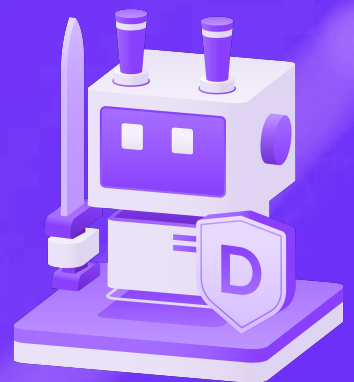


ATLAS™ Security Validation Platform 2025 Annual Report

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



Contents

Executive Summary

Key Findings

ATLAS™ Security Validation Platform Attack Library Annual Updates

Global Threat Actor Activity

Malware Distribution

Target Ecosystem & Supply Chain Risks

Top High-Risk Vulnerabilities

MITRE ATT&CK Mapping & Technique Distribution

Web Application Threat Analysis

Direct Web Validation Rule Distribution

Security Product Coverage

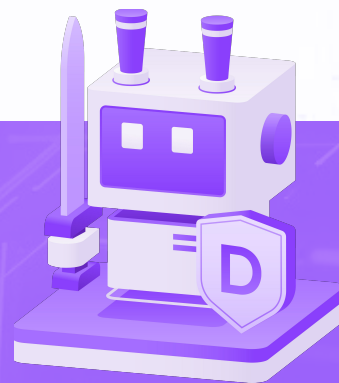
Executive Summary

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

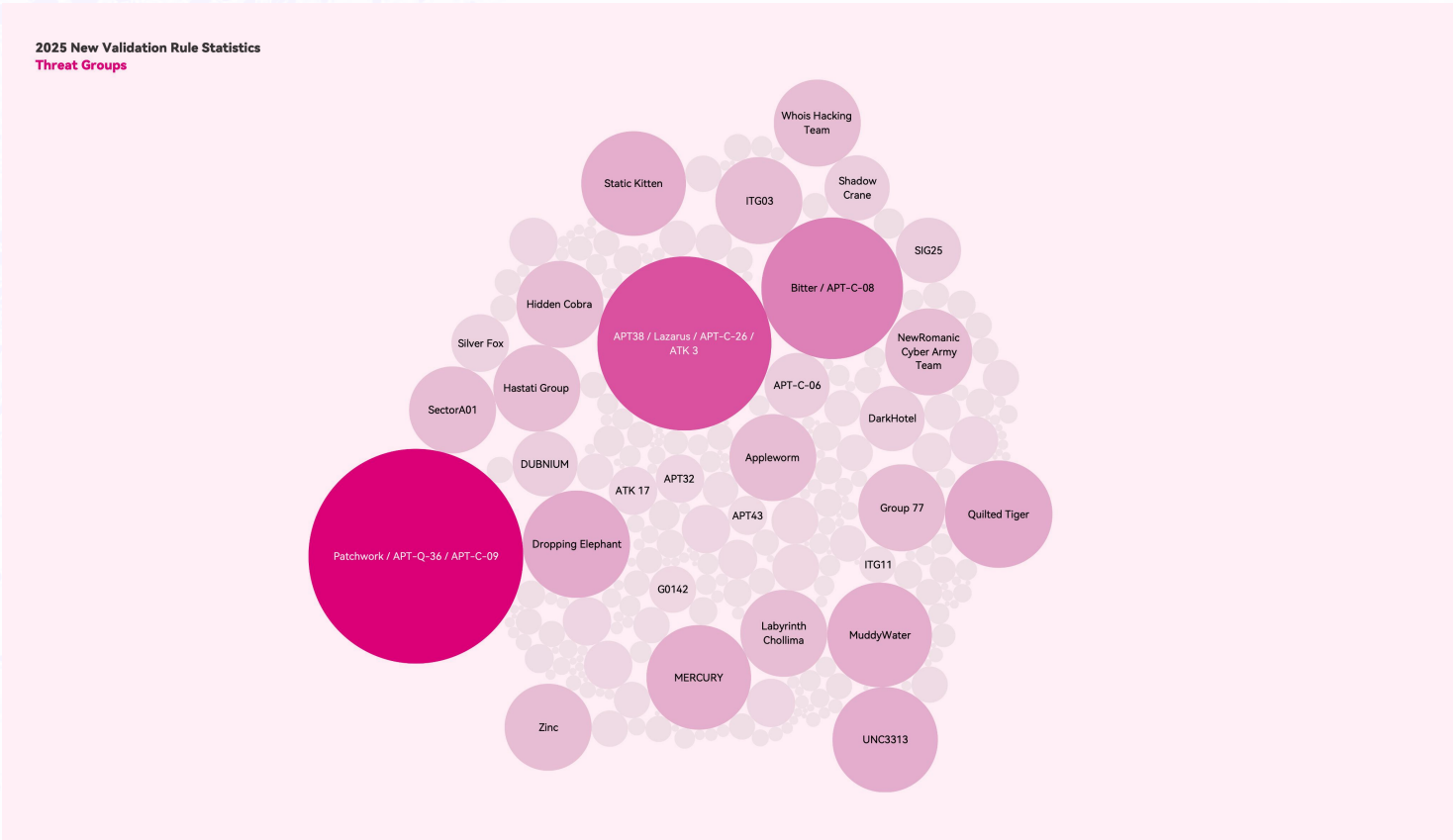
Coverage for Cloud Environments and Industrial Control Systems (ICS) continues to expand, now encompassing 18 cloud environment types and 18 ICS-specific attack techniques, supporting validation across hybrid and converged architectures.



