WIZ

The Crying Out Cloud

CHRONICLES

Latest Vulnerabilities & Threats Uncovered by Wiz Research

Issue Vol.2 JAN 2026 $4.00

Shai-Hulud Strikes Twice: npm Supply-Chain Worm Infects Thousands of Repositories with Data-Stealing Malware

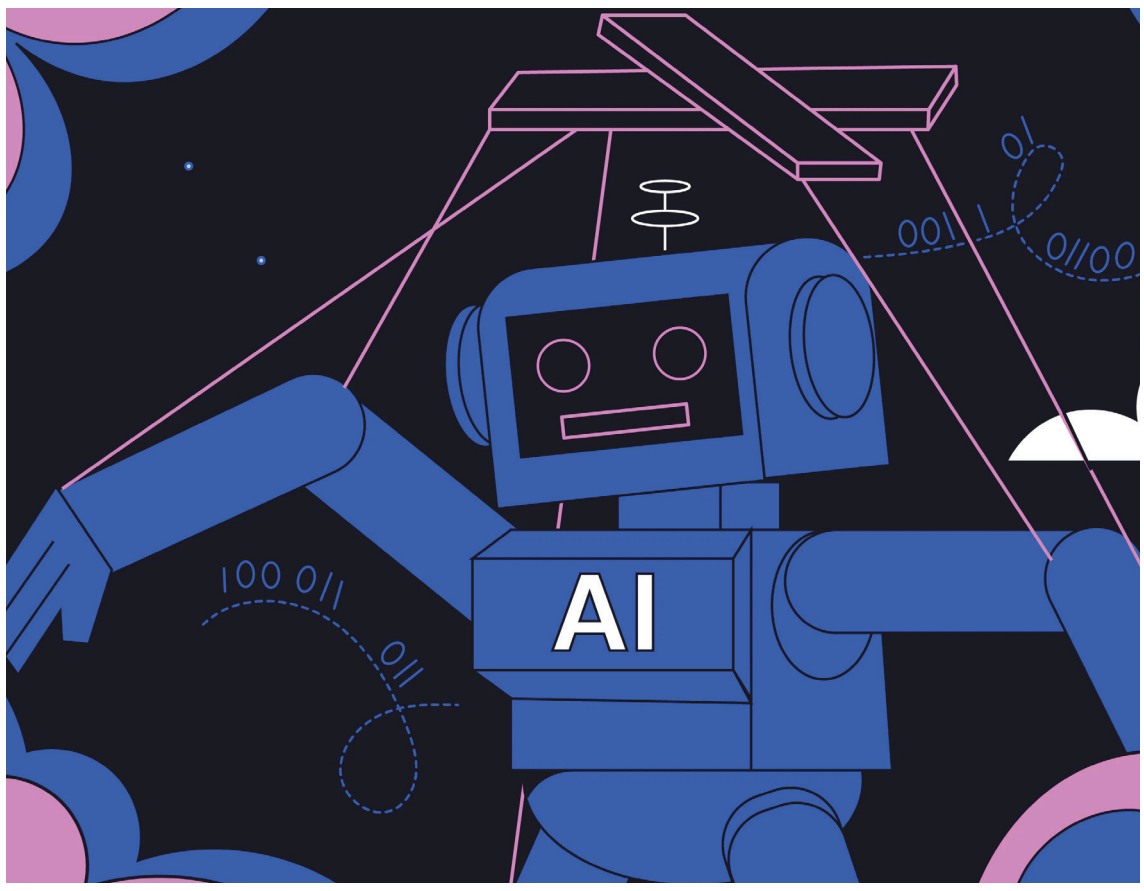
Merav Bar, Gili Tikochinski, Barak Sharoni, Hila Ramati

Wiz covered "Shai-Hulud," a worm-like supply chain attack that infiltrated the npm ecosystem by publishing malicious versions of over 100 packages. Once installed, these packages harvested GitHub and GitLab credentials from developer environments and used them to automatically publish further malicious packages under compromised accounts. This design gave the campaign autonomous propagation capabilities.

Infected packages also exfiltrated SSH keys, environment variables, and cloud provider credentials before continuing their spread. Because npm packages often serve as foundational dependencies across entire organizations, a single infected machine could poison a company's entire development pipeline. Multiple high-profile projects unknowingly integrated some of the malicious components before the attack was discovered. The coordinated cleanup required widespread credential rotation, package takedowns, and registry-wide scanning to ensure no further backdoored versions remained.

