Why Control Systems Environments Need Cortex XSOAR

Digital transformation and its products are continuing to provide customers with an improved user experience. From on-demand reporting on critical assets to enhancing ease of use in supply chains, the advancements and the technology driving them are quickly working their way into every facet of business operations. These enhancements also open new security challenges by increasing an organization's attack surface and potential cybersecurity risk. In their efforts to remain competitive in the digital world while protecting business-critical systems and assets, cybersecurity professionals must continually evaluate and consume new technologies.

The cybersecurity industry and its solutions are growing rapidly, and cybersecurity professionals constantly labor to keep pace with the technology fueling digital transformation. Investing in new technologies to gain market share through product superiority is a standard business practice, especially as more companies adopt a digital approach to their daily operations.

As companies dependent upon industrial automation and control systems (IACS) conform to digital transformation practices, their process control networks (PCNs) are exposed to the same evolving cyberthreats as IT. The additional risk introduced by this increased connectivity affects both the business and any surrounding communities, with potentially devastating consequences depending on the business's industry and products.

The world is facing a massive shortage of qualified cybersecurity personnel, especially when looking for security professionals with the necessary background to support the specific needs and concerns of operational technology (OT). The threat landscape of OT systems is evolving rapidly as integrations with IT systems grow. Thus, security professionals are struggling to keep up with the volume of alerts and repetitive tasks on the IT side, let alone tackle an ecosystem that generates even higher volumes of alerts and notifications. Introducing security solutions within the OT environment layers on additional requirements and expertise to safely manage and operate security solutions.

Amid the rapidly growing threat landscape, IT security teams began merging three distinct technology markets—security orchestration and automation, security incident response platforms (SIRP), and threat intelligence platforms (TIP)—to combat the problem. This blending of technologies, labeled by the Gartner research group as security orchestration, automation, and response (SOAR), enables IT organizations to collect, aggregate, and across a broad set of tools. Providing the best results when working with high-fidelity alerts.

What Is Cortex XSOAR?

Palo Alto Networks Cortex® XSOAR helps security operations centers (SOCs) and security analysts scale up their existing resource capabilities, improve incident response times, and capture evidence while collaboratively resolving issues. Cortex XSOAR combines intelligent automation using bots and playbooks.

Alert data ingested from various sources is used to generate incidents. Every incident category can be handled by a playbook that collects the required information and performs enrichment on involved network entities, saving security analysts time and effort. In some instances, playbooks include automatic response steps, minimizing what the analyst may need to do manually.

Some security incidents need human interaction and collaboration from other analysts or subject matter experts (SMEs), as would be the case in an ICS/SCADA environment. Cortex XSOAR facilitates this with a unique feature called ChatOps. This virtual war room allows SOC members to work together to investigate and resolve cyberthreats. In the highly customized OT space, this feature invites stakeholders and SMEs to be a part of the process, helping ensure that production does not suffer due to a security analyst's lack of knowledge of system interworking. War room meetings are interactive, and a bot provides team members with all relevant data to support the investigation. In addition to communicating with each other, participants can direct the bot to take action, assign tasks, and set due dates for those tasks.

As security analysts and stakeholders investigate a potential breach, it is a best practice to collect evidence. Cortex XSOAR helps by collecting and documenting evidence as well as tying it to the appropriate chain of custody in case legal actions are required. All processes and actions taken to resolve the incident are recorded and become shareable for those working on similar or future incidents. Cortex XSOAR automatically generates reports after addressing incidents, and more than 100 predefined automation scripts quickly and easily incorporate into existing and future playbooks.

Cortex XSOAR playbooks contain all the steps to handle a specific type of incident. These can be automated playbook-run tasks or manual steps to be taken by an analyst or system stakeholder, providing the power and flexibility to adjust playbooks as the threat landscape evolves. The system can also detect duplicate incidents, empowering analysts to address multi-pronged attacks consistently using one team, instead of having multiple teams resolving the same issue.

Cortex XSOAR is designed to expedite the handling of cyberthreat incidents, orchestrating and automating the processes and procedures required. It can also automate the enrichment of data from external systems—another mundane, time-consuming task for human analysts. With time and effort saved, a security analyst can gather the necessary documentation and metrics, and then collaborate with peers in a single pane of glass to address a cyber incident.

To learn more about the power and capabilities of Cortex XSOAR, visit us online.

Overcoming Security Challenges with Better SOAR

As the threat landscape expands, the number of disruptive threats to IT and OT is growing far more quickly than the number of qualified security personnel. Cortex XSOAR can help secure both your carpeted and plant floor environments. Businesses in all sectors, and of all sizes, can use Cortex XSOAR to improve their OT security posture and agility to quickly identify and respond to cyberthreats in their control systems infrastructure. Both IT and OT security professionals can apply consistent security across business units according to their specialized needs.

Cortex XSOAR can be customized to address the OT team's needs in a way that ensures minimal production impact and safe, expedient resolution of threats based on OT best practices and procedures. This is key to resolving the problems in systems designed to maintain high uptimes, and safety is a primary concern. Cortex XSOAR supports your cybersecurity and OT teams simultaneously. The following sections describe how.

