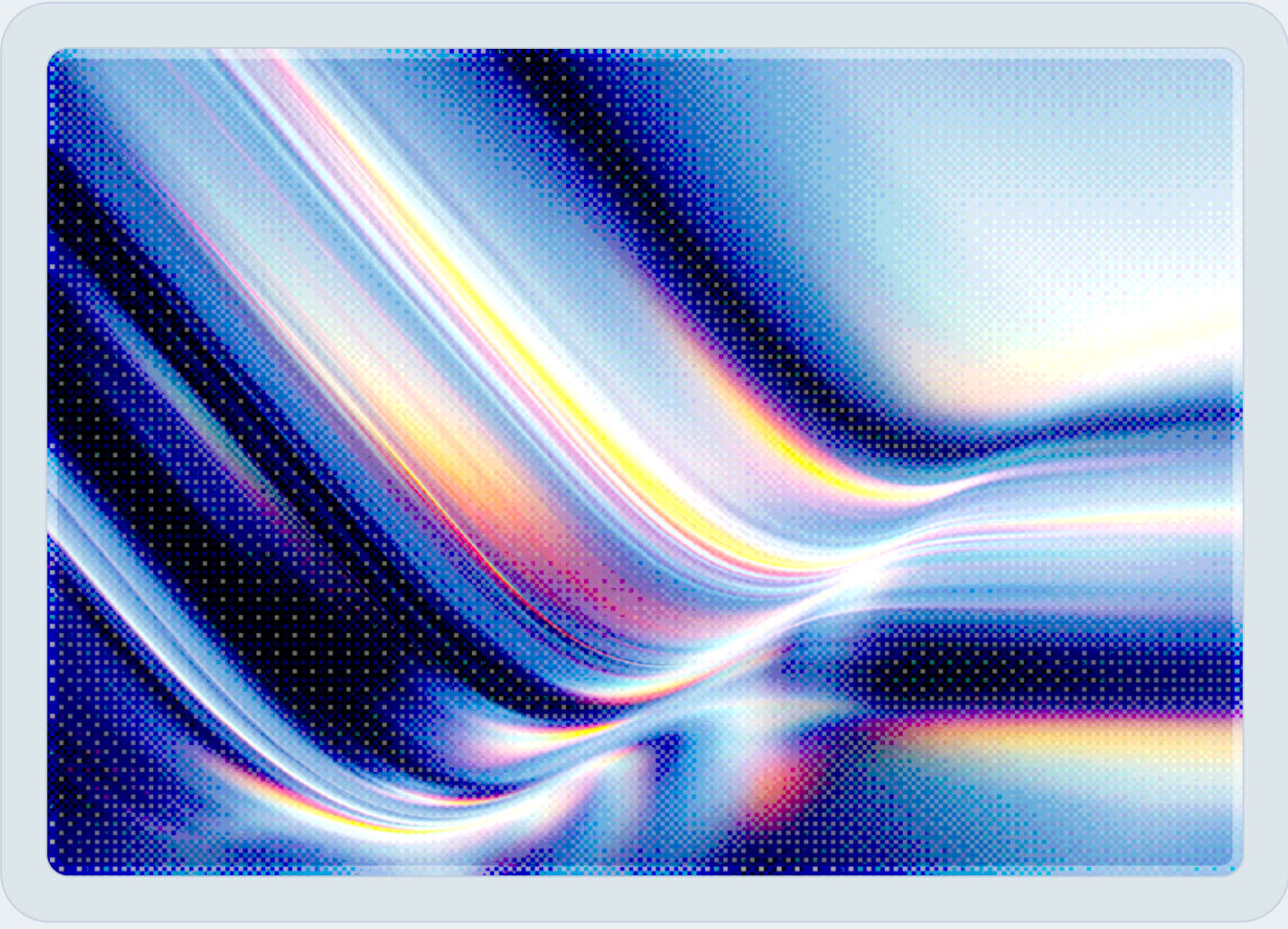
CSAI Foundation | Cloud Security Alliance

The AI-Compressed Exposure Window: A Unit 42 Reading

What the 2026 Global Incident Response Report Means for Vulnerability Management

2026-07-20

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

© 2026 Cloud Security Alliance. Some rights reserved.

You may download, store, display, view, print, redistribute, and link to this document in its original, unmodified form, provided that attribution to the Cloud Security Alliance is maintained and all trademark and copyright notices remain intact.

This document may not be modified or altered. You may quote portions of the document as permitted by the Fair Use provisions of the United States Copyright Act, provided that attribution is given to the Cloud Security Alliance.

This document may be shared on professional and social media platforms in its original form with attribution.

