

THE DEFENSE CHRONICLES



Ioana-Andreea Cuc
Technical writer at EVIDEN

Automated penetration testing across the cloud-edge continuum: Advancing cyber resilience through controlled attack simulation

As critical infrastructures continue their digital transformation journeys, the cybersecurity landscape is becoming increasingly complex. Modern environments no longer operate within clearly defined boundaries. Instead, organisations rely on interconnected cloud services, edge computing platforms, enterprise applications, industrial control systems (ICS), and cyber-physical assets that collectively support essential services.

Why traditional security validation is no longer enough

While this transformation improves operational efficiency, it also expands the cyber-attack surface. Traditional penetration testing approaches often struggle to keep pace with the scale and complexity of these distributed environments, while manual penetration testing remains resource-intensive and difficult to scale. To address this challenge, we aim to develop a penetration testing and simulation environment capable of supporting automated security validation across the cloud-edge continuum.

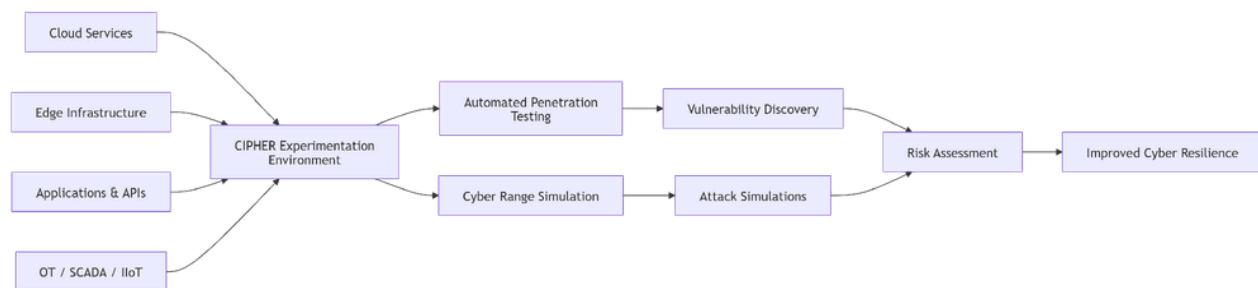


Figure 1 - Automated Security Validation Across the Cloud-Edge Continuum

The objective extends beyond vulnerability identification. Thus, we aim to provide an experimentation environment where organisations can safely emulate realistic infrastructures, assess cyber risks, validate security controls, and strengthen resilience through controlled attack simulations and cyber-range exercises. This work directly supports the project's broader mission of improving cybersecurity preparedness for critical infrastructure operators across Europe.

The CIPHER experimentation laboratory has been designed to emulate information management systems and operational technology infrastructures, covering environments ranging from cloudified services to Industrial IoT, SCADA, and cyber-physical systems. It is intended to enable realistic security experimentation in controlled environments where organisations can safely evaluate their exposure and preparedness against emerging cyber threats.

A key aspect of this approach is the ability to simulate multi-vector attack scenarios. Rather than relying on isolated security tests, the environment supports the evaluation of attack paths that may traverse multiple technology domains. This mirrors the reality of modern threat campaigns, where attackers frequently exploit weaknesses across interconnected infrastructures, moving between cloud services, network resources, applications, and operational technology environments. By reproducing these conditions in a controlled setting, the project enables organisations to better understand how vulnerabilities, misconfigurations, and attack techniques interact within complex ecosystems.

Scaling assessments through orchestration

To support automated assessments, we also investigate opportunities for scalable orchestration of security testing activities through containerised and service-oriented architectures. One example explores an architecture where orchestration components interact with a security toolset through managed interfaces, enabling automated execution of security scans while maintaining separation between orchestration logic and testing engines. This type of architecture supports repeatable, traceable, and extensible security assessments across heterogeneous infrastructures.

Thus, we are exploring the integration of open-source security testing and orchestration technologies. The implementation plan references the use of cyber-range technologies and established security testing frameworks, while the technical use-case definitions further demonstrate how automated vulnerability validation can be orchestrated through structured workflows.

