TELOS ACA™

Telos®

Telos ACA for Energy

Cyber Criminals Target Critical Infrastructure: Accelerated Industrial Cybersecurity Initiatives are Required

Challenges:

The digitization of industrial operations and IT/OT convergence are creating greater security risks and larger attack surfaces for energy and other organizations in critical infrastructure.

OT/ICS network security lags behind IT security, making it difficult to effectively address the vulnerabilities in today's Industry 4.0 environments.

Solution

Proactive advanced cyber analytics as-a-service that enriches and analyzes all traffic transmitted in and out of your systems and hunts for malicious activity

Provides cybersecurity subject matter expertise without requiring organizational restructuring or additional human resources

Supports OT and IT environments to protect converged industrial environments, mitigating the risk of breaches, malware, operational disruption and the resulting reputational damage and litigation expenses

The FBI's warning about Russian state hackers targeting critical infrastructure (CI) – issued just nine months after the Colonial Pipeline hack in May 2021 – forecasts a stark future for the various organizations that support the country's essential operations. Organizations that operate CI rely on industrial technology practices to provide the required deliverables for their daily operations, to include the use of operational technology (OT). As Industry 4.0 continues to extend digitization, automation, and artificial intelligence (AI) to industrial practices, the OT environment needs to evolve and implement successful cybersecurity practices in the same manner as information technology (IT) to provide sufficient threat mitigation.

Since critical infrastructure is vital to the nation's physical infrastructure, its incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Cyber criminals understand the severity of damaging the energy sector and deliberately use threats against it to extort these types of organizations. For example, after the Russian cyber criminals hacked Colonial Pipeline, they employed ransomware asking for US $5 million. Colonial Pipeline manages 45% of gas transportation throughout the eastern U.S.; the resulting suspended transport and fuel shortages negatively impacted hundreds of thousands of people and businesses throughout the region. Cyber criminals around the globe understand the severe impact an event like this would have and use that threat to leverage similar organization through ransomware, with the total cost of attacks averaging US$4.5 million per IBM's "Cost of a Data Breach 2022."

Digital Convergence, IT/OT Integration Create Greater Threats to Energy and Utilities

Due to the physical infrastructure and industrial services provided by the energy sector, the industry is required to manage both IT and OT environments. As the industrial landscape transitions to digitization, automation, and AI, IT/OT convergence has become a greater necessity. Unfortunately, the security of OT infrastructure has lagged behind that of IT security, allowing cyber criminals to exploit these vulnerabilities to conduct malicious cyber operations. According to Ponemon Institute's 2021 State of Industrial Cybersecurity Report, only 35% of companies have unified security strategies that secure both the IT and OT environment, demonstrated by the 63% of organizations that had an ICS/OT-related cybersecurity incident between 2020 and 2021. Additionally, only 21% of companies say their ICS/OT program activities are fully deployed and that their senior leadership is regularly informed about the efficiency, effectiveness and the security of the OT program.

According to the Ponemon report, a major reason for the lack of OT cybersecurity development is that the majority of ICS/OT security is under the supervision of the VP of engineering. This role makes sense for ensuring that sustainable and effective industrial systems are implemented to support critical operations; however, cybersecurity subject matter expertise is needed to implement sustainable security solutions to compete in the new digitized industrial environments, a need that will continue to grow as automation, AI, and digitization expand.

The Solution: Proactive Cyber Threat Intelligence

An excellent way to provide cybersecurity without hiring new employees or consultants is to implement a solution-as-a-service through a third-party vendor. Employing a cyber analytics service that enriches and analyzes all traffic transmitted in and out of your systems to hunt for malicious activity will provide subject matter expertise without requiring restructuring within the organization. Additionally, this will create a sustainable solution that is not impacted by positional shifts within the company. Cyber analytics will not only support the OT environment but also the IT environment as well. A solution of this scale will be able to ingest the data from both environments, illuminating the hacker ecosystem and, in return, mitigating data theft and keeping malware and distributed denial of service (DDoS) attacks from disrupting operations.

The Telos Advanced Cyber Analytics solution is a service that will mitigate these risks. Telos' solution will enable the partner to know in real time what malicious activity is occurring, resulting in the cyber attack being stopped before any significant damage and financial impact occurs to the organization's systems. Additionally, by implementing the security solution, the risk of class action for negligence is mitigated due to the organization taking all necessary steps to not only implement cybersecurity principles to the IT system but also the OT. Telos Advanced Cyber Analytics will mitigate the risk of a data breach, malware, operation disruption, reputational damage, and long-term litigation expenses.

Learn more at
www.telos.com/telos-advanced-cyber-analytics/

Telos® Solutions that **empower** and **protect** the enterprise.™