attacks means that the number of threats and their devastating potential for Operation Technology will grow in the coming years. That's why mitigating massive traffic volumes using DDoS protection solutions is considered a major cybersecurity priority for the years to come, as also described in our top challenges for network security.

Threat scenarios include DDoS attacks being initiated by hacktivists or by buyers of rentable botnets, targeting internet connections of central or remote components. Interfaces of individual components, such as application servers or databases, can also crash when being targeted - by interrupting processing logic for example.

4. Malware infection via Internet and Intranet

In 2017 Triton targetedsafety instrumented system (SIS) controllers at a Saudi Arabian petrochemical plant.This attack is especially concerning because the physical controllers and their associated software are the last line of defense against life-threatening disasters. Many more followed, such as the well-known attack on the Colonial Pipeline Company by the DarkSide ransomware. And given the fact that this malware targets a safety system, the outcome of such an attack could potentially be much worse; not only destroying machinery but threatening lives.

Closely related to Human Error, enterprise networks are often infected with malware due to human error, but also because of the use of standard components such as web servers and databases. Browsers or e-mail clients are typically connected to the Internet for example, with new vulnerabilities discovered almost every day. These vulnerabilities are being used to deploy malware, causing critical or sensitive information to be obtained by the threat agent.

Furthermore, maintaining IT security is hampered by the increasing prevalence of ethernet-based networks and protocols in ICS environments and their connection to enterprise computing (file servers, ERP and MES systems). If a threat agent manages to get into the office network, by exploiting zero-day exploits, for example, he may infiltrate the ICS network directly or via a subsequent attack. Unfortunately, many anti-viruses and email security products are not able to detect these attacks, causing them to silently gather information and cause damage. A commonly used tactic carried out by perpetrators is the 'drive-by download' method. The malware infection happens when someone simply visits a website, or when systems that are part of the control room or operating controls browse the internet. Other common threat scenarios are SQL injection, untargeted malware such as worms and cross-site scripting.

Regular and timely patching of operating systems and applications in the office and back-end networks and, if applicable, in ICS networks is essential to preventing malware infiltration. Monitoring log files for unusual connections or connection attempts and ensuring optimal hardening of all IT components (services, computers) used in the office and ICS environments is also vital.

5. Compromising cloud components

Cloud-based security solutions are indeed becoming more popular in the Industrial Control Systems (ICS) sector, offering numerous benefits such as scalability, cost-effectiveness, and redundancy. Remote maintenance solution providers, for instance, may use cloud-based systems to facilitate remote access to their client's infrastructure. Cloud-based solutions offer scalability, pay-per-use models and redundancy.

While these solutions offer significant advantages, they also introduce new challenges and risks for OT cloud security. Asset owners have limited control over the security of these components while they are connected to local production. This poses OT cloud security threats such as disrupted communication between local production and outsourced (cloud) components due to DDoS attacks. Attacks on other cloud services may also lead to interference (collateral damage) when clients of a cloud provider are insufficiently separated.

Some of the primary OT **cloud** security threats include:

- **Disrupted communication:** Distributed Denial of Service (DDoS) attacks on cloud-based components can lead to disrupted communication between local production systems and outsourced (cloud) components. This disruption can impact the stability and availability of critical ICS processes.
- **Collateral damage:** If cloud service providers do not adequately separate their clients, an attack on one client's services may inadvertently affect other clients' services. This can result in unintended consequences for ICS asset owners, even if they were not the primary target of the attack.
- **Limited control:** Asset owners often have limited control over the security measures implemented by their cloud service providers. This lack of control can make it difficult for organisations to ensure that their OT cloud security measures align with their internal security policies and industry best practices.
- **Data privacy and compliance:** Storing sensitive ICS data in the cloud can raise concerns around data privacy and compliance with regulatory requirements. Organisations must carefully assess their cloud provider's data protection measures and ensure they meet industry standards.

To mitigate these risks, organisations should consider the following best practices when adopting cloud-based security solutions for their ICS environments:

Work with reputable cloud service providers:

Select providers with a strong track record of security and reliability, and ensure they comply with relevant industry standards and regulations.

Perform thorough assessments of potential cloud service providers to understand their security measures, incident response capabilities, and any potential risks associated with using their services.

- **Maintain strong network segmentation:** Segregate OT networks from IT networks and implement additional security measures, such as firewalls and intrusion detection systems, to minimise the potential impact of cloud-based security threats on local production systems.
- **Implement strong access controls:** Use robust authentication and authorisation methods for remote access to cloud-based ICS components, and restrict access to only those personnel who require it.
- **Monitor and log activity:** Continuously monitor and log activity within your ICS environment, including cloud-based components, to enable the timely detection and response to potential security incidents.