In the DevSecOps scenario, tools such as Nuclei, OWASP ZAP, Schemathesis, Trivy, and Gitleaks are integrated into automated pipelines. Their outputs are collected, analysed, and incorporated into security decision-making processes, allowing organisations to identify vulnerabilities before production deployment.

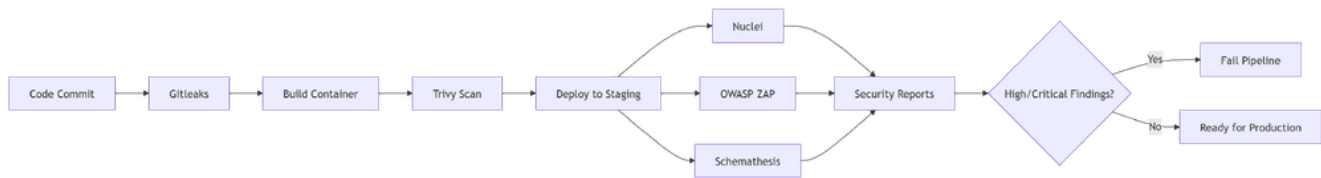


Figure 2 - Continuous Security Validation Pipeline

The same philosophy extends into operational technology environments, where testing activities must be carefully balanced against safety and availability requirements.

Protecting critical infrastructure without disrupting operations

Automated security validation becomes significantly more challenging within operational technology environments. Unlike traditional enterprise systems, industrial control systems frequently support critical operational processes where aggressive testing can negatively impact availability. For this reason, we investigate approaches that balance security validation requirements with operational safety objectives.

A notable example is the proposed Automated OT Security Validation Framework, which introduces a "Safe-Gate" model for performing cybersecurity assessments with multiple layers of safeguards.

The proposed Automated OT Security Validation Framework introduces a tiered confidence model that progresses from passive observation to protocol-aware validation and, only when explicitly authorised, controlled active testing.

Asset discovery is performed through passive traffic analysis, protocol fingerprinting relies on standard device identification operations, and vulnerability assessment is correlated with known CVE information before any active validation is considered. Human approval and safety interlocks remain central components throughout the process.

Particularly important in OT environments is the implementation of safeguards designed to prevent disruption of production systems. The framework introduces controls such as protocol-specific interrogation, packet-rate throttling, health monitoring, state awareness, and emergency stop mechanisms.

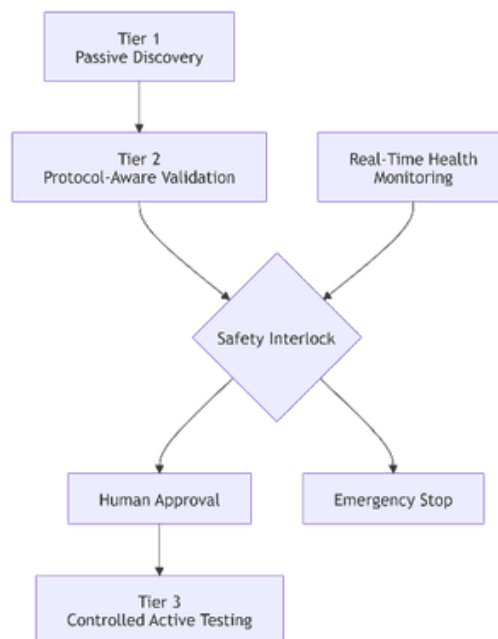


Figure 3 - Safety Interlock and Tiered Validation Workflow

Continuous observation of system behaviour enables the testing environment to detect communication anomalies or operational issues and immediately halt active validation activities when required. This demonstrates how automated penetration testing can remain compatible with the operational constraints of critical infrastructure systems.

The broader value of these capabilities lies in their integration with the CIPHER cybersecurity ecosystem. Automated penetration testing is not treated as a standalone activity. Instead, assessment results feed into risk analysis, continuous monitoring, and preparedness activities conducted across the platform. Thus, our work in CIPHER is helping establish the technical foundations required to bring automated penetration testing and cyber resilience validation closer to the operational realities faced by today's critical infrastructure operators.

References:

https://gitlab.apps.efp-global.eu/cipher/automated-pentesting_



FOLLOW US!