Direct Web Validation Rules Focus

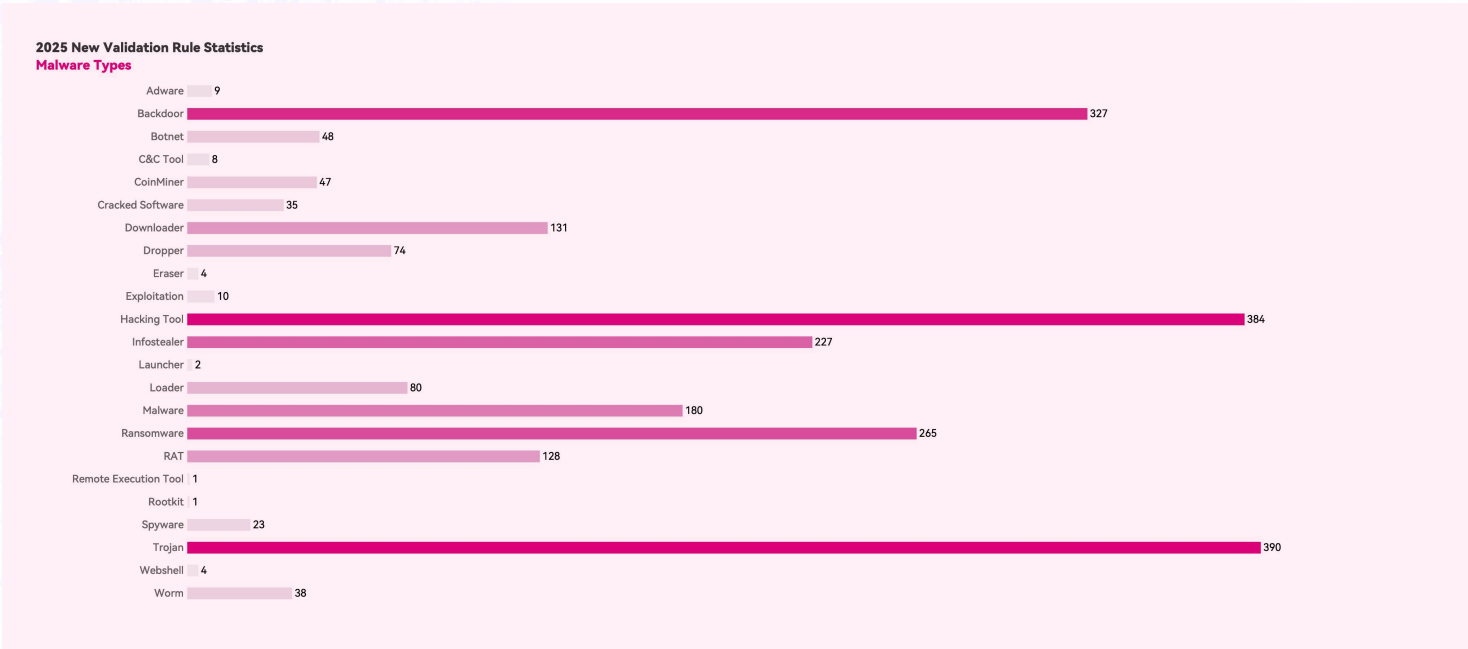
Direct Web validation rule development increasingly concentrates on core data assets and server privileges. Coverage has expanded beyond general office software to include industry-specific business systems (e.g., Logistics, Media) and Video Surveillance IoT platforms, addressing modern supply-chain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