This document was generated with AI assistance and has not undergone official CSA review and approval processes.

Key Takeaways

- Palo Alto Networks' Unit 42, drawing on more than 750 incident response engagements across over 50 countries, found that the fastest quartile of 2025 intrusions reached data exfiltration in 72 minutes from initial access, down from 285 minutes in 2024 — a fourfold acceleration that Unit 42 attributes to AI acting as a "force multiplier" across the attack lifecycle rather than to any fundamentally new method of compromise [1][2].
- Identity weaknesses, not software vulnerabilities, now dominate initial access: identity-based techniques drove 65% of initial access, and Unit 42 reports that identity weaknesses "played a material role in almost 90%" of investigations, compared with 22% of initial access attributable to exploited vulnerabilities [2][3].
- Unit 42's 2026 report reiterates a benchmark it first documented in 2022 — that attackers begin scanning for exploitation opportunities within roughly 15 minutes of a CVE's public disclosure — and frames AI tooling as generalizing this behavior across a wider population of attackers, though the report does not present a re-measured 2025 timing figure confirming that the benchmark itself has held or tightened [4][5].
- More than 90% of the breaches Unit 42 investigated were enabled by preventable misconfigurations or visibility gaps rather than novel attacker sophistication, and an analysis of over 680,000 cloud identities found that 99% carried excessive permissions — which this note reads as evidence that the exposure window is, in most cases, a governance failure that AI speed simply makes more costly, rather than a product of attacker sophistication [2][3].
- Because AI compresses both discovery and exploitation, CSA's guidance argues that vulnerability management must shift from a periodic patch cadence to continuous, largely automated triage and containment; this note connects the Unit 42 findings to that guidance and to concrete steps organizations can take in the next 30 to 90 days.

Background

Unit 42's Global Incident Response Report has tracked attacker dwell time and exploitation speed for several years, but the 2026 edition, published in February 2026 and based on analysis of more than 750 major incidents investigated in 2025 across over 50 countries and every major industry, marks the point

at which artificial intelligence measurably changed the shape of the data [1][2]. The report's central claim is not that AI has introduced new categories of attack. Ransomware deployment, credential theft, phishing, and known-vulnerability exploitation remain the dominant techniques, and Unit 42 is explicit that AI "is acting as a force multiplier to increase the speed and efficiency of attacks, but is not significantly redefining methods of compromise" [1]. What has changed is the time available to defenders between an attacker's first foothold and the point at which the incident becomes unrecoverable through normal detection and containment processes.

That compression is best illustrated by the report's headline statistic: in the fastest quartile of 2025 investigations, attackers moved from initial access to data exfiltration in just 72 minutes, a fourfold improvement in attacker speed over the 285-minute figure Unit 42 recorded for the equivalent cohort in 2024 [2]. Unit 42's own framing of this trend, in a companion blog post titled "Attacks Now 4x Faster," positions AI-enabled automation as the primary driver of accelerated reconnaissance, credential validation, and lateral movement [2]. In practice, automation at this level can let a single operator, or a small team supported by generative tooling, execute what previously required a coordinated, multi-stage manual effort — an extension of Unit 42's framing rather than a figure the report itself quantifies. The report also describes early evidence of "AI-enabled tradecraft" among nation-state actors and documents nascent techniques such as agentic ransomware capable of managing multiple attack stages with limited human supervision, LLM-assisted command-and-control frameworks, and "token jacking" that targets credentials exposed through cloud AI services [1].

Alongside speed, the report reframes where organizations should expect to be tested. Unit 42 found that 87% of intrusions spanned two or more attack surfaces — endpoints, networks, cloud, SaaS, and identity systems — with some incidents touching as many as ten distinct surfaces simultaneously, and that browser-based activity, largely credential harvesting through malicious or spoofed web pages, played a role in 48% of investigations [2][3]. Rather than a single hardened perimeter, defenders are contending with a distributed set of entry points that AI-assisted attackers can probe in parallel. This note reads that structural shift as one that likely favors attackers economically — the cost of testing one more surface probably falls faster for an attacker than the cost of monitoring one more surface rises for a defender — though Unit 42's report does not itself quantify that asymmetry.

Security Analysis

Identity, Not Code, Is the Primary Exposure Window

This note treats identity as the single most consequential finding for vulnerability management practitioners, and notably, one that is not about vulnerabilities at all. Unit 42 attributes 65% of initial access in its 2025 caseload to identity-based techniques — social engineering, credential misuse, and token theft — while software vulnerabilities accounted for only 22%, and identity weaknesses of some kind contributed to nearly 90% of all investigations [2][3]. A supporting analysis of more than 680,000 cloud identities found that 99% carried excessive permissions relative to what the identity's function required, and the report separately notes a 3.8-fold increase in attacks involving third-party SaaS applications since 2022, now present in roughly 23% of cases and frequently exploiting OAuth tokens and API keys rather than application code [3][4].