Exposure Report: 65% of Leading AI Companies Found with Verified Secret Leaks

November 10, 2025 — Shay Berkovich, Rami McCarthy

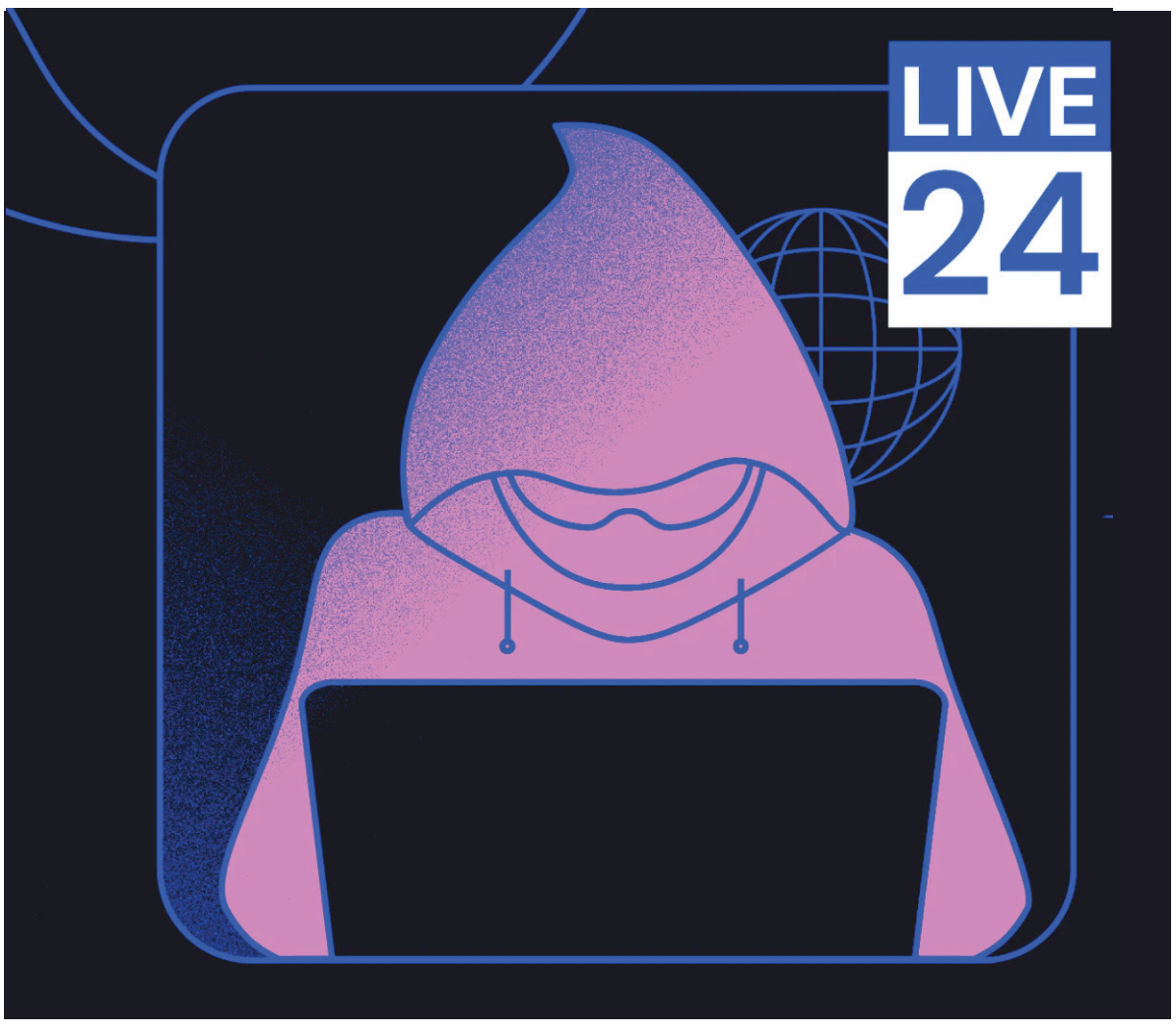


Wiz researchers revealed that 65% of companies featured on the Forbes AI 50 list were leaking sensitive credentials on GitHub, including API keys, authentication tokens, and cloud access secrets. The research found that many exposed secrets offered direct access to internal staging environments, vector databases, and even full development clusters — all without any sandboxing or rate-limiting.

