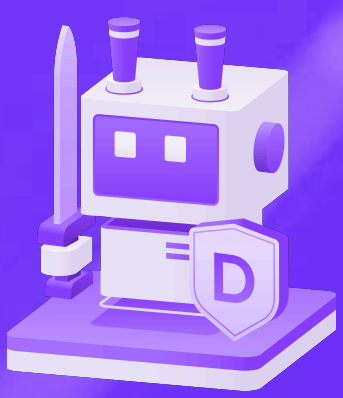
digiDations

ATLAS™ Security Validation Platform 2025 Annual Report

Empowering Defense Readiness: Aligning Security Controls with Real-World Threat Evolution

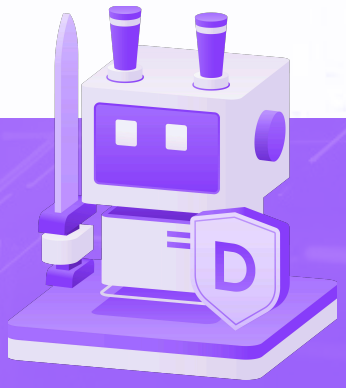


Contents

Executive Summary

In a rapidly evolving threat landscape, the gap between an organization's deployed defenses and the actual tactics used by adversaries continues to widen. For security leaders, the challenge is no longer just "Do we have security tools?" but "Do our controls effectively stop today's specific, weaponized threats?"

The ATLAS™ Security Validation Platform 2025 Annual Report provides a strategic overview of how digiDations has evolved its attack library to mirror the shifting realities of global cyber warfare. By continuously ingesting threat intelligence and translating it into actionable validation rules, ATLAS™ serves as a dynamic benchmark for enterprise resilience.



This report highlights critical updates to the platform, driven by the most impactful trends observed over the past year:

- Targeting the "Crown Jewels": A significant expansion of validation rules targeting Enterprise Core Software, reflecting the adversary's pivot toward supply chain penetration and business-critical system compromise.
- Closing the Visibility Gap: Enhanced coverage of Evasive Command & Control (C2) and Persistence techniques, enabling organizations to test their ability to detect stealthy, long-term intrusions that bypass traditional perimeter defenses.
- Validating Against Weaponized Vulnerabilities: A focused update on high-frequency exploit chains, ranging from legacy N-day vulnerabilities to emerging Web application threats, ensuring defenses remain robust against both automated botnets and targeted APT campaigns.

For our customers, this report is not just a statistics summary—it is a roadmap for prioritization. It offers the insights needed to tune detection rules, patch critical blind spots, and validate that security investments are delivering measurable protection against the threats that matter most.

Key Findings

Evolution of Threat Characteristics

C2 Evasion Becomes a Strategic Priority

Adversaries are placing increasing emphasis on the stealth of Command and Control (C2) communications. The use of DNS tunneling, ICMP channels, legitimate web protocols, and non-application-layer protocol tunneling has risen significantly, enabling attackers to evade traffic inspection and traditional anomaly detection mechanisms.

Enterprise Software as a Primary Target

Exploitation activity targeting enterprise-grade management software, including ERP, CRM, and OA systems, has increased significantly. As mission-critical systems with minimal downtime tolerance, these platforms frequently experience delayed patch cycles, making them ideal entry points for supply chain attacks.

The Commoditization of Offensive Tooling

The use of commercial hacking tools, Trojans, and modular attack frameworks continues to grow rapidly. Attackers are increasingly prioritizing persistent access, long-term control, and data exfiltration, rather than short-lived disruptive ransomware operations.

Expanding the Boundaries of Security Validation

The Emergence of AI Application Security Validation

Security validation is expanding into AI workloads, with the emergence of validation rules targeting AI applications and LLM-driven services. This reflects growing recognition of risks unique to model interaction layers, data handling, and AI-driven business logic.

SQL Injection Remains the Dominant Web Threat

Despite years of defensive investment, SQL Injection continues to be the most prevalent web-layer attack vector. Attacker focus has increasingly shifted toward direct database access, privilege escalation within data layers, and destructive data manipulation.

ATLAS™ Security Validation Platform Attack Library Annual Updates

6,882
New Validation Rules

1,099
New Direct Web Validation Rules

393
New Validation Scenarios

35
New Full-Chain Attack Playbooks

Validation Scenarios

While ransomware remains a key focus, the 2025 scenario library significantly strengthens coverage of the Command and Control (C2) and Persistence phases. These scenarios reflect real-world campaigns where attackers prioritize maintaining access and operational longevity over rapid “smash-and-grab” attacks.

