Secure the Future: Energy Sector

Brian Sowers

Columbia University

Executive Summary

Due to the critical nature of its resources, the international energy sector has and is being targeted by malicious cyber threat actors including Advanced Persistent Threats (APTs), state—sponsored actors, and hacktivist groups. A successful attack on an energy supplier has devastating effects, and it is of the utmost importance to governments to ensure adequate cybersecurity is implemented for these organizations. A loss of power is a loss of life. Recent attacks such as Stuxnet, the Colonial Pipeline attack, and Russian attacks on Ukrainian power plants prove this. With the advent of the Internet-of-Things, more companies are becoming increasingly connected to the Internet, and the energy sector is no exception. This rapid onset of connectivity has brought with it more avenues of attack for malicious actors and this report summarizes the current difficulties and challenges the energy sector faces. This report hopes to illuminate the future of the energy sector's cybersecurity posture by looking at what current trends in technology potentially offer the best solution moving forward.

Section 1: Adversarial Behavior, Artificial Intelligence and Machine Learning

Most famously, a worm called Stuxnet was discovered in 2010 that sought to deprecate Iran's nuclear program. In April 2022, an attempted cyber-attack on a Ukrainian energy provider would have "deprived roughly two million people of electricity and made it difficult to restore power" (UKRAINE: Timeline of Cyberattacks on Critical Infrastructure and Civilian Objects, 1) had it not been prevented. In the summer of 2021, the company Colonial Pipeline suffered an attack when one of its oil pipelines was made inoperable after an adversary compromised the system with a single known password. Industrial Control Systems (ICS) use AI and machine learning to manage energy flow and optimize energy usage. Machine learning uses predictive analytics to estimate how much energy will need to be stored and/or distributed to save money and help prevent unexpected outages (Cyberpedia, 1). SD-WAN solutions with ML-based capabilities include intelligent alerts and recommendations for network changes after analyzing how different events affect the network and help to improve application performance and security (Energy, 1). Cortex XDR, a SOAR, uses AI-driven local analysis to block malware and detect and respond to malicious activity using automated playbooks.

Section 2: Threat Intelligence, Intelligence Sharing and Adversary Playbooks

Two sources needed in the energy sector's threat intelligence are Tech Intelligence (TECHINT) and Cyber Intelligence (CYBINT). TECHINT is defined as "intelligence gathered on equipment and material to assess the capabilities of adversaries" (Secure Business Systems Operations Module 2, 9). Knowing what intelligence can be gathered from the sector's own equipment is just as crucial as the intelligence used to determine the capabilities of adversaries. CYBINT is defined as "the collection of data via signals intelligence, open-source intelligence, and electronic intelligence," (Secure Business Systems Operations Module 2, 11). For example, knowing what system responses are made from adversarial scanning attempts will help organizations ascertain what information can be aggregated by adversaries. Searching available information about its systems online will also help to understand what the adversary knows. Cortex XSOAR is a tool that utilizes playbooks to help automate responses to technical indactors for the sector and reduce response time Sharing adversarial information is crucial amongst the energy sector and other communities. Both the Protected Critical Infrastructure Program (PCII) and Cybersecurity Information Sharing Act (CISA) help to facilitate information sharing between utilities and the intelligence community (Mission Support Analysis Report, 109).

Section 3: Data Islands and Enterprise Cloud Services

Three data islands I expect to see in the energy sector are authentication keys stored on physical devices, mobile endpoints, and classified information that is prevalent in nuclear energy production. Limiting opportunity to attack by minimizing exposure, i.e. network connectivity, helps ensure the integrity of such data.

An enterprise cloud-based security management system I would implement would be a secure access service edge (SASE) solution to securely connect users and access to corporate data. "A SASE solution must provide consistent security services and access to all types of cloud applications (e.g., public cloud, private cloud and SaaS) delivered through a common framework" (Palo Alto Networks, 2023) that builds upon the Zero Trust Architecture Model. This ensures users are who they really authenticate as. Cloud-based applications will be categorized as sanctioned, tolerated, or unsanctioned and require that only sanctioned and tolerated applications be used. Lastly, I would use Next Generation Firewalls from Palo Alto to inspect all traffic – including applications, threats, and content. Additionally, I would use Palo Alto's Prisma to help secure SaaS applications.