The investigation found that one-third of the leaked secrets were high-impact, enabling access to private repositories, SaaS services, and internal developer tooling. Even more concerning: many companies had leaked similar secrets repeatedly over multiple months, suggesting long-term operational gaps in secret hygiene practices. The problem was worsened by rapid hiring and distributed development workflows typical in the AI sector, leading to inconsistent security processes across teams.

Response to disclosures was mixed. While some firms acted quickly to rotate keys and close exposures, nearly half failed to remediate within two weeks, and several never responded at all. Wiz recommends mandatory secret scanning in CI pipelines, organization-wide GitHub secret-detection tooling, and strict governance for developer tokens — especially in fast-moving AI companies ."

Critical Vulnerability in React – CVE-2025-55182



December 3, 2025 – Gili Tikochinski, Merav Bar, Danielle Aminov

A critical React Server Components (RSC) vulnerability, CVE-2025-55182 ("React-2Shell"), allows unauthenticated RCE via a single crafted HTTP request. The flaw stems from unsafe deserialization in the react-server package and affects default React 19 and Next.js installations.

Wiz data shows 39% of cloud environments run vulnerable React/Next.js apps, many exposed publicly. Attackers are already exploiting the bug for credential harvesting and cryptomining.

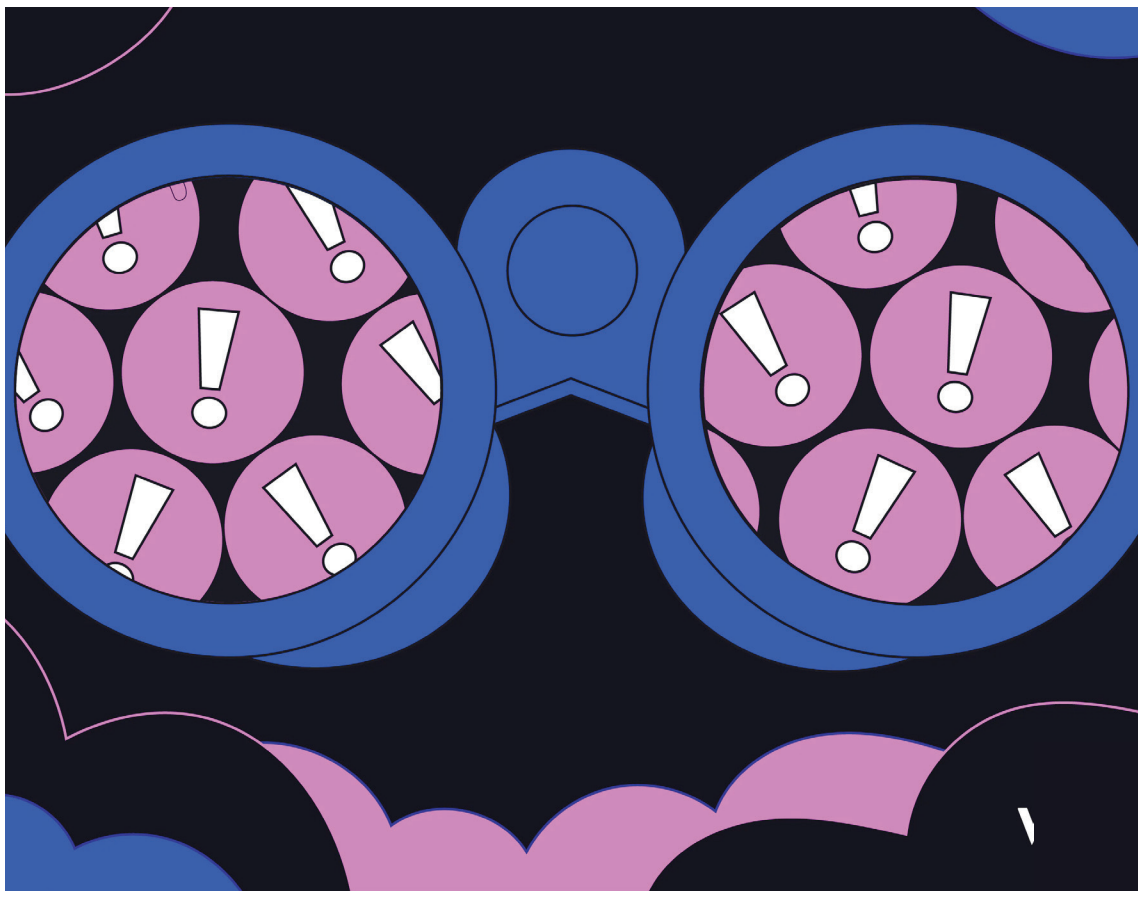
Patched versions include react-server-dom-* 19.0.1, 19.1.2, 19.2.1 and the latest stable Next.js releases. Organizations should upgrade immediately and monitor for suspicious shells, IMDS access, and mining activity.