Attack Playbooks

Thirty-five new full-chain playbooks were added this year, reconstructing the complete kill chains of active APT groups such as APT38 (Lazarus) and Patchwork. These playbooks simulate the entire lifecycle, from Initial Access through Privilege Escalation, Lateral Movement, and Data Exfiltration, with sector-specific tailoring for Finance, Energy, and High-Tech Manufacturing.

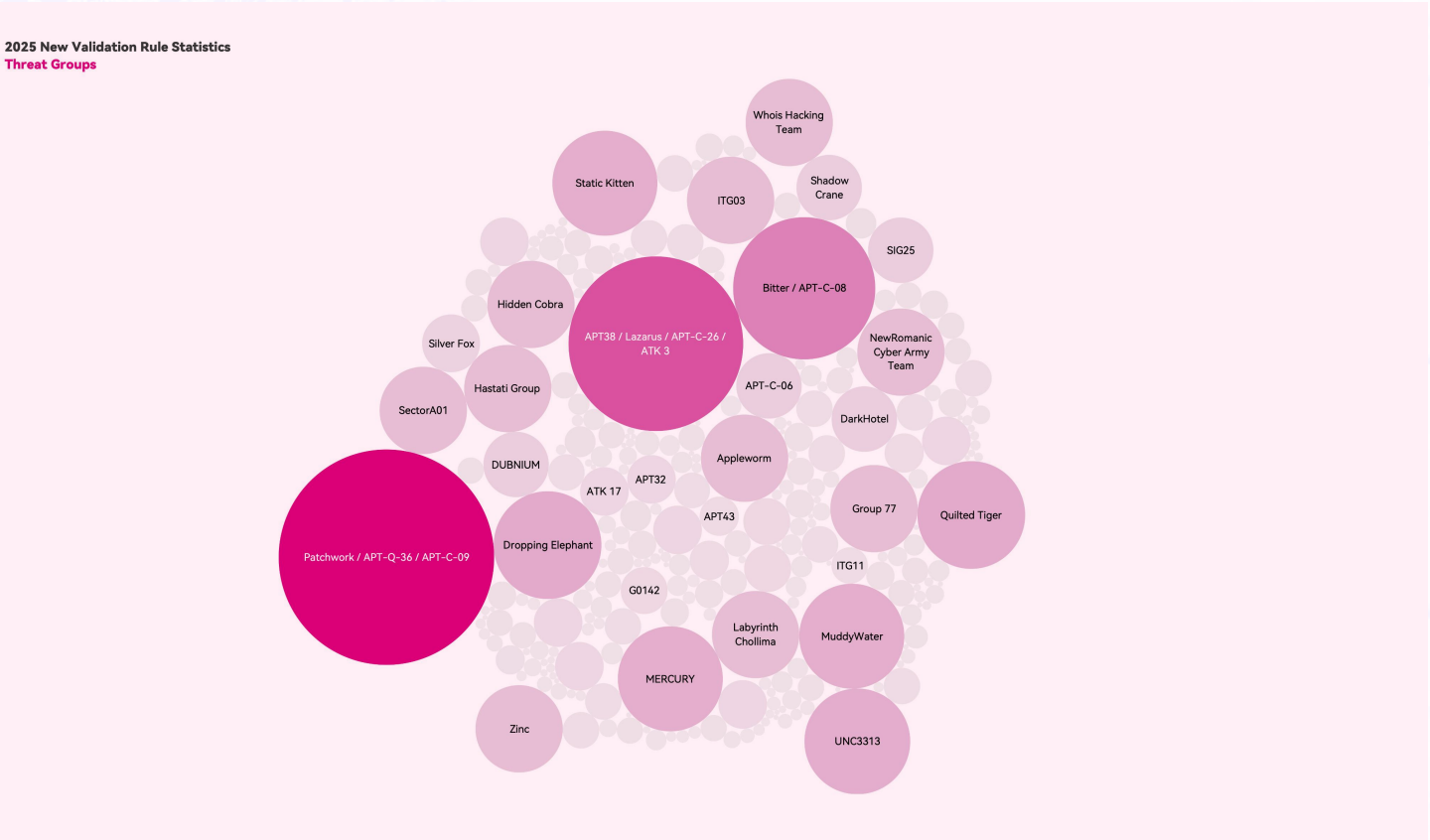
Emerging Technology Coverage

Coverage for Cloud Environments and Industrial Control Systems (ICS) continues to expand, now encompassing 18 cloud environment types and 18 ICS-specific attack techniques, supporting validation across hybrid and converged architectures.

