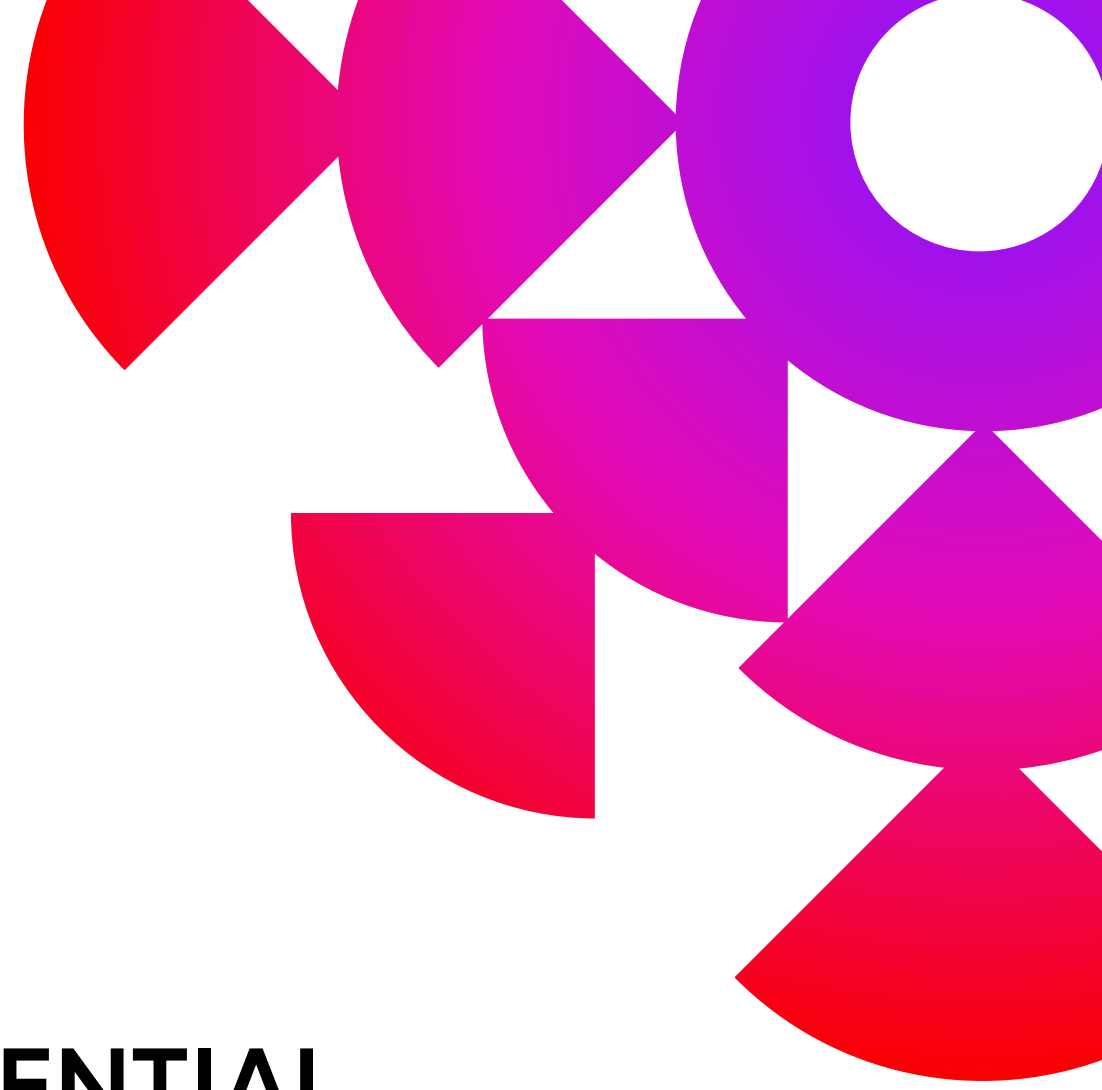


# FIVE ESSENTIAL STEPS FOR A CONVERGED IT/OT SOC

By Guilad Regev, SVP of Customer Care at Claroty

CLAROTY

# INTRODUCTION

Until recently, enterprise operational technology (OT) environments have been air-gapped from organizations' information technology (IT) environments and connections to the internet. As such, OT has long been immune to a great extent from cyber threats, and therefore, cyber defense has not been a priority until relatively recently. The importance of OT cybersecurity has increased dramatically with digital transformation, because the convergence of the distinct worlds of IT and OT introduces cyber risk to highly vulnerable industrial control systems (ICS).