3 Recent OAuth-Attack TTPs – And How to Detect Them

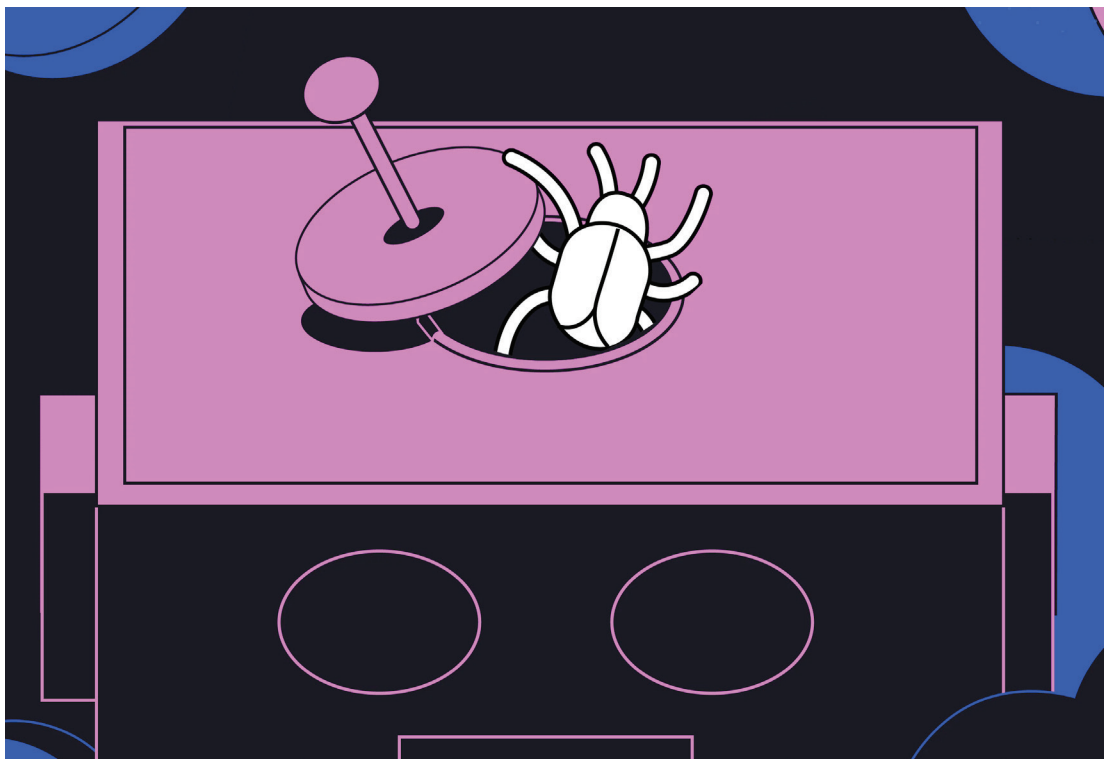
November 27, 2025 - Sapir Federovsky

Wiz researchers highlight three OAuth attack techniques increasingly used to bypass MFA: device-code phishing, ROPC abuse, and token-based persistence through device registration and Windows Hello for Business. These attacks succeed because many tenants still permit weak or legacy authentication flows. Wiz telemetry shows that Conditional Access blocks only 0.3% of device-code attempts and 0.2% of ROPC logins—leaving most environments exposed.

Using Entra ID logs, defenders can detect these attacks by correlating device-code sign-ins, flagging ROPC events, and identifying suspicious device-registration activity. Wiz provides KQL queries to operationalize these detections.



RediShell: Critical Remote Code Execution Vulnerability (CVE-2025-49844) in Redis, 10 CVSS score



October 6, 2025 — Benny Isaacs, Nir Brakha

Wiz uncovered a critical remote code execution vulnerability in Redis — a memory-corruption flaw introduced in 2012 and hiding in plain sight for over a decade. The vulnerability, CVE-2025-49844, allows attackers with authenticated access to craft a malicious Lua script that escapes the scripting sandbox and executes arbitrary native code on the Redis host. Redis, used by approximately 75% of cloud environments, is typically deployed in highly privileged positions inside cloud architectures, making the implications severe.

The bug, nicknamed "RediShell, stems from a use-after-free condition inside Redis Lua stack handling. Despite Redis being widely regarded as a simple and secure data store, its built-in scripting engine dramatically expands the attack surface when not isolated or gated properly.