Direct Web Validation Rules Focus

Direct Web validation rule development increasingly concentrates on core data assets and server privileges. Coverage has expanded beyond general office software to include industry-specific business systems (e.g., Logistics, Media) and Video Surveillance IoT platforms, addressing modern supply-chain and internal pivoting risks.

Global Threat Actor Activity



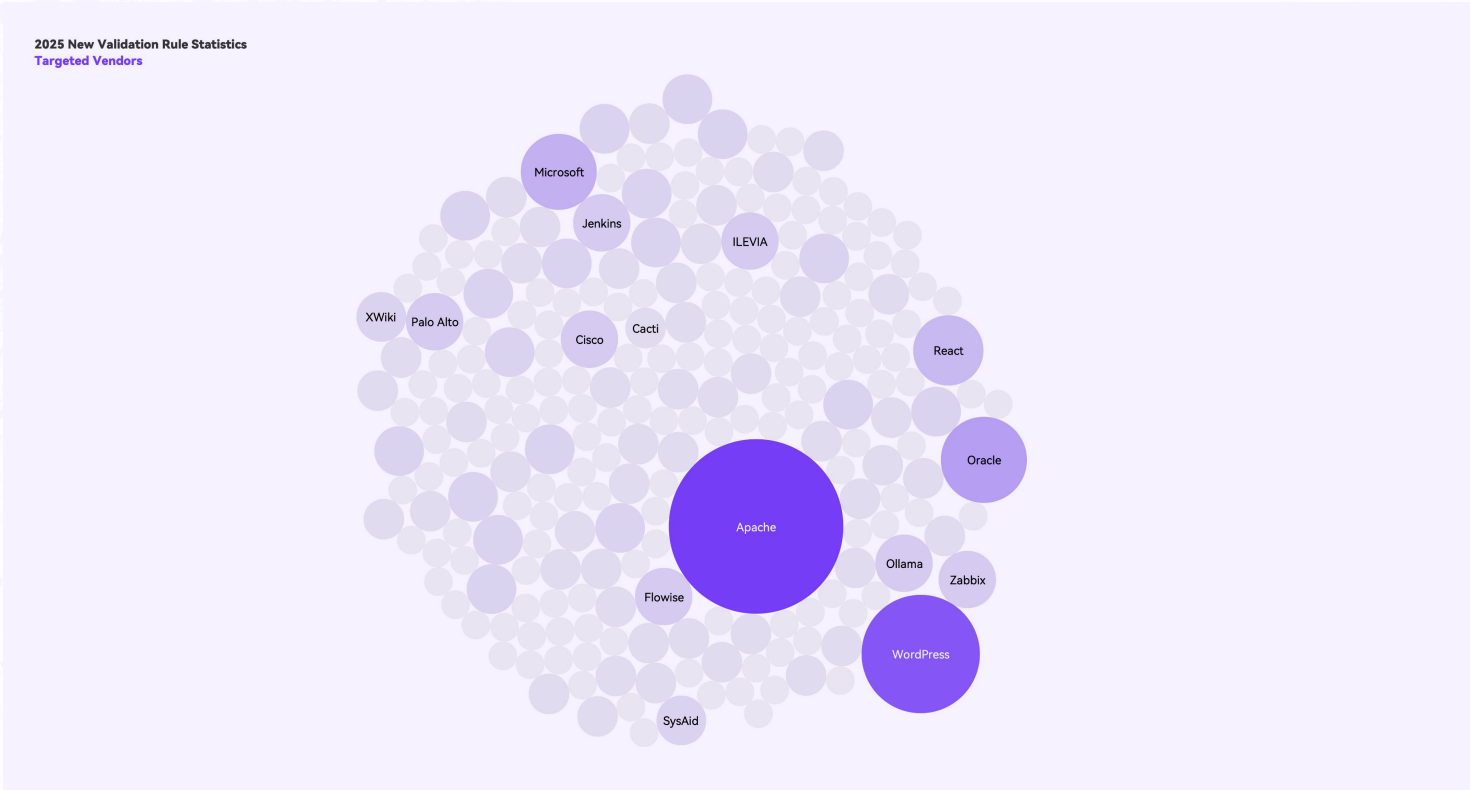
In 2025, 270 threat groups were tracked.
APT38 (Lazarus) and Patchwork remain among the most active, conducting espionage-driven campaigns targeting government, finance, and research institutions, particularly in the APAC region.