When it comes to the need for strong industrial cybersecurity, many enterprises received a major wake-up call when NotPetya—widely regarded as the one of the costliest and most destructive cyber attacks in history—caused billions of dollars in damages and affected IT and OT environments alike. NotPetya's infiltration of OT was largely unintentional and opportunistic collateral damage made possible by IT/OT convergence. However, in the years since NotPetya, adversaries have grown more deliberate in their targeting of industrial technology, exploiting poor IT/OT segmentation to gain access to targeted systems. To combat the growing threat of cyber attacks against OT, CISOs are faced with the task of protecting industrial technology that was not designed with security in mind.

As the digitization of OT and other industrial technologies grows increasingly ubiquitous, security leaders cannot afford to leave things to chance when it comes to the threat of a cyber attack against critical infrastructure and industrial processes. That being said, security teams face some unique challenges in defending OT assets. In particular, the use of proprietary protocols, a lack of standardized technology, and the complexity of OT environments make traditional IT security tools, legacy systems, and network equipment ineffective—thus necessitating purpose-built industrial cybersecurity tools.

## MAKING THE CASE FOR A CONVERGED IT/OT SOC

While OT does require specific tools for industrial cybersecurity, one area where enterprises can leverage their existing resources and personnel is the security operations center (SOC). At Claroty, we believe the best industrial cyber-defense strategy is to present a unified front against threats to IT and OT assets by establishing a converged SOC that protects these once-separate technology environments in a holistic manner.

The SOC is already widely accepted as a hallmark of mature IT security programs. By consolidating OT security with your existing, IT-centric SOC, you can achieve greater visibility across the entire enterprise, enhanced security monitoring, and comprehensive threat mitigation. IT/OT SOC convergence also enables a standardized approach to enterprise security that facilitates a secure digital transformation by enabling rapid configuration changes, new policy implementation, and compliance to new regulations or industry standards from one view. Collectively, these benefits amount to better risk management.

Like any major cybersecurity initiative, executive buy-in is typically a prerequisite for moving forward with a consolidated approach to IT and OT security. To do this, you will need to clearly articulate the benefits of a converged IT/OT SOC, which we will discuss in this section.

## PERFORMANCE ADVANTAGES

The holistic approach to IT and OT security detailed in this white paper grants the CISO a singular, cohesive view of risk for the entire organization. Moreover, a converged IT/OT SOC team that is accountable for all risks allows for centralized incident response that includes triage, investigation, and mitigation. As a result, organizations are able to respond to security incidents significantly faster and more effectively.

Cyber threats to OT almost always enter via the IT network before spreading laterally to the OT environment. For this reason, a singular OT security task force that operates separately from existing IT security teams would be far less effective and significantly more costly than an integrated IT/OT SOC.

## EFFICIENCY ADVANTAGES

In addition to delivering the performance advantages described above, properly executed convergence of the SOC to secure IT and OT can significantly reduce technology total cost of ownership (TCO) while utilizing the skills of existing staff.

### TCO: PEOPLE

Since the approach to IT/OT SOC consolidation detailed in this white paper largely relies on leveraging existing personnel rather than hiring new employees, it is designed to optimize and expand upon current security capabilities with minimal headcount impact. Moreover, this approach requires almost no change in SOC personnel's method of operation. By partnering with OT-security vendors that deliver contextual, actionable alerts that can be consumed by existing IT analysts, along with the training necessary for these personnel to respond to these alerts, organizations can broaden the scope of their security team in a highly efficient manner. Furthermore, an integrated IT/OT SOC eliminates the need for redundant roles across two separate teams.