The research highlights how many Redis instances are still deployed without authentication, or are publicly accessible due to DevOps misconfigurations. Even with authentication enabled, the vulnerability still allows authenticated attackers to escalate privileges. Redis maintainers have released a patch, and Wiz urges organizations to disable Lua if not required, restrict network exposure, and enforce strong authentication policies.

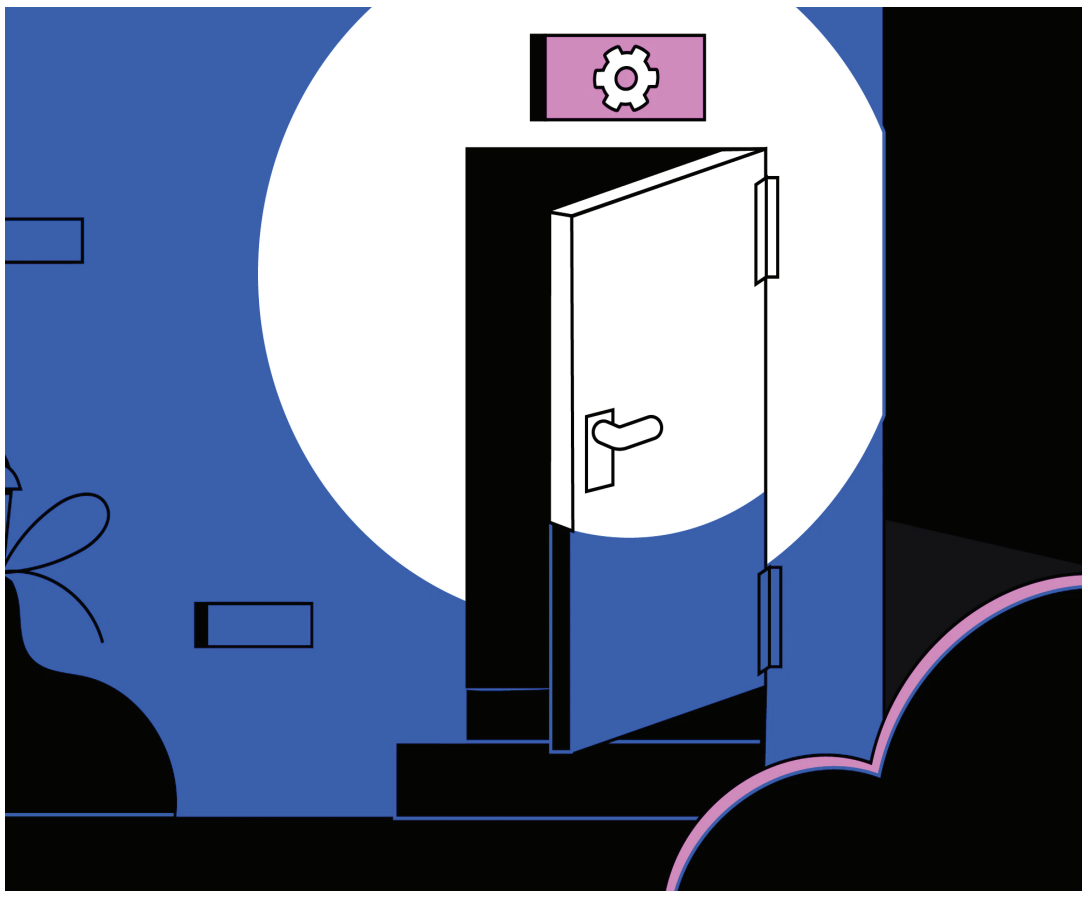
Supply Chain Risk in VS Code Extension Marketplaces