Malware Distribution

The Shift Toward Tooling

The library now covers 415 malware families.
Trojans and HackTools account for the largest share, surpassing ransomware in volume, indicating a focus on remote access, persistence, and data theft.

Target Ecosystem & Supply Chain Risks



Enterprise Core Software as the Bullseye

Attack activity is highly concentrated on enterprise-grade business software. Vendors providing ERP, CRM, and OA platforms occupy the center of the target map, reflecting attackers' focus on business-critical systems with high downstream impact.

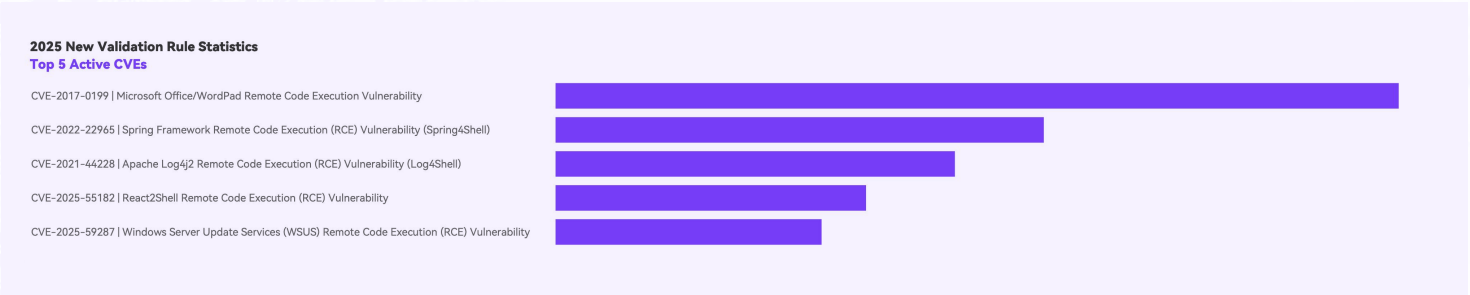
Infrastructure Risks Persist

- Apache ecosystem components (e.g., Tomcat, Struts2) remain high-risk.
- Microsoft Exchange and SharePoint continue to experience frequent exploitation.

Broad Coverage

The 2025 update spans 453 software products, covering operating systems, databases, application frameworks, and business systems, illustrating the expansive modern attack surface.

Top High-Risk Vulnerabilities



The update involves 350 CVEs. The TOP 5 most utilized vulnerabilities include both persistent legacy issues and critical 2025 threats:

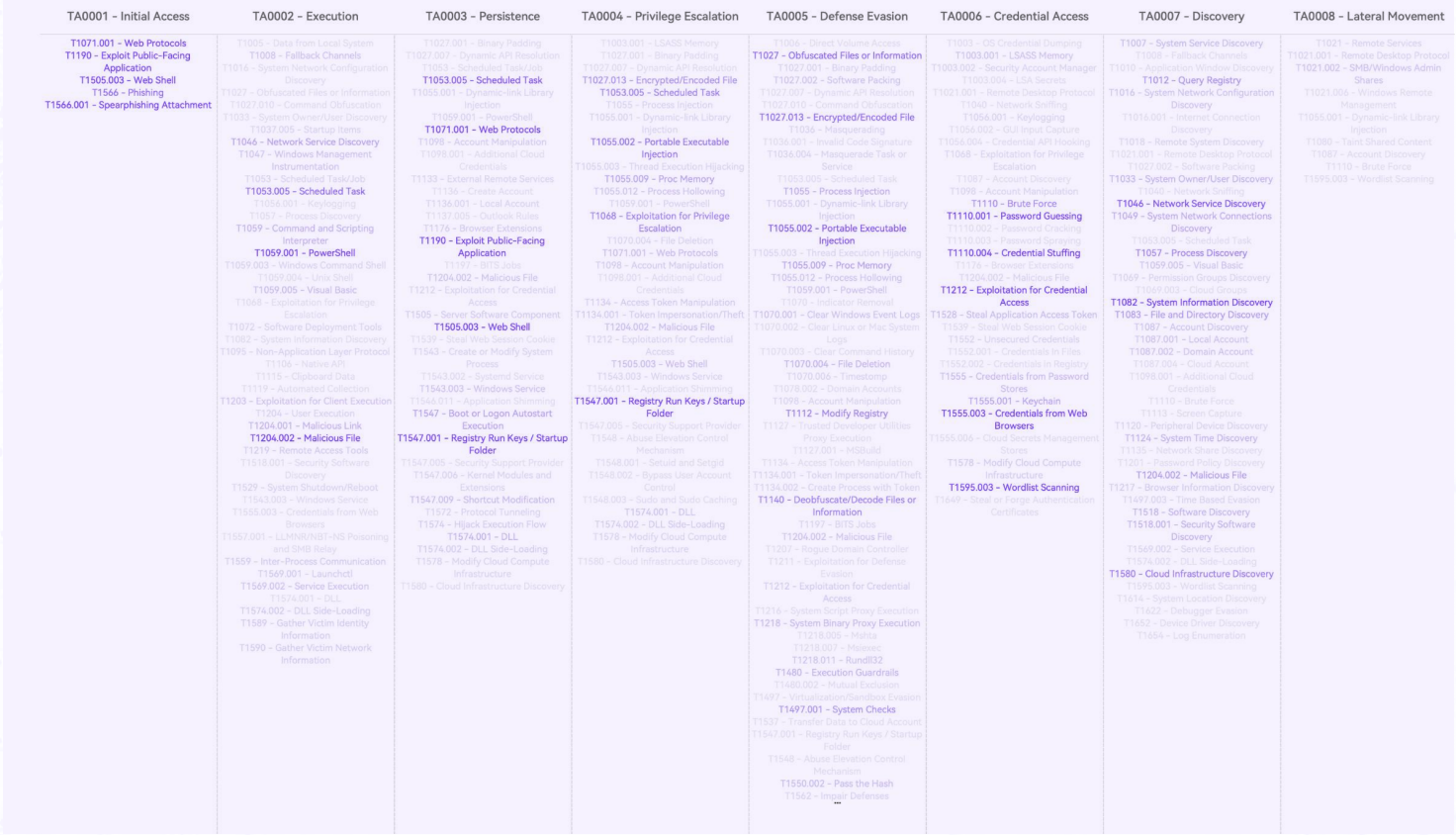
1. CVE-2017-0199 (Microsoft Office RTF): An enduring document exploit, continuously used in phishing campaigns.
2. CVE-2022-22965 (Spring4Shell): A critical RCE in the Spring Framework, posing a massive threat to the Java ecosystem.
3. CVE-2021-44228 (Log4j): The "Nuclear-level" vulnerability, still heavily scanned and exploited by botnets and APT groups.
4. CVE-2025-55182 (React2Shell RCE): A new high-risk vulnerability in a popular frontend framework emerging in 2025, allowing direct server control.
5. CVE-2025-59287 (Windows Server Update Services - WSUS): Attacks targeting enterprise patch distribution servers; compromising this leads to total internal network compromise.