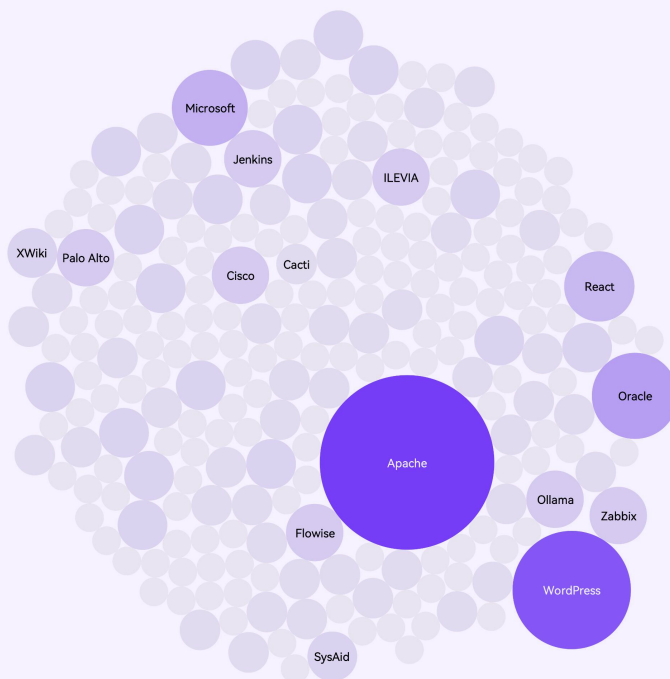


The Shift Toward Tooling

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

2025 New Validation Rule Statistics
Targeted Vendors



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

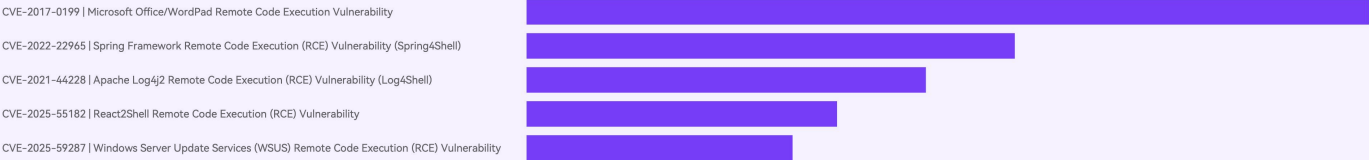
- Apache ecosystem components (e.g., Tomcat, Struts2) remain high-risk.
- Microsoft Exchange and SharePoint continue to experience frequent exploitation.