October 15, 2025 – Rami McCarthy

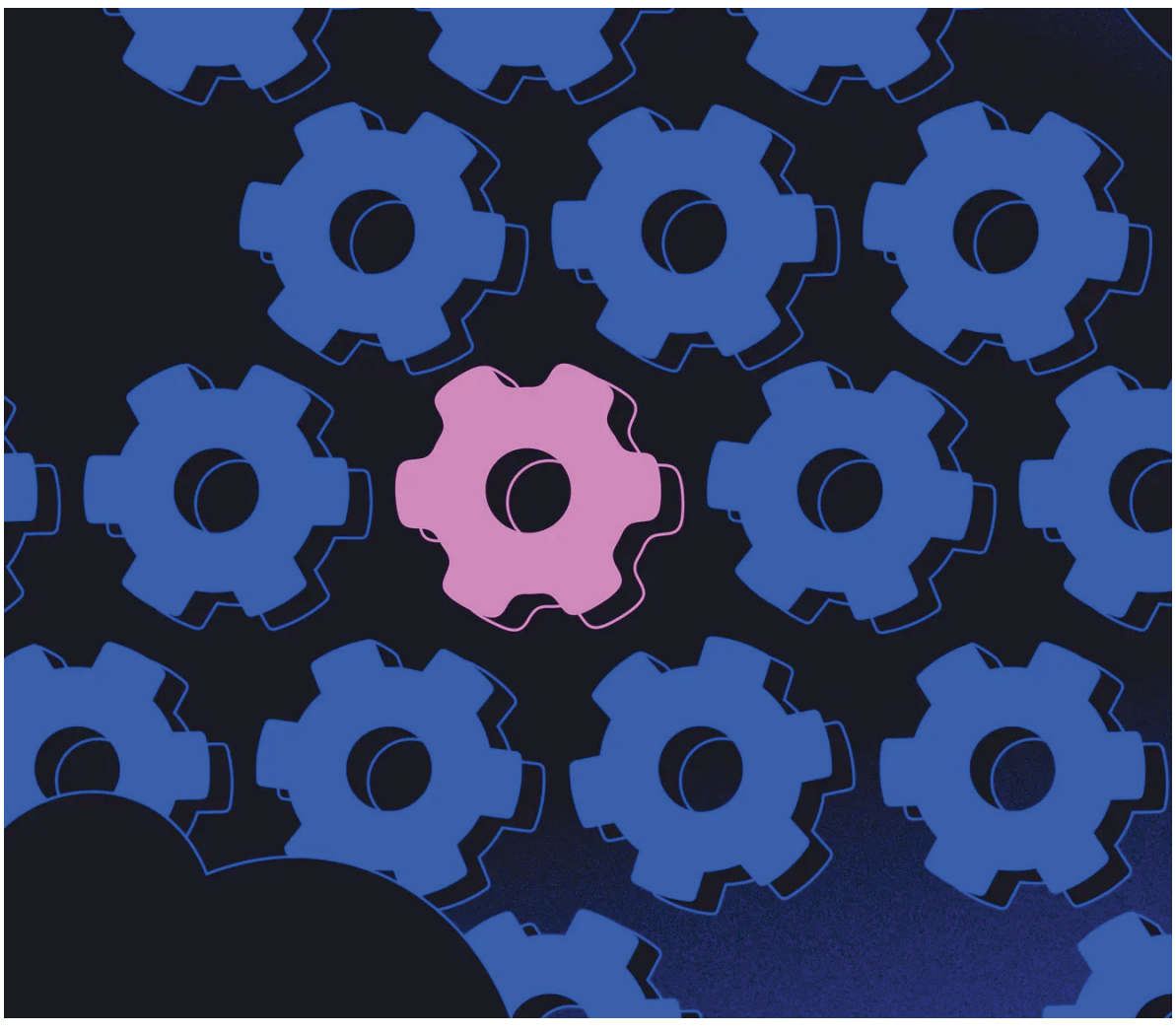
Wiz researchers analyzed the Visual Studio Code and Open VSX extension marketplaces and discovered more than 550 hard-coded secrets across 500+ extensions, including OAuth tokens, publishing credentials, and API keys that could be used to push updates. This exposed a significant supply-chain risk because VS Code installs and updates extensions automatically — meaning a single leaked token could allow an attacker to distribute malicious updates to thousands or even millions of users.

Several leaked tokens belonged to maintainers of highly popular extensions, some with 100,000 installations, giving attackers potential access to enormous downstream impact. The lack of enforced secret scanning across extension ecosystems allowed these defects to propagate unnoticed for months. Stolen tokens could silently distribute credential stealers, backdoors, or dependency-poisoning payloads.

Following coordinated disclosure, Microsoft and other ecosystem maintainers implemented enhanced controls, including secret scanning for extensions, automated token invalidation, and enforced token expiry. Wiz recommends that enterprises review extension allow-lists, disable auto-updates for high-privilege environments, and require developers to use isolated, short-lived publishing tokens to reduce supply-chain exposure.