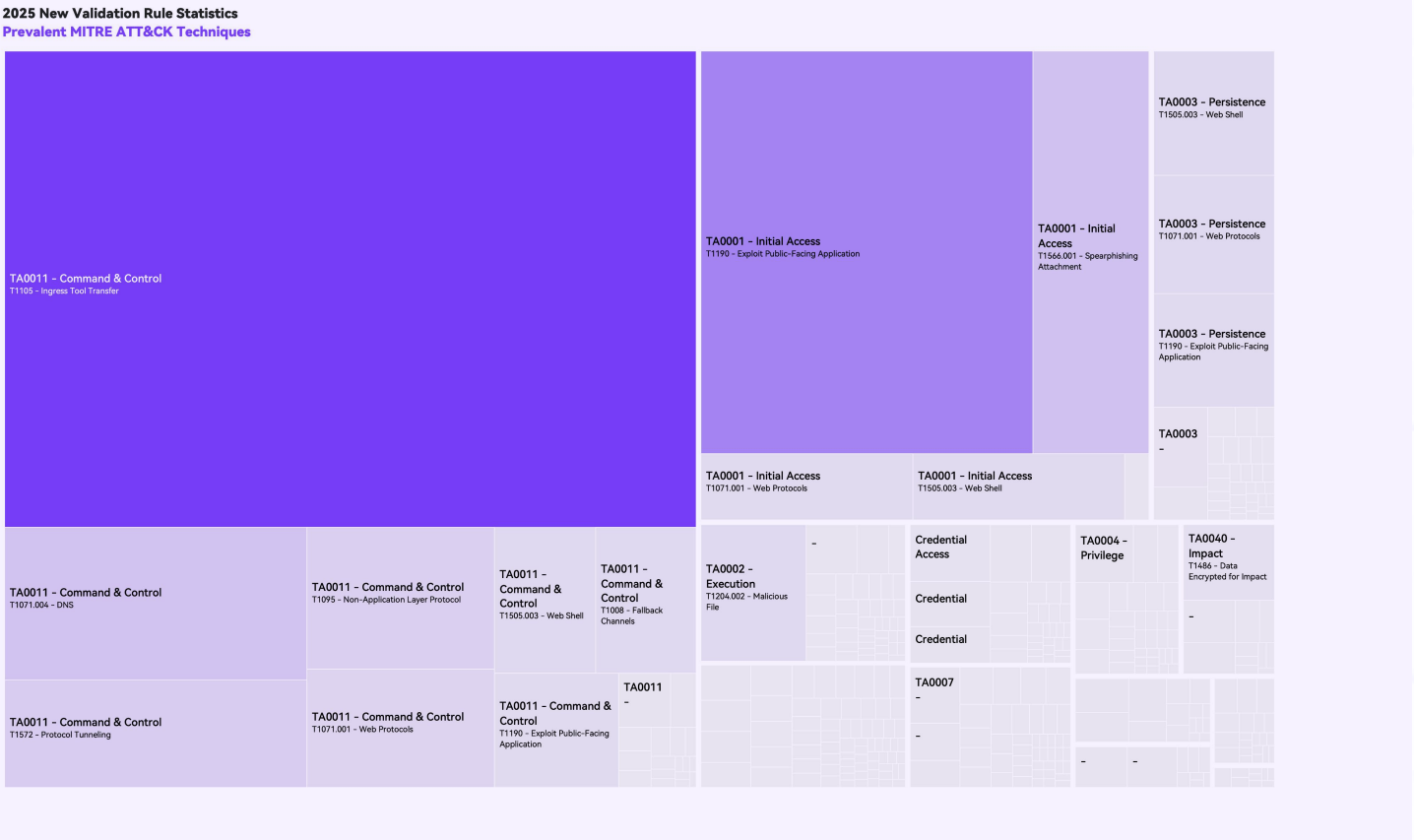
Trend Analysis: Old and new vulnerabilities coexist. The rampant use of historical vulnerabilities (2017, 2021) indicates significant blind spots in enterprise patch management, while the rapid weaponization of 2025 vulnerabilities demands agile emergency response capabilities.

MITRE ATT&CK Mapping & Technique Distribution

2025 New Validation Rule Statistics

MITRE ATT&CK Mapping





Command & Control (C2) Takes Center Stage

The 2025 ATT&CK heatmap shows TA0011 (Command and Control) accounting for a significant proportion of new rules, particularly:

- T1071 – Application Layer Protocol
- T1572 – Protocol Tunneling

This reflects sustained attacker investment in covert communication channels designed to evade network visibility and inspection.

Balancing Initial Access and Persistence

- Initial Access (TA0001): Exploiting public-facing applications (T1190) and phishing remain dominant.
- Persistence (TA0003): Webshell implantation and system process hijacking continue to be widely used to maintain long-term footholds.

Technical Insights

New rules now cover 214 distinct ATT&CK techniques. Defense Evasion (TA0005) and Credential Access (TA0006) techniques have diversified, reflecting attacker adaptation to improved encrypted traffic inspection and memory-based detection controls.

Web Application Threat Analysis

SQL Injection Dominance

SQL Injection remains the most prevalent web attack vector, with 455 rules covering multiple bypass and exploitation techniques aimed at direct database compromise.