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

2025 New Validation Rule Statistics
Top 5 Active CVEs



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							
TA0001 - Initial Access	TA0002 - Execution	TA0003 - Persistence	TA0004 - Privilege Escalation	TA0005 - Defense Evasion	TA0006 - Credential Access	TA0007 - Discovery	TA0008 - Lateral Movement
T1071.001 - Web Protocols T1190 - Exploit Public-Facing Application T1505.003 - Web Shell T1566 - Phishing T1566.001 - Spearphishing Attachment	T1005 - Data from Local System T1008 - fallback Channels T1016 - System Network Configuration Discovery T1027 - Obfuscated Files or Information T1027.010 - Command Obfuscation T1033 - System Owner/User Discovery T1037.005 - Startup Items T1046 - Network Service Discovery T1047 - Windows Management Instrumentation T1003 - Scheduled Task/Job T1053.005 - Scheduled Task T1054.001 - Keylogging T1057 - Process Discovery T1059 - Command and Scripting Interpreter T1059.001 - PowerShell T1059.003 - Windows Command Shell T1059.004 - Unix Shell T1059.005 - Visual Basic T1068 - Exploitation for Privilege Escalation T1072 - Software Deployment Tools T1082 - System Information Discovery T1095 - Non-Application Layer Protocol T1106 - Native API T1115 - Clipboard Data T1119 - Automated Collection T1203 - Exploitation for Client Execution T1204.001 - Malicious File T1219 - Remote Access Tools T1549.001 - Security Software Discovery T1529 - System Shutdown/Reboot T1543.003 - Windows Service T1555.003 - Credentials from Web Browsers T1557.001 - LLMNR/NBT-NS Poisoning and SMB Relay T1559 - Inter-Process Communication T1569.001 - Launches T1569.002 - Service Execution T1574.001 - DLL T1574.002 - DLL Side-Loading T1589 - Gather Victim Identity Information T1590 - Gather Victim Network Information	T1027.001 - Binary Padding T1027.007 - Dynamic API Resolution T1027.008 - Dynamic API Invocation T1053.005 - Scheduled Task T1055.001 - Dynamic-link Library Injection T1059.001 - PowerShell T1071.001 - Web Protocols T1098 - Account Manipulation T1098.001 - Additional Cloud Credentials T1133 - External Remote Services T1136 - Create Account T1136.001 - Local Account T1137.005 - Outlook Rules T1176 - Browser Extensions T1190 - Exploit Public-Facing Application T1197 - BITS Jobs T1204.002 - Malicious File T1212 - Exploitation for Credential Access T1505 - Server Software Component T1505.003 - Web Shell T1539 - Steal Web Session Cookie T1543 - Create or Modify System Process T1543.003 - Systemd Service T1543.011 - Application Shimming T1547 - Boot or Logon Autostart Execution T1547.001 - Registry Run Keys / Startup Folder T1547.005 - Security Support Provider T1547.006 - Kernel Modules and Extensions T1547.009 - Shortcut Modification T1572 - Protocol Tunneling T1574 - Hijack Execution Flow T1574.001 - DLL T1574.002 - DLL Side-Loading T1578 - Modify Cloud Compute Infrastructure T1580 - Cloud Infrastructure Discovery	T1003.001 - LSASS Memory T1027.001 - Binary Padding T1027.007 - Dynamic API Resolution T1027.013 - Encrypted/Encoded File T1053.005 - Scheduled Task T1055 - Process Injection T1055.001 - Dynamic-link Library Injection T1055.002 - Portable Executable Injection T1055.003 - Thread Execution Hijacking T1055.009 - Proc Memory T1059.012 - Process Hollowing T1059.001 - PowerShell T1068 - Exploitation for Privilege Escalation T1070.004 - File Deletion T1071.001 - Web Protocols T1098 - Account Manipulation T1098.001 - Additional Cloud Credentials T1134 - Access Token Manipulation T1134.001 - Token Impersonation/Theft T1204.002 - Malicious File T1212 - Exploitation for Credential Access T1505.003 - Web Shell T1543.003 - Windows Service T1543.011 - Application Shimming T1547.001 - Registry Run Keys / Startup Folder T1548 - Abuse Elevation Control Mechanism T1548.001 - Setuid and Setgid T1548.002 - Bypass User Account Control T1548.003 - Sudo and Sudo Caching T1574.001 - DLL T1574.002 - DLL Side-Loading T1578 - Modify Cloud Compute Infrastructure T1580 - Cloud Infrastructure Discovery	T1006 - Direct Volume Access T1027 - Obfuscated Files or Information T1027.001 - Binary Padding T1027.007 - Dynamic API Resolution T1027.010 - Command Obfuscation T1027.013 - Encrypted/Encoded File T1036.001 - Invalid Code Signature T1036.004 - Masquerade Task or Service T1053.005 - Scheduled Task T1055 - Process Injection T1055.001 - Dynamic-link Library Injection T1055.002 - Portable Executable Injection T1055.003 - Thread Execution Hijacking T1059.012 - Process Hollowing T1059.001 - PowerShell T1070.003 - Clear Windows Event Logs T1070.002 - Clear Linux or Mac System Logs T1070.003 - Clear Command History T1070.004 - File Deletion T1070.006 - Timestamp T1078.002 - Domain Accounts T1098 - Account Manipulation T1127 - Modify Registry T1127.001 - MSBuild T1134 - Access Token Manipulation T1134.001 - Token Impersonation/Theft T1134.002 - Create Process with Token T1140 - Deobfuscate/Decode Files or Information T1197 - BITS Jobs T1204.002 - Malicious File T1207 - Rogue Domain Controller T1211 - Exploitation for Defense Evasion T1212 - Exploitation for Credential Access T1216 - System Script Proxy Execution T1218 - System Binary Proxy Execution T1218.002 - Mutual Exclusion T1218.001 - Molevec T1218.011 - Rundll32 T1480 - Execution Guardrails T1480.002 - Mutual Exclusion T1497 - Virtualization/Sandbox Evasion