inflexion point

Cyber Glossary

Terms defined as they relate to Industrial Control Systems (ICS) and Operational Technology (OT) security

Cyber vs Cybersecurity

"Cyber" relates to anything involving computers or digital networks. "Cybersecurity" is the practice of protecting these systems, including ICS and OT, from digital attacks.

MSP vs MSSP

A Managed Service Provider (MSP) offers general IT services, whereas a Managed Security Service Provider (MSSP) provides specialized security services critical for ICS/OT protection.

SPAN vs mirror vs TAP

These are network monitoring configurations. SPAN and mirror ports copy network traffic to another port for analysis. A Test Access Point (TAP) is a dedicated device that also allows monitoring of network traffic with minimal impact on the network.

ISOC vs CSOC vs OTSOC vs SOC

- ISOC (Information Security Operations Center) focuses on information security.
- CSOC (Cyber Security Operations Center) is dedicated to cybersecurity response.
- OTSOC (Operational Technology Security Operations Center) specializes in ICS/OT security.
- SOC (Security Operations Center) is a unified facility that oversees security.
- Converged SOC integrates both IT and OT security monitoring and management.

Pen Test vs OT Pen Test vs OT Network Pen Test vs OT Physical Pen Test

Penetration Testing (Pen Test) is simulating cyber attacks to find vulnerabilities. OT Pen Test focuses on OT systems specifically. OT Network Pen Test targets the OT network components, while OT physical pen tests involve attempting to exploit physical vulnerabilities in OT environments.

Red team vs Blue team vs Purple team

These terms refer to security training exercises. A red team simulates attackers to test defenses, a blue team defends, and a purple team analyzes and improves the cooperation between the red and blue teams.

NOC vs SOC

A Network Operations Center (NOC) manages network components, while a Security Operations Center (SOC) focuses on security aspects. Both are critical for maintaining ICS/OT integrity.

SASE

Secure Access Service Edge (SASE) is a cybersecurity concept that combines network security functions with WAN capabilities to support the dynamic, secure access needs of organizations, including those with ICS/OT.

Industrial Datacenters

Industrial datacenters refer to highly specialized facilities designed to host mission-critical industrial control systems and operational technology infrastructure. These datacenters are equipped with robust security measures tailored to the specific requirements of industrial environments, such as SCADA (Supervisory Control and Data Acquisition) systems, DCS (Distributed Control Systems), and PLCs (Programmable Logic Controllers).

The security considerations for industrial datacenters include physical security to protect against unauthorized access, network security to shield against cyber threats, and environmental controls to ensure the systems are operating within safe parameters. Due to the sensitivity of the operations managed within these datacenters, such as utility services, manufacturing, and critical infrastructure, the emphasis on reliability, availability, and resilience is significantly higher compared to standard commercial datacenters. This includes redundant systems, disaster recovery capabilities, and strict compliance with industry-specific regulations.

SD-WAN

Software-Defined Wide Area Network (SD-WAN) is a method of managing network traffic that is critical for connecting and securing distributed ICS/OT components.

OT SDN

Operational Technology Software-Defined Networking (OT SDN) applies SDN principles to OT networks to improve flexibility and security in industrial control systems.

Endpoint computing

Devices like Schweitzer Blue Frame focus on securing endpoints in an OT network, which can include control systems, sensors, and other field devices.

Dockers/Containers

Docker is a platform used to develop, ship, and run applications inside containers, which can also be applied to securely manage applications within ICS/OT environments.

Kubernetes/Pods

Kubernetes is an orchestration system for Docker containers, with pods being the smallest deployable units created and managed on Kubernetes, often used in cloud-based ICS/OT applications.

Network monitoring

It involves continuously analyzing network traffic and performance to detect and respond to anomalies that might indicate security issues in ICS/OT networks.

Tabletop Exercise (TTX)

A discussion-based exercise used to practice emergency response plans, including ICS/OT incident response, in a simulated environment without live networks or systems.