This matters for how organizations should read the "exposure window" framing embedded in Unit 42's title data. A traditional vulnerability management program measures exposure as the interval between a CVE's disclosure and an organization's patch deployment. Unit 42's data indicates that, for most 2025 incidents, that interval was not the operative variable at all — the initial foothold came through a credential or a token, and the AI-driven speed gains showed up downstream, in how quickly that foothold was converted into lateral movement and exfiltration. Practically, this means a vulnerability management function that measures its own success purely by patch latency is optimizing for a smaller share of the actual risk than it was five years ago, even as the consequences of any single unpatched, internet-facing flaw have grown more severe because of how quickly it can now be found and weaponized.

Where Vulnerabilities Still Matter, the Window Has Collapsed

For the 22% of initial access still attributable to exploited vulnerabilities, the timeline evidence is unambiguous. Unit 42's research indicates that attackers routinely begin scanning for a newly disclosed CVE within about 15 minutes of the advisory going public, often before a security team has finished reading it [4][5]. This is not a new phenomenon exclusive to 2026 — Unit 42 first documented the 15-minute scanning benchmark in its analysis of CVE-2022-1388, a critical F5 BIG-IP remote code execution flaw, recording 2,552 scanning and exploitation attempts within ten hours of disclosure [5]. What the 2026 report adds is a broader narrative of AI as a "friction reducer for adversaries," extending automated scanning into exploit adaptation and not just reconnaissance [1][2]. That framing is consistent with a plausible lowering of the skill floor required to participate in mass exploitation attempts across many disclosed vulnerabilities simultaneously, though the report does not itself quantify a shift in attacker skill composition.

The practical consequence is that any organization whose patch cycle assumes a multi-day or multi-week grace period between disclosure and real-world exploitation is operating against data that no longer describes the threat environment. Internet-facing assets, in particular, should be treated as being under active reconnaissance from the moment a relevant CVE is published, which argues for automated, pre-authorized patching pathways for critical, internet-facing vulnerabilities rather than change-managed cycles that assume defenders have days to plan a response.

Most Exposure Traces to Preventable Gaps, Not Attacker Sophistication

This note treats the finding that Unit 42 links more than 90% of the breaches it investigated to misconfigurations or security coverage gaps — rather than to attacker sophistication or genuinely novel techniques — as the most directly actionable for security leadership [2][3]. Sam Rubin, Unit 42's SVP of Consulting and Threat Intelligence, summarized this succinctly: "Enterprise complexity has become the adversary's greatest advantage" [9]. Combined with the finding that forensic evidence of intrusion frequently existed in security logs but went undetected because teams could not correlate data across disconnected tools, this indicates that the compressed exposure window is, in large part, a function of how much of an organization's own attack surface it can actually see and reason about at any given moment [2]. In this note's reading, AI-driven attack speed exploits this visibility gap rather than creating it, though Unit 42's report does not frame the relationship in these terms directly.

This reframing carries a specific implication for how CISOs should prioritize investment. Faster attacker timelines argue for faster detection and response capability, but Unit 42's data suggests the higher-leverage investment for most organizations is closing the underlying visibility and configuration gaps — reducing excessive permissions, consolidating fragmented identity estates, and correlating telemetry across the endpoint, cloud, SaaS, and identity domains the report identifies as the dominant multi-surface attack pattern — rather than simply purchasing faster tooling to react to an exposure created by preventable governance failures.

Recommendations

Immediate Actions

Security teams should treat the 15-minute post-disclosure scanning window as an operating assumption for any internet-facing asset and establish a pre-approved, automated patching pathway for critical CVEs on those assets so that remediation does not wait on a standard change-management cycle [4][5]. In parallel, given that identity weaknesses were a factor in close to 90% of investigated incidents,

organizations should conduct an immediate audit of standing administrative permissions across cloud identities — Unit 42's finding that 99% of the 680,000 identities it examined carried excessive permissions suggests most organizations will find material over-provisioning without needing to look far [3]. Any credential or API token associated with SaaS integrations or AI services warrants particular scrutiny given the report's documented rise in SaaS-facilitated attacks and emerging "token jacking" techniques targeting AI credentials [1][4].