- **Establish incident response and recovery plans:** Develop comprehensive plans for responding to and recovering from security incidents affecting cloud-based ICS components, and test these plans regularly to ensure their effectiveness.

By carefully considering the risks associated with cloud-based security solutions and implementing appropriate best practices, organisations can reap the benefits of these services while maintaining a strong OT security posture.

OT cybersecurity preparedness

It is difficult to provide an exact percentage of industrial organisations that have invested in sufficient cybersecurity defenses; however, there are several reports and studies conducted by industry experts and cybersecurity firms that highlight the underpreparedness of industrial organisations in the face of growing cyber threats targeting Operational Technology (OT) environments. Here are three notable reports:

SANS Institute - 2020 SANS ICS Cybersecurity Survey: This report provides an analysis of the current state of ICS cybersecurity, revealing that only 27% of the surveyed organisations had a comprehensive OT/ICS cybersecurity program in place. The study also discusses the challenges organisations face in securing their ICS environments and provides recommendations for improving security posture.

Deloitte - 2020 Cyber Threats in the Energy Sector: Deloitte's report focuses on the energy sector, which is increasingly being targeted by cyberattacks. It highlights the growing risks to the sector's OT systems and critical infrastructure, emphasising the need for organisations to invest in enhancing their cybersecurity defenses.

Fortinet - 2020 State of Operational Technology and Cybersecurity Report: Fortinet's report examines the OT cybersecurity landscape and the challenges organisations face in securing their ICS environments. It highlights the need for increased collaboration between IT and OT teams and the adoption of a comprehensive, risk-based approach to cybersecurity.

https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-state-of-operational-technology.pdf

These reports collectively show that many industrial organisations are underprepared for the growing cyber threats targeting OT environments, emphasising the need for increased investment in cybersecurity measures, employee training, and robust security policies.

This gap in preparedness can be attributed to several factors, including:

- **Legacy systems:** Many industrial organisations are still using outdated hardware and software that lack modern security features, making it difficult to implement sufficient cybersecurity defenses.
- **Lack of awareness:** Some organisations may not fully understand the potential consequences of a successful cyber attack on their OT environments, leading to insufficient investment in cybersecurity.
- **Resource constraints:** Smaller organisations, in particular, may have limited budgets or personnel available to dedicate to OT cybersecurity, resulting in less comprehensive defenses.
- **Complexity:** The integration of IT and OT systems can create complex environments that are challenging to secure, requiring specialised tools and expertise that many organisations may not possess.
- **Skills shortage:** There is a well-documented shortage of skilled cybersecurity professionals, making it difficult for organisations to find and retain the talent necessary to secure their OT environments effectively.

While some industrial organisations have made significant progress in securing their OT environments, it is clear that many are still underprepared. As cyber threats continue to evolve and grow in sophistication, it is crucial for organisations to prioritise OT cybersecurity and invest in the necessary tools, processes, and personnel to protect their critical infrastructure.

Actions you can take against OT security threats

- Consult with supplying parties on possible attack vectors via the management plane, aim to restrict the surface(s) via RBAC, two-factor authentication and extend logging from the remote management/maintenance supplier into your SIEM.
- Zero Trust is important, also in stopping OT security threats. Zero Trust policies begin to address device restrictions and insecure-by-design PLCs, IoT sensors and controllers.
- Isolate critical infrastructure from office automation, production networks, IT devices, and staff using segmentation and micro-segmentation strategies.
- Implement two-factor authentication, including biometrics (e.g. fingerprint, voice, facial recognition, etc.), and establish role-based Identity and Access Management (IAM) for all employees, as well as privileged identity management (PIM) for administrators. Restrict access to “legacy management ports” (i.e. serial port) and implement logging of use.
- Invest in and build out SCADA/ICS, OT, and IoT-specific security expertise.
- Ensure continuous logging and analysing of network traffic (security analytics) with SIEM.
- Consult with government bodies such as the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and implement common standards such as I SA/IEC-62443 or ISA-99.
- Implement critical network security controls, such as NGFW, IPS, and Sandboxing at the edge of the OT environment; increasing the centralisation of device management and decision making; encrypting data and traffic; and given the highly sensitive nature of the sensors and systems deployed in critical infrastructure environments, establishing passive monitoring and controls within the OT environment.