File Operation Vulnerabilities

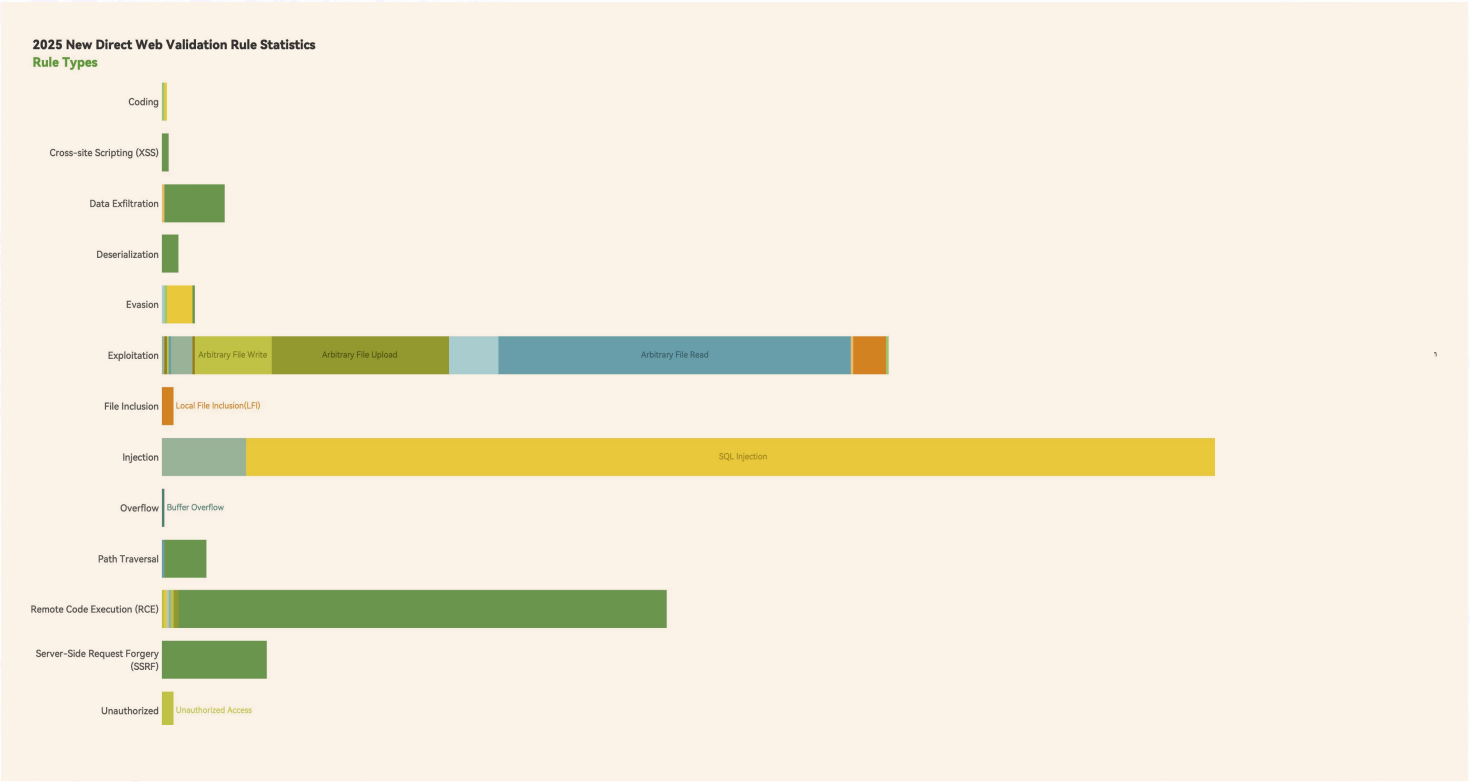
- Arbitrary File Read: 146 rules
- Arbitrary File Upload: 84 rules

These vulnerabilities frequently serve as gateways for Webshell deployment and sensitive data leakage.