IMDS Anomaly Hunting: Finding a Zero-Day Through BEHAVIORAL DETECTION



September, 2025 – Hila Ramati, Gili Tikochinski

Wiz researchers revealed how monitoring anomalous access patterns to the cloud Instance Metadata Service (IMDS) led to the discovery of a previously unknown zero-day vulnerability exploited in the wild. Because IMDS provides temporary credentials to compute workloads, unauthorized access often indicates SSRF attacks, privilege escalation attempts, or misconfigured services.

By modeling large-scale patterns of "normal" IMDS behavior across cloud environments, the team identified rare and suspicious signals — including unexpected binaries querying metadata, requests from nonstandard user agents, and IMDS calls occurring immediately after malformed HTTP traffic. These anomalies revealed active exploitation of a real-world web service zero-day, allowing attackers to extract credentials and pivot deeper into the victim's cloud account.

This research demonstrates why behavioral detection outperforms signature-based approaches in modern cloud environments, where ephemeral workloads and constantly changing infrastructure make static indicators unreliable. Recommended mitigations include enforcing IMDSv2, restricting metadata access at the firewall level, logging all IMDS queries, and integrating anomaly detection into cloud security programs.

Soco404: Multiplatform Cryptomining Campaign Hides in Fake Error Pages

July 23, 2025 — Maor Dokhanian, Shahar Dorfman & Avigayil Mechtinger

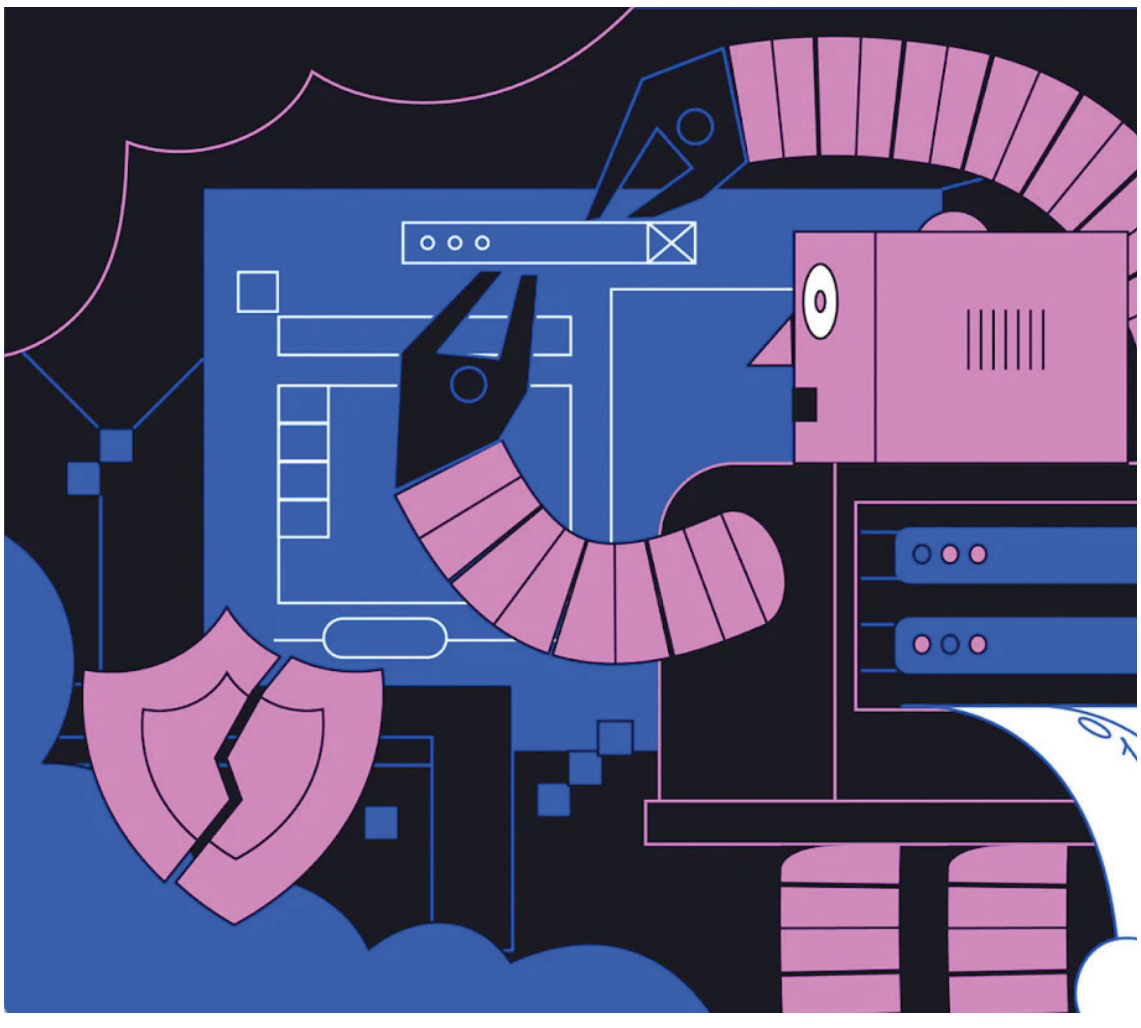
Wiz Research has identified a new cryptomining campaign dubbed Soco404, notable for its stealthy, cross-platform tactics. Attackers register domains that display fake 404 error pages while secretly embedding malicious payloads directly into the HTML. This approach misleads users and bypasses security controls that focus on more obvious threat patterns.