T1497.001 - System Checks T1537 - Transfer Data to Cloud Accounts T1547.001 - Registry Run Keys / Startup Folder T1548 - Abuse Elevation Control Mechanism T1550.002 - Pass the Hash T1562 - Impair Defenses	T1003 - OS Credential Dumping T1003.001 - LSASS Memory T1003.002 - Security Account Manager T1003.004 - LSA Secrets T1021.001 - Remote Desktop Protocol T1040 - Network Sniffing T1056.001 - Keylogging T1056.002 - GUI Input Capture T1056.004 - Credential API Hooking T1068 - Exploitation for Privilege Escalation T1087 - Account Discovery T1087.002 - Software Patching T1093 - System Owner/User Discovery T1093.001 - Password Cracking T1110.004 - Credential Stuffing T1176 - Browser Extensions T1176.001 - Malicious File T1212 - Exploitation for Credential Access T1528 - Steal Application Access Token T1539 - Steal Web Session Cookie T1552 - Unsecured Credentials T1552.001 - Credentials in Files T1552.002 - Credentials in Registry T1555 - Credentials from Password Stores T1555.001 - Anychain T1555.003 - Credentials from Web Browsers T1555.006 - Cloud Secrets Management Stores T1578 - Modify Cloud Compute Infrastructure T1593.002 - Wordlist Scanning T1649 - Steal or Forge Authentication Certificates	T1007 - System Service Discovery T1008 - fallback Channels T1010 - Architecture Windows Discovery T1012 - Query Registry T1016 - System Network Configuration Discovery T1016.001 - Internet Connection Discovery T1018 - Remote System Discovery T1021.001 - Remote Desktop Protocol T1027.002 - Software Patching T1033 - System Owner/User Discovery T1033.001 - Password Cracking T1093 - System Information Discovery T1093.001 - Visual Basic T1099 - Permission Groups Discovery T1108 - File and Directory Discovery T1139 - Screen Capture T1120 - Peripheral Device Discovery T1124 - System Time Discovery T1135 - Network Share Discovery T1201 - Forensic Policy Discovery T1204.002 - Malicious File T1217 - Browser Information Discovery T1497.003 - Time Based Evasion T1518 - Software Discovery T1518.001 - Security Software Discovery T1549.002 - Service Execution T1549.003 - Side-Loading T1580 - Cloud Infrastructure Discovery T1595.003 - Wordlist Scanning T1614 - System Location Discovery T1622 - Debugger Evasion T1652 - Device Driver Discovery T1654 - Log Enumeration	T1021 - Remote Services T1021.001 - Remote Desktop Protocol T1021.002 - SMB/Windows Admin Shares T1021.006 - Windows Remote Management T1055.001 - Dynamic-link Library Injection T1080 - Taint Shared Content T1087 - Account Discovery T1110 - Brute Force T1195.003 - Wordlist Scanning
TA0009 - Collection	TA0010 - Exfiltration	TA0011 - Command & Control	TA0040 - Impact	TA0043 - Reconnaissance			
T1005 - Data from Local System T1025 - Data from Removable Media T1033 - System Owner/User Discovery T1048 - Exfiltration Over Alternative Protocol T1049 - System Network Connections Discovery T1056 - Input Capture T1056.001 - Keylogging T1056.002 - GUI Input Capture T1057 - Process Discovery T1082 - System Information Discovery T1083 - File and Directory Discovery T1087.001 - Local Accounts T1113 - Screen Capture T1115 - Clipboard Data T1119 - Automated Collection T1204.002 - Malicious File T1518.001 - Security Software Discovery T1557.001 - LLMNR/NBT-NS Poisoning and SMB Relay T1560 - Archive Collected Data T1560.001 - Archive via Utility	T1001.003 - Protocol or Service Impersonation T1041 - Exfiltration Over C2 Channel T1048 - Exfiltration Over Alternative Protocol T1048.001 - Exfiltration Over Symmetric Encrypted Non-C2 Protocol T1048.002 - Exfiltration Over Asymmetric Encrypted Non-C2 Protocol T1071.001 - Web Protocols T1095 - Non-Application Layer Protocol T1486 - Data Encrypted for Impact T1490 - Inhibit System Recovery T1537 - Transfer Data to Cloud Account T1560 - Archive Collected Data T1567 - Exfiltration Over Web Service T1571 - Non-Standard Port T1572 - Protocol Tunneling T1578 - Modify Cloud Compute Infrastructure	T1001.002 - Steganography T1001.003 - Protocol or Service Impersonation T1008 - fallback Channels T1025 - Data from Removable Media T1048.001 - Exfiltration Over Symmetric Encrypted Non-C2 Protocol T1048.002 - Exfiltration Over Asymmetric Encrypted Non-C2 Protocol T1071.001 - Web Protocols T1071.002 - File Transfer Protocols T1071.004 - DNS T1072 - Multi-Targeted Attacks T1090.001 - Internal Proxy T1095 - Non-Application Layer Protocol T1102.002 - Bidirectional Communication T1103 - Multi-Targeted Attacks T1132.001 - Standard Encoding T1190 - Exploit Public-Facing Application T1204.002 - Malicious File T1219 - Remote Access Tools T1505.003 - Web Shell T1571 - Non-Standard Port T1572 - Protocol Tunneling T1573.001 - Symmetric Cryptography T1573.002 - Asymmetric Cryptography	T1041 - Exfiltration Over C2 Channel T1204.002 - Malicious File T1485 - Data Destruction T1486 - Data Encrypted for Impact T1490 - Inhibit System Recovery T1491 - Defacement T1491.001 - Internal Defacement T1496 - Resource Hijacking T1529 - System Shutdown/Reboot T1589 - Gather Victim Identity Information T1590 - Gather Victim Network Information	T1021.001 - Remote Desktop Protocol T1087 - Account Discovery T1110 - Brute Force T1110.001 - Password Guessing T1204.002 - Malicious File T1529 - System Shutdown/Reboot T1589 - Gather Victim Identity Information T1590 - Gather Victim Network Information T1595.003 - Wordlist Scanning			