Vendors in OT cybersecurity

As mentioned earlier, Fortinet, a global leader in cybersecurity solutions, offers a range of products specifically designed to address the unique challenges of securing Operational Technology (OT) environments.

Some of the main Fortinet OT solutions include:

FortiGate Next-Generation Firewall (NGFW): FortiGate NGFW provides advanced threat protection, intrusion prevention, and application control specifically tailored for OT environments. It supports various industrial protocols and can be deployed in different form factors to suit specific OT requirements.

FortiNAC Network Access Control (NAC): FortiNAC enables organisations to control and restrict access to their OT networks by enforcing strict authentication and authorisation policies. It helps organisations maintain an up-to-date inventory of their OT devices and ensure that only authorised personnel can access critical systems.

FortiSIEM Security Information and Event Management (SIEM): FortiSIEM provides centralised visibility and analytics for OT security events, enabling organisations to detect, prioritise, and respond to potential threats more effectively.

FortiSandbox Advanced Threat Protection: FortiSandbox provides an isolated environment to safely execute and analyse suspicious files and malware, preventing potential threats from infiltrating the OT environment.

FortiEDR Endpoint Detection and Response: FortiEDR offers continuous monitoring, detection, and automated response capabilities for OT endpoints, helping organisations protect their critical assets from advanced threats and targeted attacks.

FortiSwitch Secure Access Switches: FortiSwitches are designed to provide secure and reliable network connectivity for OT environments, with seamless integration into the Fortinet Security Fabric. They can be used to implement robust network segmentation and enforce security policies at the access layer.

FortiAP Wireless Access Points: FortiAPs provide secure wireless connectivity for OT environments, ensuring the protection of critical systems and data from potential wireless threats. They are fully integrated with the Fortinet Security Fabric, allowing organisations to manage and monitor their wireless networks alongside their wired networks.

These Fortinet OT solutions are designed to work together as part of the Fortinet Security Fabric, an integrated security architecture that provides seamless protection across IT and OT environments. By leveraging Fortinet's comprehensive suite of OT security solutions, organisations can safeguard their critical infrastructure, maintain business continuity, and protect their reputation in an increasingly complex threat landscape.

Palo Alto Networks offers a variety of cybersecurity solutions for OT environments, including their Next-Generation Firewall and Cortex XDR platform, which provide advanced threat detection and prevention capabilities, secure remote access, and network segmentation.

Some of the main Palo Alto Networks OT solutions include:

Palo Alto Networks Next-Generation Firewall (NGFW): Palo Alto Networks' NGFW provides advanced threat protection, intrusion prevention, and application control tailored for OT environments. It supports various industrial protocols and can be deployed in different form factors to suit specific OT requirements.

IoT Security: Palo Alto Networks' IoT Security solution provides visibility into IoT and OT devices, enabling organisations to discover, profile, and secure these devices. It offers automated policy recommendations, threat prevention, and enforcement capabilities to protect OT environments from IoT-related threats.

Cortex XDR: Cortex XDR is an extended detection and response platform that provides advanced threat detection, investigation, and response capabilities across IT and OT environments. It collects and analyses data from multiple sources, including endpoints, networks, and cloud, to provide comprehensive protection against advanced threats targeting OT systems.

Panorama Network Security Management: Panorama is a centralised management platform that allows organisations to manage and monitor their security policies and devices, including those deployed in OT environments. It enables organisations to maintain a consistent security posture across their IT and OT networks.

Prisma Access: Prisma Access is a secure access service edge (SASE) solution that provides secure, cloud-delivered access to applications, data, and services for remote users and branch offices. It can be used to enable secure remote access to OT networks and systems for authorised personnel.

Prisma Cloud: Prisma Cloud is a comprehensive cloud-native security platform that provides visibility, threat detection, and compliance capabilities across multi-cloud and hybrid environments. It can be used to secure the cloud components of OT environments and ensure the protection of critical data and services.

Palo Alto Networks' OT solutions are designed to work together and integrate with their broader security portfolio, providing comprehensive protection for organisations' critical infrastructure and systems. By leveraging Palo Alto Networks' OT security solutions, organisations can defend against the growing cyber threats targeting OT environments and maintain business continuity.

Juniper Networks is primarily known for its networking and security solutions for enterprise IT environments. While they do not specialise exclusively in Operational Technology (OT) cybersecurity, their products and services can be applied to secure OT environments in conjunction with other specialised OT security solutions.

