LevelBlue

SOLUTION BRIEF / MAY 2024

Securing Operational Technology

LevelBlue's penetration testing solutions for OT environments

As the use of connected devices and systems continues to grow, cyberattacks across all environments have escalated. In the critical infrastructure, industrial, and healthcare sectors, breaches can have life-threatening consequences.

Understanding Operational Technology (OT)

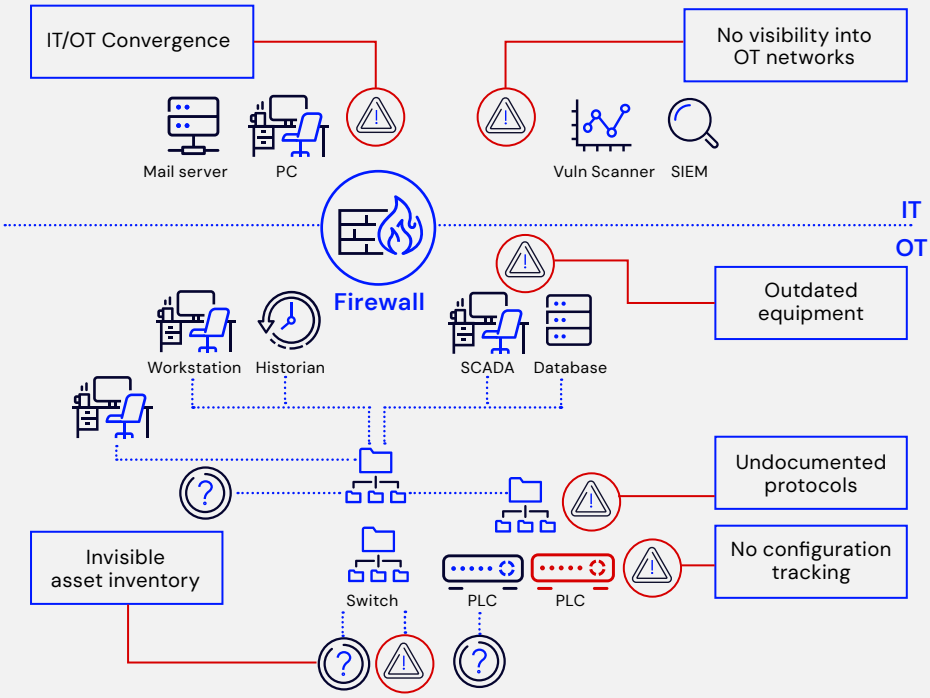
Operational Technology (OT) refers to the hardware and software systems that control and monitor physical devices and processes in critical infrastructure sectors such as energy, transportation, and manufacturing. Unlike Information Technology (IT) systems, OT systems are responsible for managing real-world processes, making them an attractive target for malicious actors.Understanding the unique characteristics of OT is crucial when conducting penetration testing.

In today's digital landscape, organizations face numerous cybersecurity risks concerning OT. The first is, that many OT systems are legacy systems, that were designed before the emergence of cyber threats, unfortunately, this can leave them exposed and can be expensive to upgrade. Another risk is that organizations often lack a complete inventory of their OT assets, making it difficult to identify and address vulnerabilities, and can lead to unseen security gaps. Increasingly, OT systems are being connected to IT systems for better data analysis and operational efficiency. This increased interconnectivity can create potential entry points for cyber threats.

Benefits of LevelBlue pen testing:

- **Spot OT-specific vulnerabilities:** Pinpoint unique vulnerabilities within Operational Technology systems, ensuring all security weaknesses are identified and addressed
- **Enhance safety mechanisms:** Strengthen the security of mechanisms critical to maintaining safe operations, preventing physical and operational threats
- **Ensure business continuity:** Mitigate risks that can lead to downtime, ensuring continuous operation and stability of the business processes dependent on OT systems
- **Comply with regulations:** Meet legal and regulatory requirements by proving your organization's active role in managing cybersecurity risks effectively
- **Build customer trust:** Enhance the confidence of your clients and stakeholders in your cybersecurity measures, securing their trust through demonstrated reliability and safety
- **Reduce overall risk:** Lower the risk of cyber threats and breaches, protecting against potential financial losses and reputational damage troubleshooting

Vulnerabilities and gaps in your OT environments



Another factor is OT systems often control critical infrastructure where downtime can have significant impacts. This can make it difficult to apply updates and patches that might disrupt service.

Organizations can face several challenges when a security incident occurs within their Operational Technology (OT) systems. A security incident could disrupt services, leading to significant operational downtime. The downtime and resources required to address a security incident can result in substantial financial loss. This includes costs for incident response, system recovery, and potential regulatory fines. In some cases, a security breach could lead to physical damage to the equipment controlled by the OT systems, especially if they involve industrial control systems. If OT systems are compromised in sectors such as chemical production or energy, there could be safety risks for the workforce and the surrounding environment.