Defense Recommendation

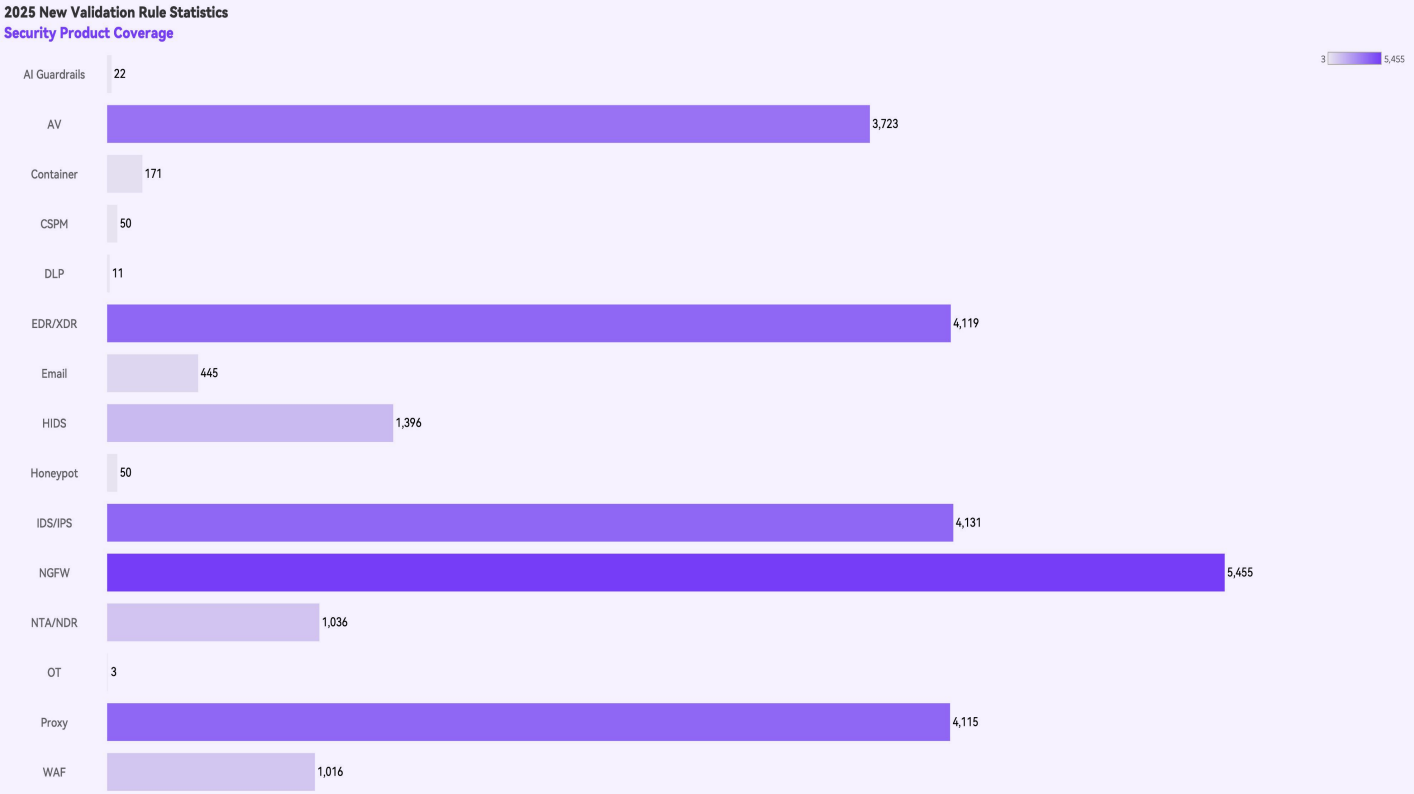
Organizations should strengthen monitoring across Web, host, and database layers, with strict control over file upload and file access interfaces.

Direct Web Validation Rule Distribution



SQL Injection dominates Direct Web Validation Rule volume due to its prevalence and impact.
File operation abuse and authentication bypass techniques show strong growth, particularly within enterprise business systems.

Security Product Coverage



Validation rules now span the entire defense-in-depth architecture:

- NGFW: 5,455 rules
- IDS/IPS: 4,131 rules
- EDR/XDR: 4,119 rules

Highlight: AI Application Security

AI applications are included as a distinct validation category in 2025, with initial rule coverage focused on common LLM exposure patterns. This area is expected to expand rapidly alongside enterprise AI adoption.

Full-Stack Coverage

From WAFs and Proxies, to AV, HIDS, and EDR, and extending into cloud-native container security, validation coverage now spans the full modern IT stack.

About digiDations

digiDations is an industry-leading provider of Intelligent Full-Stack Security Validation Solutions, helping organizations continuously and proactively validate their real security posture before adversaries do.

In a threat landscape where traditional assessments and point-in-time testing fail to keep pace with real-world attacks, digiDations combines artificial intelligence, engineered threat intelligence, and adversary tradecraft research to deliver next-generation security validation. Our platforms are designed to think like attackers, adapt like attackers, and measure defense effectiveness against how attacks actually unfold.

Built on the principles of Gartner Continuous Threat Exposure Management (CTEM), digiDations focuses on the visualization and digitization of defense efficacy, enabling enterprises to answer critical questions such as: Are our defenses effective? Which controls truly stop attacks? Where are our real gaps?

Powered by a proprietary AI Attack–Defense Reasoning Engine, digiDations integrates software supply-chain security, internet attack surface management, security control validation, and direct web validation efficacy assessment into a unified framework. Closely collaborating with Nanyang Technological University's research ecosystem, our team brings deep expertise from global cybersecurity vendors and APT research institutions, committed to becoming a long-term guardian of enterprise digital resilience.

www.digidations.com
info@digidations.com

digiDations

Continuously Validate Continuously Secure