Some of Juniper Networks' products and services that can be relevant to OT security include:

Juniper SRX Series Services Gateways: The SRX Series is a line of high-performance next-generation firewalls that can provide advanced threat protection, intrusion prevention, and application control. These firewalls can be deployed in OT environments to provide network security and segmentation.

Juniper Secure Connect: Secure Connect is a remote access solution that provides secure and encrypted communication between remote users and on-premises resources, including OT networks. It enables organisations to manage access to critical OT systems and ensure only authorised personnel can connect.

Juniper Mist Wired Assurance: This solution helps organisations manage and monitor their wired networks, ensuring high levels of performance and security. In an OT context, this can help maintain the stability and reliability of the network infrastructure that supports industrial control systems.

Juniper Sky Advanced Threat Prevention (ATP): Sky ATP is a cloud-based threat intelligence and advanced threat prevention platform that can be integrated with Juniper SRX Series firewalls to provide real-time protection against known and unknown threats targeting OT environments.

Juniper Security Director: This centralised management platform allows organisations to manage and monitor their security policies and devices, including those deployed in OT environments. It enables organisations to maintain a consistent security posture across their IT and OT networks.

Although Juniper Networks does not specifically focus on OT cybersecurity, their solutions can be used as part of a broader, multi-layered security approach to help protect OT environments. Organisations using Juniper Networks products for OT security may benefit from partnering with specialised OT security vendors to ensure a comprehensive security posture.

How can Nomios help

Transforming and securing your network is a complex and ongoing process that requires a strategic approach, careful planning, and collaboration with stakeholders. It goes beyond merely purchasing sotware tools and involves aligning technology choices with business objectives, addressing security and compliance, investing in skill development, implementing effective change management processes and addressing work culture and employee behaviour.

Here are some key factors we consider when undertaking network transformation initiatives:

1. **Assessing current infrastructure:** Conduct a thorough evaluation of the existing network infrastructure, including hardware, software, configurations, and performance. Identify bottlenecks, vulnerabilities, and areas for improvement.

2. **Defining business requirements:** Understand the specific business needs and objectives that the network transformation should address. Consider factors like scalability, performance, reliability, security, and support for emerging technologies and trends, such as cloud computing, IoT, and AI-driven applications.

3. **Developing a transformation roadmap:** Create a detailed roadmap for the network transformation, including timelines, resource allocation, and key milestones. This roadmap should align with the organisation's overall IT strategy and business objectives.

4. **Choosing the right technology and solutions:** Evaluate different networking technologies, architectures, and solutions to determine which ones best meet the organization's requirements. Consider factors like cost, performance, ease of deployment, and integration with existing systems and infrastructure.

1. **Ensuring security and compliance:** Network transformation must prioritise security and compliance, taking into account industry regulations, data protection requirements, and the evolving threat landscape. Implement appropriate security measures and controls at each stage of the transformation process.

2. **Training and skill development:** Ensure that the IT staff and network administrators have the necessary skills and knowledge to manage the new network infrastructure and technologies effectively. Invest in training and development programs to bridge any skills gaps.

3. **Change management and communication:** Network transformation can have a significant impact on an organisation's operations and workflows. Establish a clear change management process, involving all relevant stakeholders, to ensure a smooth transition and minimize disruptions.

4. **Monitoring and optimization:** Continuously monitor the performance and health of the transformed network, making adjustments and optimisations as needed. Leverage analytics and automation tools to proactively identify and address potential issues.

5. **Engaging partners and vendors:** Collaborate with technology partners, vendors, and service providers who have the expertise and resources to support the network transformation process. Their insights and guidance can help ensure a successful outcome.

Nomios provides full consultancy services to help organisations understand requirements, create high and low level design and provide full pre-staging, implementation and logistics management.

Our end-to-end managed network support services provide break-fix, device management, full NOC and SOC options together with a suite of as-a-service offerings. We adapt to meet your business needs and will provide unrivalled industry expertise; our cutomer feedback is testamony to this.

nomios

Lewis Sinclair
Technical Consultant
Nomios UK&I

Connect with Lewis on LinkedIn ***here***

We pride ourselves on being easy to do business with, our customer testimonials demonstrate this. We are uncomplicated and do our best to demystify and simplify what often seems to be an over complicated industry. Why not put us to the test? Get in touch and speak to one of our network experts and see how we can help you and your business.

nomios

Nomios UK&I Ltd.
Basecamp
2 Elmwood, Chineham Park
Basingstoke
Hampshire, RG22 8WG
United Kingdom

Find out more about Nomios OT and IoT security ***here***

Discover us

Connect with us

See what we do