Section 4: DevSecOps, SOAR and Enterprise Security

My solution for secure authentication to an application would be to first mandate a cyber security awareness program so end users understand what to be aware of. Second, I would implement SASE that depends on the aero trust model architecture "to provide directto-app connectivity while reducing the attack surface without impacting performance or the user experience" (Palo Alto Networks, 2023). I would use Palo Alto's Prisma to help secure SaaS applications and the hybrid workforce. Cortex XDR, a SOAR that uses playbooks, will be used to automate threat responses to malicious activity that will help to reduce manual interaction with alerts and analyst fatigue. I will use a DevSecOps approach to help achieve API security. Enterprise solutions should be adopted for organizations wishing to secure their networks. Doing so will ensure they get the best-in-class protection without needing any of their personnel having a high degree of technical knowledge. Cloud-based enterprise solutions eliminate infrastructure costs to organizations and provide the personnel needed to properly implement the solutions. Palo Alto offers a multitude of enterprise-based solutions such as Prisma, Cortex XDR, and Next Generation Firewalls (Palo Alto Networks, 2023). Unless a network is configured to a high degree of complexity, independent security product implementations should be limited. They are frequently outdated and rarely maintained adequately by organizations, thus providing attack vectors for actors.

Conclusion

Due to the rapid modernization of Operation Technology (OT) networks in the energy sector specifically, many Information Technology (IT) protocol suites are used, such as FTP and RDP servers. Power distribution control and power grid monitoring is now done remotely by digital equipment communicating with protocols originally designed to be implemented by Information Technology (IT) networks. Adversaries are now able to use many of the same methods to gain access to OT networks as they would with IT networks. A large number energy producers in the sector continue to use Commercial-Off-The-Shelf (COTS) (Cairl, et. al, 88) equipment to meet customer and business demand, but these products are prone to be out of date in software upgrades or are completely no longer supported by the manufacturer. Security analysts suffer from fatigue and have become desensitized from security alerts. The solution is to use cloud- based enterprise solutions, such as Cortex XDR and Prisma from Palo Alto Networks, to help eliminate vulnerabilities and exposure to attackers. The future state of cybersecurity will include AI driven analysis and machine learning to identify trends in energy usage and improve security. Current solutions such as perimeter-based security are quickly becoming out of date.

Works Cited

Cairl, Brian, and Keliris, Anastasis, and Khorrami, Farshad, and Krishnamurthy, Prashanth, and Hossein Salehghaffari. “Machine Learning-based Defense Against Process-Aware Attacks on Industrial Control Systems.” Accessed: 28 January 2023.

“Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector.” *Mission Support Center Analysis Report.* “https://www.paloaltonetworks.com/CourseFiles/Cyber_Threat_Vulnerability_Analysis_U.S._Electric_Sector.pdf. Accessed: 28 January 2023.

"Purpose built in the cloud to secure today's hybrid workforce." *Palo Alto Networks.* https://www.paloaltonetworks.com/sase/access. 28 January 2023.

“Secure Business Operations Module 2, https://s3.amazonaws.com/assets.paloaltonetwor ksacademy.net/sbo/Business_Operations_Module_1.pdf. Accessed: 28 January 2023.

"Top 10 applications of AI and Robotics in Energy Sector." *Energy.* https://energydigital.com/top10/top-10-applications-of-AI-and-Robotics-in-Energy-Sector. 28 January 2023.

“UKRAINE: Timeline of Cyberattacks on Critical Infrastructure and Civilian Objects.” *Cyber Peace Institute.* 08 June 2022. https://cyberpeaceinstitute.org/ukraine-timeline-ofcyberattacks/. Accessed: 30 October 2022.

“What is Machine Learning?” *Palo Alto Networks*. https://www.paloaltonetworks.com/cyberpedia/what-is-machine-learning. Accessed: 28 January 2023.

"Why Machine Learning (ML) and Artificial Intelligence (AI) Are Key Technologies for SD-WAN." *Cyberpedia*. https://www.paloaltonetworks.com/cyberpedia/what-i-machine-learning-in-sd-wan. Accessed: 28 January 2023.