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.

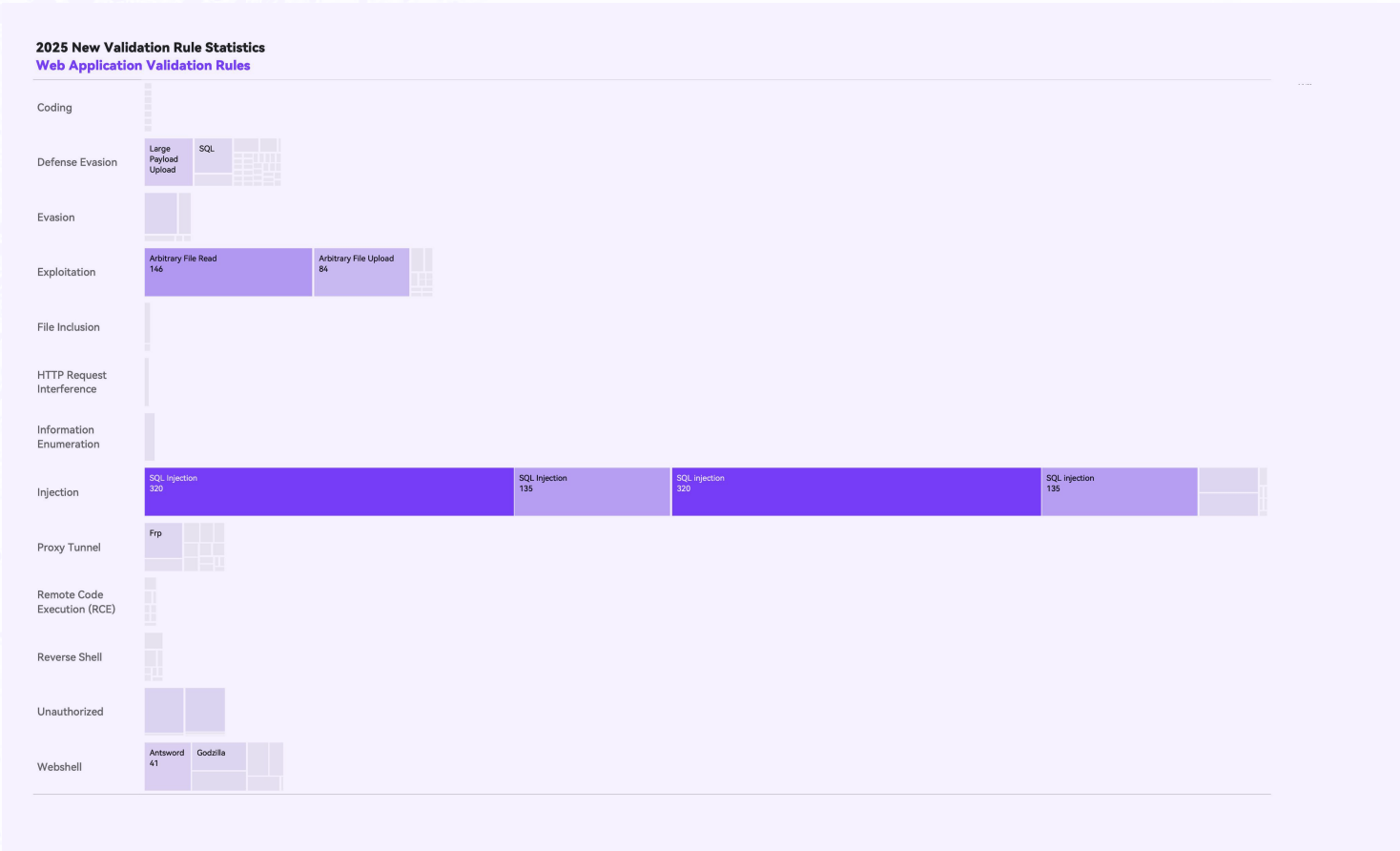
Balancing Initial Access and Persistence