### TCO: TECHNOLOGY

Executed properly, IT/OT SOC consolidation can also substantially reduce technology TCO and complexity, since this approach encourages the use of existing tools whenever possible. Organizations can maximize ROI on existing security-management interfaces, detection and response tools, and network-security technologies by integrating OT security datasets, alerts, and forensic information with IT security tools and datasets. In addition to cost advantages, the consolidation of IT and OT toolsets also enables the SOC to perform more centralized maintenance and upgrades that cover the enterprise network as a whole.

# FIVE ESSENTIAL STEPS FOR ESTABLISHING A CONVERGED IT/OT SOC

When it comes to establishing a converged IT/OT SOC, attaining stakeholder buy-in from leadership is just a precursor to the real work. Based on Claroty's experience guiding industrial enterprises across the globe successfully through this journey, we have identified some essential steps that have proven instrumental in optimizing the efficacy, efficiency, and implementation time of such initiatives.

While in most cases, the appointment of an IT/OT cybersecurity program manager should be the first step taken in this process, the order in which the following steps are implemented may be tailored to your organization's requirements, existing capabilities, and resources.

## APPOINT A DESIGNATED IT/OT CYBERSECURITY PROGRAM MANAGER

Once you attain the stakeholder support necessary to move forward with IT/OT SOC consolidation, you need to designate one individual to lead this initiative, reporting directly to the CISO. The IT/OT cybersecurity program manager will play a central role throughout the remaining steps described in this white paper, so great care should be taken to select a strong, detail-oriented leader to oversee this undertaking.

Ideally, the IT/OT cybersecurity program manager should be appointed internally. In large part, this is because having strong, preexisting working relationships within the organization can be valuable for overcoming some of the challenges involved with building such a program. In addition, those tasked with appointing the program manager will have a clearer understanding of their work ethic and leadership style when hiring internally. However, given the importance of the role, it should be treated as a full-time position in itself, rather than an additional responsibility taken on.

Given the differing—and sometimes conflicting—priorities of IT and OT personnel, the IT/OT cybersecurity program manager must be capable of finding middle ground and moving these once separate teams toward common objectives. The individual in this role needs to be able to serve as a leader, mentor, and educator that can help IT and OT personnel understand each other's differing perspectives in order to work together to mitigate business risk effectively.

For instance, while IT personnel may err on the side of implementing patches and compensating controls to minimize the likelihood of an incident, their OT counterparts may be more concerned with how the downtime needed to implement these controls will disrupt operational continuity. Strong leadership can be instrumental in overcoming these inherent tensions, making the role of the IT/OT cybersecurity program manager especially crucial.

## ACHIEVE OPTIMAL ALIGNMENT WITH EXISTING CYBERSECURITY CAPABILITIES

Since maximizing ROI is one of the key advantages to a consolidated IT/OT SOC, it is important to leverage your existing cybersecurity infrastructure as much as possible. This necessitates a thorough assessment of these current capabilities, with the objective of identifying areas in which tools already at your disposal can be leveraged, while zeroing in on gaps in existing technology where you will need to bring in new solutions. The objective of such an evaluation should be to

identify opportunities to optimize utilization of existing capabilities while augmenting them with additional capabilities when necessary.

