Attacks on physical infrastructure and operational environments in an era of “phygital” integration — similar to the cyber attacks on IT infrastructure that already beset enterprises and their customers — have raised the risk level for companies exponentially.

Expanding cyber vigilance by means of an integrated IT and operating technology (OT) security operations model can mitigate these risks.

Finding and distributing in-house resources to address both OT and IT security, particularly for globally dispersed operations, can challenge an enterprise’s talent pipeline.

Fortunately, service providers able to address emerging attack methods and replication techniques across both technology platforms and operational environments can enable and manage integrated security at scale.
Integrated operations require integrated security

The threat ‘surface’ of enterprises is widening with the closer integration of operational technology, IT systems and the internet. The increasing use of industrial IoT devices add additional exposure to cyber threats. This can be seen in the sharp rise in the number of cyber attacks on critical industrial control systems and IoT assets in the past few years.

The security of industrial control systems has become a strategic issue for corporations, utilities, public works facilities, and other such users of operational technology, or “OT.” The increasing frequency and severity of attacks on OT systems only illustrates the importance of designing and deploying “defense-in-depth” security architectures that can ensure a timely detection and rapid response to such breaches.

Establishing a centralized ‘security operations center’ for such industrial control systems — similar to such centers for IT security in which most large organizations have invested— helps establish a continuous cyber vigilance over the OT environment, enabling early attack detection and quick recovery through rapid responses.

Our experience in providing integrated IT-OT security operations services for our customers globally has revealed a set of best practices and priorities in addressing the cyber security challenges of such integration. Key among our findings: The adoption of newer technologies, operating models, and architectures can enable security teams to detect and respond to such attacks effectively.

The challenge

Violations of data security already have increasingly dire risks for enterprises and their customers. Similar attacks on physical infrastructure and machinery — in an era of internet-connected dams and power plants, autonomous vehicles, and intelligent roadways, to name just a few examples of “phygital” integration today — raise the risk level exponentially.

Organizations have achieved a varying degree of success in monitoring and securing their industrial control system (ICS) assets, depending on how effectively the organization gathers information from the ICS environment and uses it to identify threats and attacks. In most cases, these implementations have been restricted to collecting, correlating, and
analyzing event logs from IT systems deployed in an ICS environment, using security information and event management (SIEM) technology. However, this leaves the organization blind to any direct threats to the process control networks and the ICS assets themselves.

Some of the common challenges with ICS or OT security monitoring include:

- The distributed nature of ICS assets, which make accurate inventory collection difficult
- The use of legacy systems, proprietary software, and poorly documented OT protocols
- ICS assets not capable of generating event logs or using proprietary, non-standard logging formats
- Sensitive ICS environments vulnerable to any fluctuation in data transfer, due to very limited bandwidth, precise data, continuous availability, and high integrity requirements.

Peeking in

Visibility into the security of the ICS environments starts with gathering information on the assets and the events affecting them. The event log collection and log forwarding should be enabled in such a way as to gain visibility of all critical systems and networks in the environment.

The methods used for collecting event data from ICS environments vary based on their location. It may be feasible to use traditional approaches (log forwarding configurations, log events gathered from network devices and standard systems based on common operating systems that are deployed in the network’s manufacturing and operations zones (often referred to as “Level 3”). However, for other systems in the supervisory zone (control systems, or Level 2) and the process and device zone of sensors, analyzers, and actuators (Level 1), such basic techniques usually cannot be used, due to the nature of the systems. In such cases, it’s usually advantageous to use passive network monitoring systems for event data collection and thereby avoid obstructing the system operations. These considerations must often take into account limited available bandwidth, memory and processing power, the continued reliance on legacy systems, or the use of proprietary OT protocols at these levels.

Passive network monitoring systems that are specialized for ICS — like CyberX, Tenable.ot, Nozomi Guardian, and others — provide capabilities not only to monitor the process control network and report security events, but also to identify the assets deployed and the vulnerabilities found in the environment. This can provide added insights into the security of the overall industrial control system. Most of these solutions also support detailed investigation of security events as a part of their incident responses.
Understand what is going on

Now that events of interest are available, the security configuration must analyze and correlate the event logs from other related systems within the same site environment and send the event data to the centralized SIEM platform.

This consolidated approach is especially beneficial when limited bandwidth is available for sending log data to the SIEM platform. As an added advantage, this model can also provide the visibility into the security status of the ICS environment for local site and plant operations teams.

Act on it

With the technology aspects addressed, the next step is to determine who monitors and acts on the alerts that a SIEM system generates.

An integrated IT-OT security operations center (SOC) is generally more effective than a dedicated ICS SOC approach. This can be achieved by leveraging the same SIEM platform used for IT SOC. Additional, custom use cases and alerts can be defined, taking into consideration the ICS process flows applicable to a particular site or plant.

The target operating model for an integrated IT–OT SOC will be a combination of technologies governed by specific processes run by people skilled in both the enterprise IT and ICS systems. New processes and operating procedures are developed, or existing ones are modified to accommodate ICS operations.