To mitigate these challenges and overcome these risks, organizations need to invest in proactive measures, like conducting regular penetration tests or pen tests.

Importance of OT penetration testing

OT penetration testing is a proactive approach to identify vulnerabilities in OT environments before they are exploited by adversaries. By simulating real-world attack scenarios, organizations can gain valuable insights into the security posture of their critical infrastructure systems. This enables them to implement necessary countermeasures and safeguards to protect against potential threats. OT penetration testing helps in:

- Identifying and addressing vulnerabilities in OT environments reduces the risk of successful attacks
- Ensuring compliance with industry level standards and regulations
- Building trust with stakeholders by demonstrating a commitment to security

LevelBlue OT Penetration Testing

LevelBlue Penetration Testing is a proactive strategy that helps organizations identify and address vulnerabilities in their OT environments and focuses on enhancing a client's OT network security posture. These strategies can help organizations mitigate risks associated with OT vulnerabilities through several different ways:

Simulating a cyber-attack by ethical hackers on OT systems, to identify security weaknesses, ranging from outdated software to insecure configurations, or other vulnerabilities that could be exploited by attackers.

Validating whether current security measures like firewalls, intrusion detection systems, and access controls are functioning correctly. If a Pen Test can bypass these measures, there's a good chance a real attacker could too.

Risk prioritization by helping organizations understand the potential impact of different vulnerabilities, allowing them to prioritize their remediation efforts based on risk level. Testing and improving incident response capabilities by observing how the organization detects and responds to a simulated attack, can identify areas for improvement.

Managing regulatory compliance requirements by proving evidence that an organization is actively managing its cyber risks.

How does LevelBlue perform a Pen Test in an OT environment?

LevelBlue's approach to OT pen testing involves an evaluation of the client's existing network and connected device environment, identifying potential gaps in the deployed devices and capabilities, and offering tailored recommendations through our team of cybersecurity consultants. Our consulting team consists of highly skilled and experienced professionals who specialize in cybersecurity, ensuring that your organization receives top-notch guidance and best-of-breed tools.

We start by performing a comprehensive assessment of the security landscape through a structured and phased approach.

The process begins with the "Information and Configuration Gathering" phase, which lays the groundwork for the entire engagement. During this phase, we determine and collect current state information on the technologies under review. We establish an interview schedule, and the interview candidates ideally include all project stakeholders. We also collect and review configurations as defined in your current security standards.

Following this, we transition into the "Analysis" phase. Here, we meticulously examine the data collected in the previous phase and the specific security capabilities under scrutiny. To help you better understand the implementation of your overall security standards, LevelBlue Consulting assigns a security standards posture rating to each technology configuration under review.

Best practices for OT penetration testing

To ensure successful OT penetration testing, we recommend the following best practices:

- Tailor testing methodologies to OT environments and systems, considering their unique attributes
- Foster close collaboration between IT and OT teams throughout the testing process to ensure comprehensive assessments
- Develop a comprehensive testing plan that includes different scenarios and attack vectors, testing the system's resilience
- Prioritize the remediation of identified vulnerabilities and implement security

Within these engagements, LevelBlue consultants will be looking for the gaps within the security of the system to minimize security incidents. The security analysis will concentrate on the following:

EXTERNAL PENETRATION TESTS	EXTERNAL PENETRATION TESTS
TESTS	
Vulnerabilities associated with the current deployment	• Device OS, firmware, software, patches, security updates • Authentication and access controls • Encryption and secure data transmission • Wireless security testing • Network architecture, segmentation, and traffic analysis • Vulnerability scanning and exploitation • Supporting controls and policies
Risks from OT devices from various OT devices and the other devices within the network	• Risks introduced to the network from various OT devices and the other devices within the network
Assessing the Core of the OT network to ensure proper configuration of functional and security controls	• Access control of OT devices – process controls • Ability to monitor for rogue devices connecting to the OT network • Verify and validate that monitoring and alerts are in place and functioning
Identifying any potential risks associated with the utilization of remote access devices within the network Risk Assessment	• Evaluating POTS and cellular modems to ensure the configuration with the network and other devices doesn't introduce any risks or vulnerabilities into the OT network
Potential infiltration points within the IT or OT network that could be used as a staging area for penetrating one environment from the other. The approach that the security assessment team will follow includes:	• **Assess** the vulnerabilities of critical assets to those threats • **Determine** the associated risk (likelihood and consequences of attacks and threats) • **Identifying** any potential points within the IT or OT network that could be used as a staging area for penetrating one environment from the other

Upon completion of the information gathering and analysis phases, we move to the "Deliverables" phase. LevelBlue Consulting provides both technical and executive reports, offering a comprehensive view of your security landscape.

These reports include a review of the technology component template, a rating for your security deployment posture, and a narrative output or commentary on the posture analysis, where applicable. We aim to provide you with a thorough understanding of your security posture and practical recommendations for improvement.

LevelBlue

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.

Contact us to learn more, or speak with your LevelBlue sales representative.