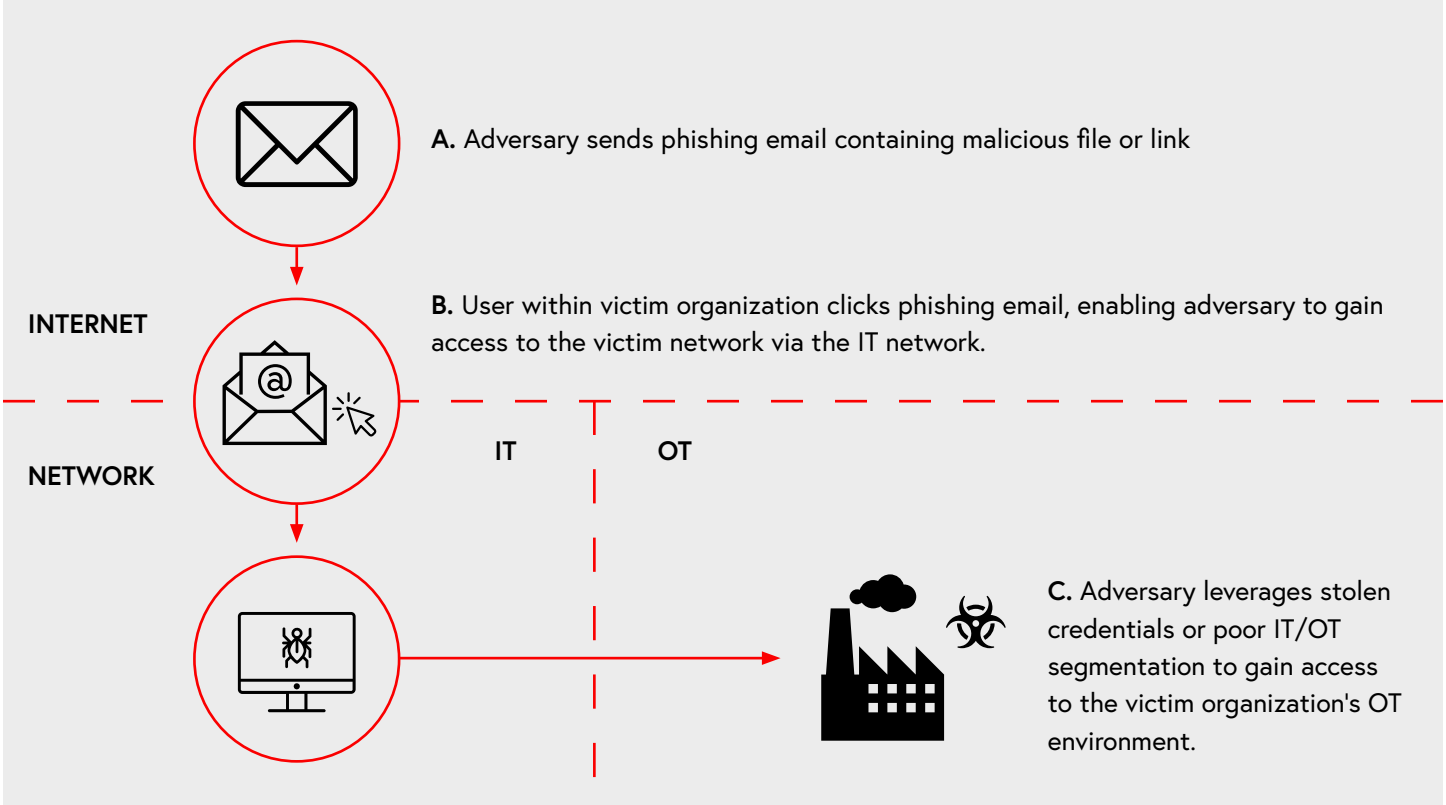
When it comes to closing technology gaps in your OT security capabilities, integrations and vendor strength should be top of mind. It's important for these new solutions to be compatible with existing IT security tools as much as possible. When evaluating potential technology integrations for your SOC, decision makers should take care to assess alternatives based on the value and functionality they deliver, rather than simply checking off various boxes.

Your SOC team should also have a centralized system that allows for easy access to all key resources, including integrations with SIEM systems, such as QRadar, Splunk, and ArcSight; SOAR tools, such as Splunk Phantom, Cortex XSOAR from Palo Alto Networks, IBM Security SOAR; and full restful API.

A strong, centralized ecosystem of integrations can significantly bolster ease of maintenance and upgrades, while also enabling automatic health checks and monitoring. Integrations also facilitate the incorporation of existing standard operating procedures (SOPs) and other playbooks into the converged IT/OT SOC.

## GAIN VISIBILITY INTO IT AND OT SECURITY ALERTS WITHIN THE OT ENVIRONMENT

With increased interconnectivity to IT networks, OT environments are exposed to IT-centric cyber threats they were previously isolated from. Over the past several years, cyber attacks such as WannaCry and NotPetya have wrought havoc upon OT environments around the globe. While devastating, these attacks have also led to increased awareness of the need to detect the cross-proliferation of IT cyber threats within OT environments.