- 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

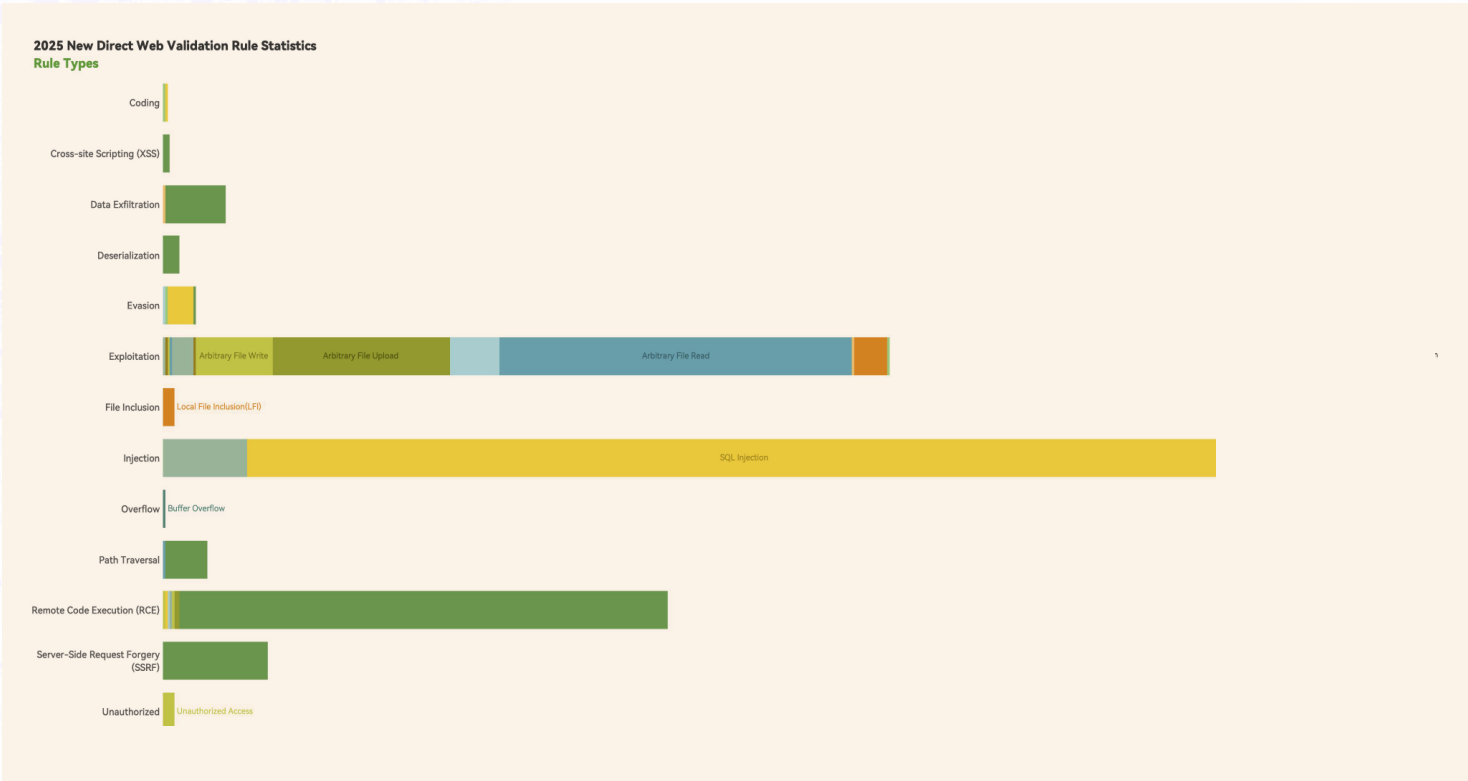
- Arbitrary File Read: 146 rules
- Arbitrary File Upload: 84 rules

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.