Improving Operational Efficiency and Efficacy

Managing disparate security products of IT systems alone puts enormous strain on SOC security personnel. Adding disparate OT-centric security systems compounds this issue further. These separate security technologies require continuous monitoring and tuning to ensure proper performance, and they may generate tens of thousands of notifications and alerts, ultimately leading to alert fatigue for those charged with their "care and feeding." Security monitoring for OT environments is even more strenuous due to the nature of the cyber-physical assets that must be protected.

Cortex XSOAR can help ease the management of cybersecurity in OT systems. With playbooks, it has the potential to help with day-to-day operations as well. Not restricted only to addressing possible compromises, playbooks can be used in routine activities like the deployment of new systems and devices, in addition to other capabilities that any OT group would find beneficial, especially when it comes to the deployment of cyber-physical devices.

Ensuring Higher Quality Intelligence Through a Holistic View of IT and OT Systems

When addressing sophisticated cyberthreats, in-depth understanding of tactics, techniques, and procedures (TTPs)—and the competency to accurately and efficiently identify them—is essential. Aggregation of security data from across the entire enterprise and control system domains is crucial to a strong cybersecurity posture. By ingesting and validating multiple data sources (e.g., TIPs, exchanges, industry-related ISACs, firewalls, intrusion detection systems, and SIEMs) through Cortex XSOAR, your IT-OT SOC becomes intelligence driven. With this merged data, you gain better visibility across all business units, giving your security personnel the power to contextualize incidents for IT and OT networks.

Digital convergence is progressing at an accelerated pace in the OT space. Quick changes and the demand for more information from the shop floor require more connections to devices capable of protecting themselves from the evolving threat landscape. Cortex XSOAR enables security personnel and SOCs to keep up with the pace of targeted OT threats. Because Cortex XSOAR playbooks cover a process and procedure from end to end, they guide analysts through all necessary steps and departments to notify them, complementing the OT workflow. Automation teams are always looking for tools to help streamline and document their processes, and playbooks can be a powerful tool for doing this.

Playbooks are currently used in the notification process during an investigation. When incidents occur, depending on the severity, departments from IT Security to HR may receive notifications requesting they proceed with key actions. If the potential breach involves OT systems, notifications will be sent to those stakeholders as well. This end-to-end coverage can also be useful in the day-to-day maintenance of OT systems to ensure all necessary personnel are in the loop and addressing their part, with the added benefits of initiating, updating, and closing the change management requirements particular to OT.

Enhancing Incident Response

Breaches to a company's ICS/SCADA environment can have cataclysmic and cascading effects on the environment and community. Unauthorized access into ICS/SCADA networks has resulted in the loss of proprietary data and intellectual property, which can leave a company in financial ruin due to reputational damage and loss of public trust. Cortex XSOAR helps IT and OT teams reduce their mean time to detect (MTTD) and mean time to respond (MTTR). More importantly for OT organizations, enhanced incident response leads to a faster mean time to recovery—the most crucial aspect for a team concerned with maintaining both system uptime for maximum production and, more importantly, operational safety to prevent loss of property or life.

Many organizations currently use playbooks to ensure that enterprise security and IT teams respond to potential incidents consistently and effectively. They define the processes and procedures that keep incident response in line with compliance obligations. Until recently, these processes and procedures were manual, which resulted in inconsistencies in data collection and pockets of specialized knowledge within teams, with certain individuals having an aptitude for addressing the situations. A common parallel in OT environments is how systems are designed, built, and deployed. Cortex XSOAR can help OT teams by turning these tasks into playbooks in the digital library, ensuring that devices are correctly deployed with proper security in place.

Having system deployments housed in the playbook library provides a means for users uninitiated in controls systems to look up and learn about the system in question. Understanding how an OT process works is vital to ensuring it does not get shut down inadvertently. Playbooks also guide SOC analysis through remediation steps, enabling less-experienced team members to act with confidence and surgical precision. For instance, playbooks can guide inexperienced technical personnel through system deployments. Playbooks are adaptable, which makes their use in the OT environments ideal.

Conclusion

IT teams figured out years ago that bolt-on and just-in-time security measures are ineffective in the digital world, and OT teams must establish the same mindset. A belief in "security through obscurity" and air gaps proves less and less effective every day as attacks become more targeted against OT systems. Many motorcycle riders believe there are two types of riders: those who have crashed and those who will. Everyone eventually falls. Cybersecurity professionals should hold a similar belief: their systems are either being attacked or about to be attacked, with the worst-case scenario being that the system is already compromised and they're not yet unaware.

OT systems present unique challenges to security professionals for several reasons. For one, security measures tend to slow response, which is unacceptable in systems controlling cyber-physical devices. Other related obstacles include the shortage of security professionals with a working knowledge of control systems, coupled with the fact that inadequate documentation exists to aid effective and safe implementation of protection in many deployments. In many instances, what data does exist is siloed, making it hard for analysts to access and make sense of the nature of the attacks.

Cortex XSOAR helps to address these challenges by gathering all relevant data, even from sources that may seem unrelated, allowing for the buildout of workflows that cater to the particular needs of an industrial controls network's operational requirements. It also provides bot-aided war rooms where security analysts and SMEs can safely and securely collaborate on the best course of action. Most importantly, Cortex XSOAR provides automatic documentation of all steps and processes taken to validate and resolve issues or incidents, creating a knowledge warehouse for first responders.

Visit us online to learn more about how Cortex XSOAR can help document and secure your ICS and SCADA environments.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com