*Typical cyber-attack trajectory for targeting OT environments.*

As shown in the diagram on the previous page, cyber threats to OT typically enter the enterprise technology environment via the IT network, before moving laterally to compromise OT assets. Given this typical infection pattern, it is crucial to have unified visibility across IT and OT environments.

Since SOC personnel are already trained to handle IT security alerts, it is often the case that only minimal changes need to be made to existing playbooks to make them applicable to OT. And since your team likely has existing access to IT security technologies capable of detecting IT cyber threats, all that is required of this step is to ensure those abilities are properly applied to your OT environment. However, your team will need purpose-built technology that effectively establishes visibility into the OT environment in order to take advantage of these existing capabilities.

Once your SOC has visibility into IT security alerts, the next task is to gain visibility into OT-specific alerts. When seeking to establish visibility into your OT environment, you should be wary of the fact that not all vendors who claim to offer these capabilities offer the level of accuracy and granularity required for your IT/OT SOC. To effectively monitor and defend against threats to their organization's OT environment, IT security teams need real-time visibility into three integral dimensions:

- **Asset Visibility:** Having detailed visibility into all devices on an OT network, covering extensive attributes—such as model number and firmware version—is essential for identifying and assessing vulnerabilities with precision.
- **Network Visibility:** IT security personnel also need thorough visibility and monitoring of the bandwidth, actions, and changes made during all active and past OT network sessions. This visibility enables easy, rapid detection of misconfigurations, traffic overloads, and other issues which may pose risks to reliability, availability, and safety.
- **Process Visibility:** Being able to track OT operations—as well as the code section changes and tag values for all processes which involve OT assets—is also crucial for identifying abnormal changes in OT process values or unusual behaviors indicative of an early-stage attack, operational reliability issues, or other potential risks within your industrial environment.

## DESIGNATE A CYBERSECURITY SITE LEADER (CSL) FOR EACH OT SITE

Likely the most involved step outlined in this white paper—depending on the number of sites your team is responsible for securing—will be the need to designate an OT cybersecurity site leader (CSL) at each of your organization's physical OT sites who will serve as the eyes and ears of your converged IT/OT SOC for that location.

The cybersecurity site leader (CSL) for each facility will serve as a critical liaison between OT personnel and the SOC. In contrast with the IT/OT cybersecurity program manager role, which involves a great of strategic leadership, the CSL role is an additional responsibility taken on by a designated on-site staff member to serve as a point person in the event of an incident. As such, the CSL must be knowledgeable about SOC procedures, requirements, and objectives—or alternatively, undergo thorough education and training on these subject matters. The CSL must also be able to speak the language of plant stakeholders and understand their roles well enough to work with them effectively in order to resolve critical issues.

Despite the importance of the CSL role, this responsibility can typically be assumed by an existing staff member and be handled alongside their existing work responsibilities. During a security incident, the CSL must be prepared to lead rapid response, coordinating with SOC and site-specific OT personnel. The CSL must be able to accurately gauge the severity of the event and weigh the tradeoff between the risk at hand and the potential operational disruptions that mitigation actions could cause. This level of nuanced decision-making necessitates proper training, as well clear communication of expectations regarding standard operating procedures.

The training curriculum for CSLs will likely vary based on your organization's unique requirements, but specific areas of focus will typically include connectivity architecture, management of servers and Active Directory, and how to interpret security alerts and respond to them accordingly.