CSOC

CSOC typically stands for "Cyber Security Operations Center," and it is commonly used to refer to a centralized facility that houses the personnel, processes, and technologies responsible for monitoring, detecting, responding to, and mitigating cybersecurity threats. The primary focus of a CSOC is on information technology (IT) environments.

In some contexts, the term "CSOC" may be used more broadly to encompass both IT and operational technology (OT) security operations. However, it's more common to see specialized terms like "ISOC" (Industrial Security Operations Center) or "OTSOC" (Operational Technology Security Operations Center) when referring to security operations centers dedicated specifically to industrial control systems and operational technology.

As for the idea of a converged or combined SOC, this concept refers to a Security Operations Center that integrates both IT and OT security functions. A converged SOC recognizes the increasing interconnectedness of IT and OT environments and aims to provide a unified and comprehensive approach to cybersecurity. This integrated approach is important as many organizations operate in environments where IT and OT systems are interconnected, and threats in one domain can impact the other.

The terms used can vary across industries and organizations, and you might encounter variations such as Combined SOC, Unified SOC, or Converged SOC, but the underlying idea is similar—to address cybersecurity challenges holistically across both IT and OT domains. The choice of terminology often reflects the specific focus and priorities of the organization or industry in question.

ISOC/OTSOC

In the context of Industrial Control Systems (ICS) and Operational Technology (OT), the equivalent of a Cyber Security Operations Center (CSOC) is often referred to as an Industrial Security Operations Center (ISOC) or an OT Security Operations Center (OTSOC). These centers are specifically tailored to address the unique cybersecurity challenges and requirements of ICS and OT environments.

Here are some key features of an ISOC or OTSOC:

1. Focus on ICS/OT Environments:
   An ISOC or OTSOC is designed to monitor and protect industrial control systems and operational technology environments.
2. Specialized Expertise:
   Staff in an ISOC or OTSOC are trained to understand the intricacies of ICS and OT systems, including the unique protocols, communication patterns, and potential vulnerabilities associated with these environments.

3. Continuous Monitoring:

   These centers typically provide continuous monitoring of ICS and OT networks to detect anomalies, potential cyber threats, and unusual activities that could impact the reliability and safety of critical infrastructure.

4. Incident Response in ICS/OT Context:

   Incident response procedures and protocols in an ISOC or OTSOC are tailored to address incidents specific to industrial processes. This includes procedures for handling disruptions to manufacturing processes, utilities, or other critical functions.

5. Integration with IT Security:

   While focused on ICS and OT, an ISOC or OTSOC may also coordinate with traditional IT-focused security operations to ensure a holistic and integrated cybersecurity approach.

6. Regulatory Compliance:

   Given the importance of critical infrastructure, an ISOC or OTSOC often ensures compliance with industry-specific regulations and standards governing the cybersecurity of ICS and OT systems.

The terms ISOC and OTSOC are often used interchangeably, and the specific terminology may vary based on industry practices. The main idea is to convey the notion of a security operations center specifically dedicated to safeguarding the security and reliability of industrial and operational technology systems.

Cyber vs. Cybersecurity

In the context of Operational Technology (OT), the terms “cyber” and “cybersecurity” are closely related but have distinct meanings:

- Cyber

“Cyber” is a broad term that encompasses anything related to computer systems, networks, and digital technologies. It is a prefix commonly used to indicate a connection to the digital realm. In the context of OT, “cyber” refers to the integration of digital technologies and computer systems within industrial and operational environments. It signifies the convergence of traditional industrial processes with modern digital technologies to improve efficiency, automation, and data collection.

- Cybersecurity

“Cybersecurity” specifically refers to the practice of protecting computer systems, networks, and data from various forms of cyber threats and attacks. These threats can include malware, hacking attempts, data breaches, and other unauthorized activities that can compromise the security and integrity of digital systems. In OT, cybersecurity focuses on safeguarding the digital components of industrial control systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, and other technology used in critical infrastructure and industrial processes.

In summary, “cyber” in the context of OT pertains to the integration of digital technologies within industrial environments, while “cybersecurity” specifically addresses the protection of these digital technologies and the data they handle