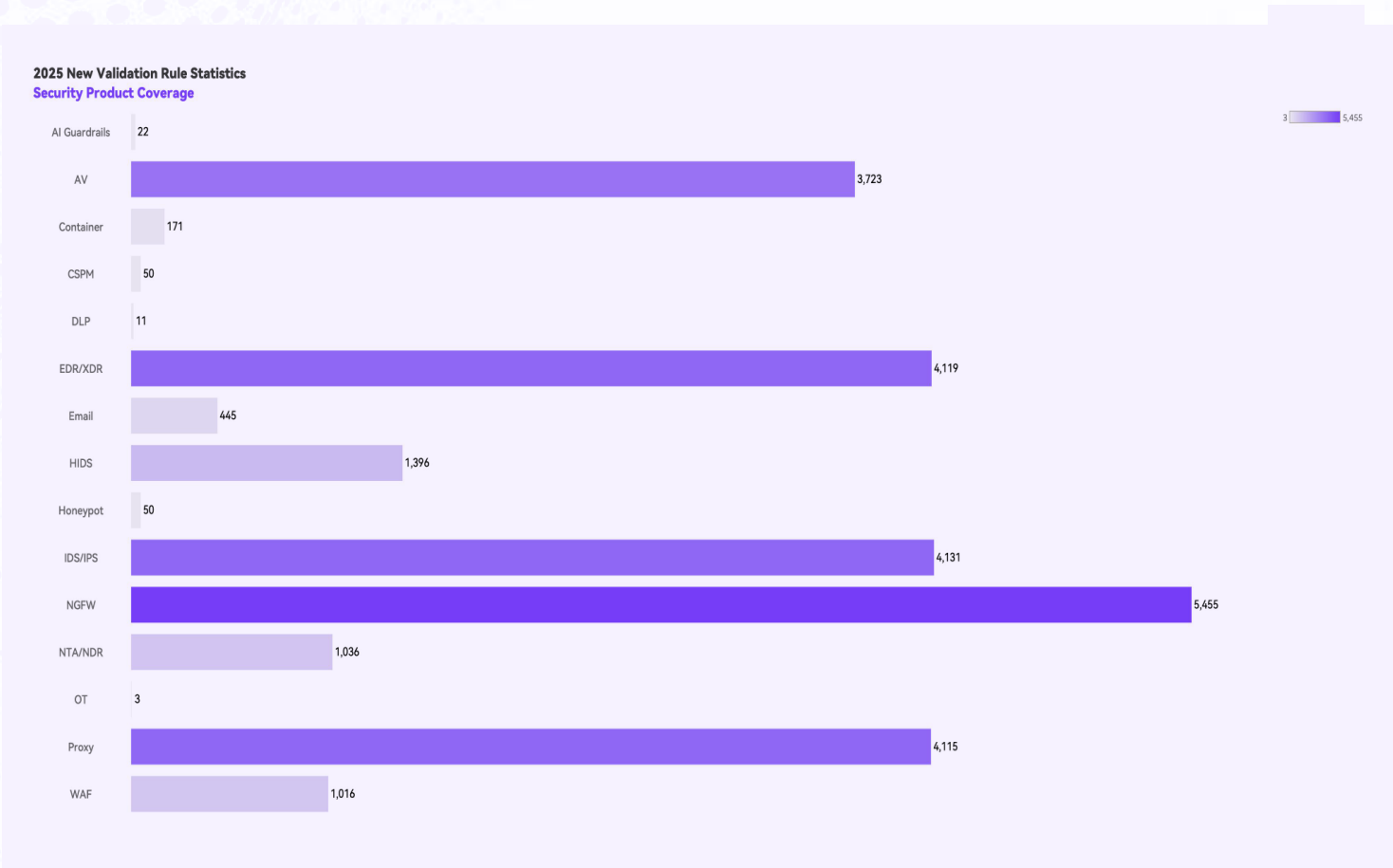
Direct Web Validation Rule Distribution



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