## Traits of an Effective Cybersecurity Site Leader

- Strong understanding of OT assets, systems, and security risks
- Knowledge of and familiarity with the network infrastructure of their plant
- Ability to communicate and leverage support from the converged IT/OT SOC, IT and security personnel, and other relevant parties
- Fast learner and quick problem solver

## What Cybersecurity Site Leaders Need to Succeed

- Initial CSL training, followed by additional trainings to familiarize with new SOPs
- Awareness of the most relevant threats to their designated site and how to monitor, detect, and remediate these threats
- Clear expectations for communicating with the SOC, PSIRT, and other relevant parties
- Participation in all IT and OT initiatives at plants to better understand the changes to the environment, threat landscape, and proactive mitigation

## Cybersecurity Site Leader: Key Responsibilities

- Serve as both the "eyes" and "hands" of incident response
- Detect and remediate critical vulnerabilities
- Support the secure deployment of new industrial technologies
- Ensure business continuity and compliance with cybersecurity policies and regulations

## ESTABLISH A PSIRT TASKED WITH HANDLING STANDARD OPERATING PROCEDURES (SOPS)

Having appointed a CSL for each physical OT site, the next step is to establish a product security incident response team (PSIRT), which will be in charge of overseeing all OT security practices and standard operating procedures (SOPs). By empowering your newly converged IT/OT SOC with purpose-built SOPs, the PSIRT will enable your organization to strengthen its holistic industrial cybersecurity across IT and OT environments over time by continuously adding new responses and tailoring existing responses as your organization encounters new types of threats and incidents. The PSIRT should also be tasked with investigating escalated OT security alerts, which can provide them with the insight needed to develop new SOPs, while refining existing ones.

For smaller organizations, the PSIRT role(s) could be entrusted to existing employees in order to avoid unnecessary costs of hiring new personnel. Qualified individuals may include members of the security team who are familiar with OT processes or, conversely, personnel from the OT side with cybersecurity knowledge. For organizations with large IT/OT environments, hiring or appointing a dedicated individual or team to focus primarily on operating the PSIRT may be beneficial.

When it comes to developing SOPs for your converged IT/OT SOC, it is important to remember that it's not necessary to reinvent the wheel, so to speak. It is best to start with some standard SOPs for addressing common scenarios. It must be noted that the same situation may require a different response in an OT context than in an IT context. As such, it's important for security leaders who are largely unfamiliar with OT to seek guidance and expertise in establishing these initial SOPs.

In any situation where the IT/OT SOC encounters an unfamiliar situation in which existing SOPs are not effective or applicable, they should coordinate with the PSIRT to determine the most appropriate course of action. When necessary, the PSIRT may escalate the alert to external cybersecurity services, typically in scenarios where the threat is severe and the most effective course of action is unclear.

Once the incident at hand has been addressed, the PSIRT will write a new SOP detailing how to respond to the event next time it occurs. This new response procedure will be added to the existing SOP repository for future reference and training for CSLs and IT/OT SOC personnel.

# CONCLUSION

The five essential building blocks of a converged IT/OT SOC described in the previous section are ambitious, but they are necessary for managing risk effectively within industrial environments. The ease, effectiveness, cost efficiency, and speed at which they can be implemented can be dramatically enhanced by partnering with a vendor that has tried-and-true expertise, experience, and purpose-built technology for securing industrial technology environments.