Where an IT SOC team already exists, it is important that the Level 1 team responsible for monitoring and triaging SIEM platform alerts is trained on ICS technologies and aware of the ICS landscape they now also monitor. Detailed playbooks for some common use cases must be developed for the Level 1 team’s reference. Their role can be augmented by skilled Level 2 and Level 3 ICS security personnel who can undertake in-depth investigations and determine the right response to a unique incident. Then, the lessons learned from these incidents should be documented for the Level 1 teams as well, to enhance their ability to detect and respond in such situations themselves, thereby reducing the overall response time.
Establishing an integrated IT–OT SOC

The integration of individual site or plant ICS environments (the OT) with a centralized SIEM system (the IT) requires careful planning, extensive data gathering and standardized execution models. A streamlined approach to setting up an integrated IT-OT SOC comprises 5 phases:

1. **Due diligence** to understand the current ICS landscape, gathering basic information about the sites to be integrated and using this to undertake a feasibility analysis. A comprehensive review helps the SOC designers understand the current governance models, any site specific architectures, infrastructure capacities, network connectivity and other details required to develop an implementation strategy.

2. **Strategy development** to prepare for deployment, keeping in mind the criticality of the ICS infrastructure, implementation priorities and other deployment schedules. This includes prioritization of sites for ICS/SIEM integration, identifying assets or type of assets to be monitored, defining a strategy for log generation and collection, and developing a deployment plan.

3. **Site security assessment** undertaken for each plant or site, which is used to validate available asset data, evaluate the current security landscape, assess the business criticality of assets, and determine the readiness of a site for integration.

4. **SIEM Integration** involves the finalization of the design for log collection and forwarding and the subsequent implementation of the design. This may also involve deployment of supporting technologies — for example, the passive data collection tools — required to collect the logs from the ICS environments. Also undertaken at this stage: designing and configuring the various use cases to monitor, establishing rules for alert, templating reports and dashboards specific to ICS on the SIEM.

5. **Enable operations** so the IT SOC team can also handle ICS security events, both by means of training and by augmenting the team with ICS security experts.
Skills and talent

The number and geographical distribution of an enterprise’s sites and the limited availability of skilled ICS security architects and engineers required to establish the SOC is often a challenge to be addressed. In most cases, while organizations have engaged local service providers to provide basic IT services at their sites and in their plants, they do not have personnel with a full-stack security skillset deployed at each site. Undertaking a current state assessment and feasibility study by engaging with different local service providers, possibly including visits to each site, not only requires the security organization to scale up but can also become time-consuming and cost-prohibitive.

A partnership with a service provider who provides end-to-end specialized services in ICS security — from consulting to systems integration to managed services — with enough global presence to serve each site can ensure a quicker, standardized and effective implementation of the integrated IT-OT SOC. Such service providers add additional value from their experience designing, implementing and operating Integrated IT-OT SOC globally. In addition to leveraging global partnerships with other service providers, they can often move quickly to implementation and operation, thanks to reusable templates for assessments, feasibility studies, and architecture blueprints, and the guidelines, best practices, and runbooks for SOC teams they’ve perfected over the course of their engagements.

Benefits of an integrated IT–OT SOC

The integrated IT-OT SOC approach has provided several benefits to TCS’ customers by means of better security and value for their investments, such as:

- **A single-pane-of-glass view** into the threats to both IT and the ICS environment
- **Broader and integrated visibility of threats** to deliver complete situational awareness of enterprise-wide risks
- **Enterprise-wide cyber resiliency** for comprehensive cyber risk management
- **Revealed cross-domain attacks** to protect ICS systems from threats identified in the IT system
- **Identified vulnerabilities** and patching priorities in their full context
- **Faster response times** by avoiding breakdowns in communication and dropped incident handling between multiple teams
- **Cost-efficiency** from leveraging synergies of the existing SIEM platform and SOC teams.

### Integration is more than mere addition

An integrated IT–OT security operations center enhances the cyber vigilance of an enterprise by extending the SOC to the industrial control system environments as well as the IT security realm. The combined forces result in operational synergy with an end-to-end visibility into the cyber security posture across the organization.

Using the right partner with the right distributed skillset, meticulous planning, detailed designs and following an appropriate deployment strategy — along with use of the best technologies and processes for both IT and OT security — will ensure a successfully integrated SOC that allows an enterprise to realize significant security and business benefits.
Contact
Email: TL.Institute@tcs.com

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that has been partnering with many of the world's largest businesses in their transformation journeys for over 50 years. TCS offers a consulting-led, cognitive powered, integrated portfolio of business, technology and engineering services and solutions. This is delivered through its unique Location Independent Agile™ delivery model, recognized as a benchmark of excellence in software development.

A part of the Tata group, India's largest multinational business group, TCS has over 453,000 of the world's best-trained consultants in 46 countries. The company generated consolidated revenues of US $22 billion in the fiscal year ended March 31, 2020, and is listed on the BSE (formerly Bombay Stock Exchange) and the NSE (National Stock Exchange) in India. TCS’ proactive stance on climate change and award-winning work with communities across the world have earned it a place in leading sustainability indices such as the Dow Jones Sustainability Index (DJSI), MSCI Global Sustainability Index and the FTSE4Good Emerging Index.

For more information, visit us at www.tcs.com