Short-Term Mitigations

Because 87% of intrusions in Unit 42's dataset spanned multiple attack surfaces, organizations should prioritize correlating telemetry across endpoint, cloud, SaaS, and identity monitoring tools rather than treating each as an independent detection domain; the report notes that forensic evidence of compromise often existed in disconnected logs that teams failed to connect during active incidents [2]. Deploying phishing-resistant multifactor authentication and moving toward just-in-time, time-bound privileged access — rather than standing admin rights — directly addresses the identity-based techniques responsible for 65% of initial access [2][4]. Given that browser-based activity featured in 48% of incidents, security teams should also extend credential-harvesting detection into browser isolation or enterprise browser telemetry rather than relying solely on endpoint and network monitoring [3].

Strategic Considerations

Over a longer horizon, CISOs should treat Unit 42's data as further evidence that vulnerability management and identity governance are converging into a single discipline rather than two adjacent programs, since the report's own recommendation is to reduce exposure, advance zero trust, and tighten identity and access management as a unified response to AI-compressed attack timelines [3][4]. Organizations should also build AI-assisted defensive capability commensurate with the AI-assisted offense the report documents: correlating events across domains at machine speed and enabling pre-authorized containment actions before an attacker completes lateral movement, consistent with the broader industry shift toward continuous, automated vulnerability operations described in CSA's own guidance on AI-accelerated threats [6].

CSA Resource Alignment

Unit 42's findings map most directly onto CSA's "AI Vulnerability Storm": Building a "Mythos-ready" Security Program, an expedited strategy briefing developed with the CSA CISO Community in response to the same structural shift — AI compressing the interval between vulnerability discovery, exploitation, and impact — that the 2026 Incident Response Report quantifies from the defender's side [6]. Where Unit 42 supplies empirical evidence that time-to-exploit has collapsed and that AI now functions as a force multiplier for attackers, CSA's briefing supplies the corresponding organizational response: it recommends establishing a dedicated Vulnerability Operations (VulnOps) function, moving to continuous rather than periodic patch triage, and pre-authorizing containment actions so that security teams can act at the speed the Unit 42 data now demands rather than the speed a traditional change-management process allows. Organizations reading the Unit 42 report for evidence of urgency should treat the AI Vulnerability Storm briefing's 90-day priority-action framework as the corresponding execution plan.

Because Unit 42 attributes the majority of initial access and nearly 90% of investigated incidents to identity weaknesses, CSA's Securing Autonomous AI Agents survey report is directly relevant to closing that gap [7]. That survey found that only 18% of organizations are highly confident their current identity systems can effectively manage agent and machine identities, that just 21% maintain a real-time inventory of active agents, and that most enterprises still rely on static API keys and shared service accounts for authentication — the same categories of excessive, poorly governed access that Unit 42's cloud-identity analysis found in 99% of the 680,000 identities it examined. Read together, the two reports support this note's assessment that identity governance, not endpoint or network hardening, is the highest-leverage area for reducing the exposure window Unit 42 describes.

Finally, CSA's AI Controls Matrix (AICM) v1.1 provides the control-level structure for operationalizing these findings, particularly its Threat and Vulnerability Management domain, which addresses continuous vulnerability triage and accelerated patching, and its Identity and Access Management domain, which addresses the excessive-permission and credential-governance failures Unit 42 identifies as enabling the majority of breaches [8]. Organizations using AICM as a governance baseline should treat this report's identity and patch-latency findings as concrete evidence to prioritize control implementation in those two domains ahead of others.

© 2026 Cloud Security Alliance. AI-assisted Rapid Research.

References

[1] Unit 42. "AI, Automation and Attacks: Unpacking the Unit 42 2026 Global Incident Response Report." Palo Alto Networks, July 2026.

[2] Palo Alto Networks. "2026 Unit 42 Global Incident Response Report – Attacks Now 4x Faster." Palo Alto Networks Blog, February 2026.

[3] Palo Alto Networks. "2026 Unit 42 Global Incident Response Report." Palo Alto Networks, February 2026.

[4] RH-ISAC. "2026 Unit 42 Global Incident Response Report." RH-ISAC, February 2026.

[5] BleepingComputer. "Hackers Scan for Vulnerabilities Within 15 Minutes of Disclosure." BleepingComputer, 2022.

[6] Cloud Security Alliance. "The 'AI Vulnerability Storm': Building a 'Mythos-ready' Security Program." CSA CISO Community, May 2026.

[7] Cloud Security Alliance. "Securing Autonomous AI Agents." CSA Survey Report, February 2026.

[8] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." CSA, 2026.

[9] Palo Alto Networks. "Unit 42 Report: AI and Attack Surface Complexity Fuel Majority of Breaches." Palo Alto Networks Press Release, February 17, 2026.