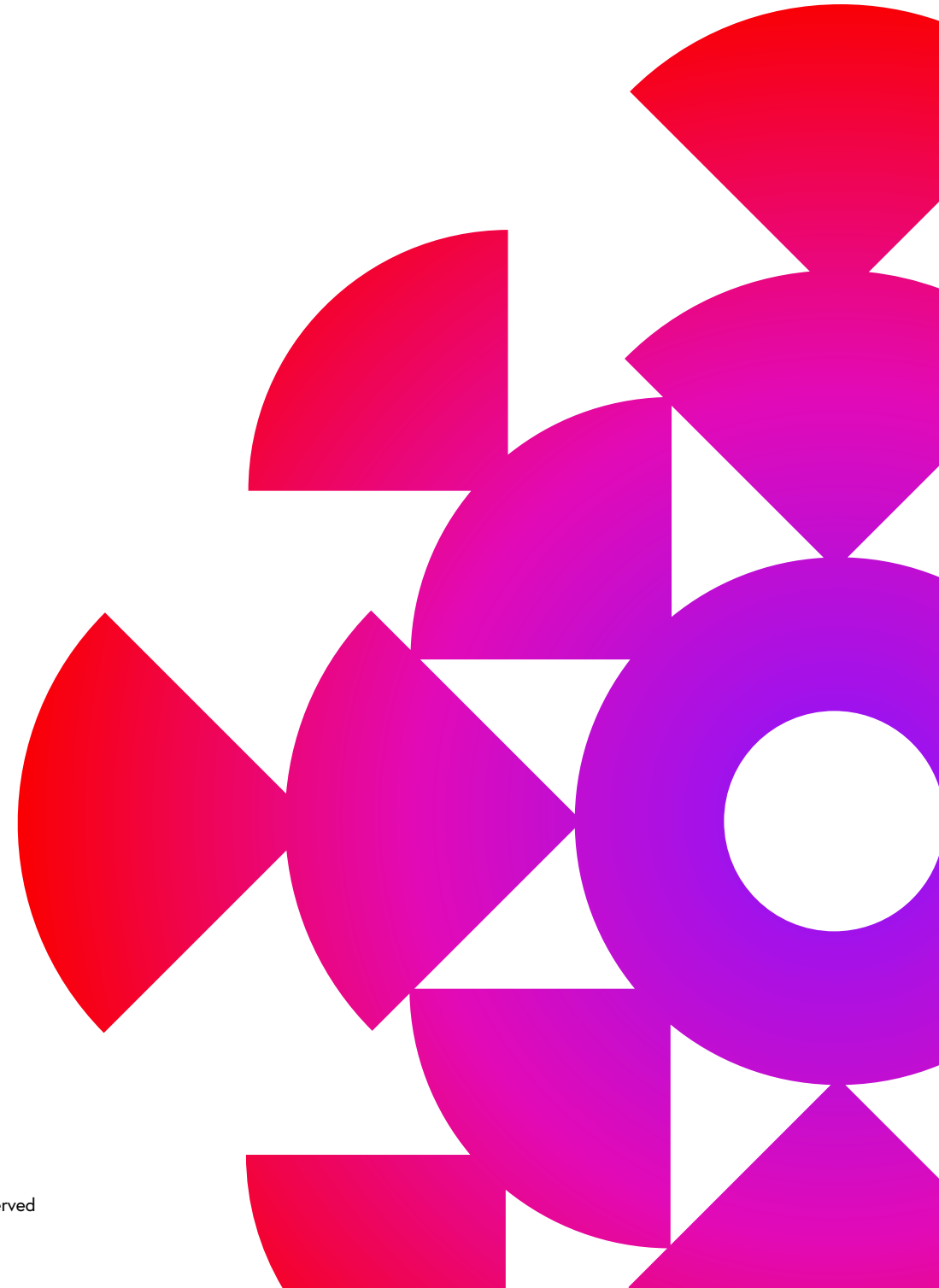
As the leading industrial cybersecurity company, Claroty's comprehensive platform and services are backed and adopted by leading industrial automation vendors, including Rockwell Automation, Siemens, and Schneider Electric. By providing a swiss-army-knife solution for improving the availability, safety, and reliability of OT assets and networks, The Claroty Platform greatly reduces the complexity of industrial cybersecurity.

As the only cybersecurity solution compatible across IT, OT, and converged IT/OT environments, Claroty is uniquely well-suited to helping enterprises implement a converged IT/OT SOC in accordance with the guidelines laid out in this white paper. And since Claroty's solutions are technology-agnostic, they can be seamlessly integrated into existing IT security management infrastructures.

# ABOUT CLAROTY

Claroty is the industrial cybersecurity company. Trusted by the world's largest enterprises, Claroty helps customers reveal, protect, and manage their OT, IoT, and IIoT assets. The company's comprehensive platform connects seamlessly with customers' existing infrastructure and programs while providing a full range of industrial cybersecurity controls for visibility, threat detection, risk and vulnerability management, and secure remote access—all with a significantly reduced total cost of ownership. Claroty is backed and adopted by leading industrial automation vendors, with an expansive partner ecosystem and award-winning research team. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America, and deployments on all seven continents.

**To learn more about how Claroty can help your organization establish a converged IT/OT SOC, visit claroty.com/request-a-demo.**



CLAROTY