The campaign infrastructure spans three clusters: deceptive "404 domains," crypto-scam websites posing as trading platforms, and compromised legitimate servers (e.g., an abused Korean transportation site running vulnerable Apache Tomcat). Attackers deliver payloads using tools such as curl, wget, certutil, and PowerShell, depending on the platform. On Linux, they establish persistence through cron jobs and shell-file injections; on Windows, they create malicious services.

The malware communicates internally using local sockets and mimics critical system processes (such as sd-pam, cpuhp, or conhost.exe) to evade detection. Soco404 represents an agile, multi-faceted threat that combines cryptojacking, social engineering, and infrastructure abuse. Organizations should monitor for unusual 404 traffic, secure web servers, and conduct threat hunting focused on error-page anomalies.

SharePoint Vulnerabilities

(CVE-2025-53770 & CVE-2025-53771): Everything You Need to Know



July 21, 2025 — Hila Ramati

Microsoft recently issued urgent guidance on two actively exploited zero-day vulnerabilities in on-premises SharePoint servers: CVE-2025-53770 (an unsafe deserialization RCE, CVSS 9.8) and CVE-2025-53771 (a header-spoofing authentication bypass, CVSS 6.3). Together, these vulnerabilities are being used in an exploit chain known as ToolShell, in which the spoofing flaw enables unauthenticated access, followed by remote code execution. These issues bypass earlier patches for CVE-2025-49704 and CVE-2025-49706, prompting Microsoft to release emergency updates between July 18–21, 2025. CISA has also added CVE-2025-53770 to its Known Exploited Vulnerabilities (KEV) catalog.
Affected environments include self-managed SharePoint servers—whether running on physical hardware or hosted in public cloud platforms such as Azure, AWS, or GCP. SharePoint Online (Microsoft 365) remains unaffected. Wiz reports that at the time of disclosure, roughly 9% of cloud environments contained vulnerable SharePoint instances; remediation efforts have since reduced this to around 5%.

ToolShell exploitation began around July 18, with proof-of-concept chains circulating as early as May. Although Microsoft addressed the original vulnerabilities in its July Patch Tuesday release, threat actors quickly identified new bypasses. Organizations should apply emergency updates, audit their SharePoint exposure, and conduct threat hunting to identify potential compromise.

Exposed JDWP Exploited in the Wild:

WHAT HAPPENS WHEN DEBUG PORTS ARE LEFT OPEN

July 2, 2025 – Yaara Shriki & Gili Tikochinski

Wiz Research captured an in-the-wild exploitation attempt against a honeypot server running TeamCity. The attacker targeted an exposed Java Debug Wire Protocol (JDWP) interface, turning a misconfigured debug port into a direct vector for remote code execution. Within hours of the honeypot coming online, the attacker deployed a stealthy cryptomining payload and established persistent access on the system.

JDWP is a Java debugging interface that enables remote inspection of a running application—including access to threads, memory, and execution flow. When exposed without proper access controls, JDWP provides attackers with the ability to issue arbitrary commands inside the Java process. In Wiz's measurements, more than 6,000 unique IP addresses scanned for exposed JDWP endpoints over a 90-day period, highlighting how aggressively attackers search for this misconfiguration.
Once inside, the attacker used JDWP commands to interact with the JVM and invoked Runtime.exec() to download and execute a malicious script named logservice.sh. The script deployed a modified XMRig miner with a hard-coded configuration, communicated through mining-pool proxies to obscure wallet details, and implemented persistence mechanisms designed to survive reboots and evade detection.

Organizations should disable JDWP in production environments and ensure it is never exposed externally. When JDWP must be used, strict network restrictions and continuous monitoring are essential to detect and prevent exploitation attempts.

DevOps Tools Targeted for Cryptojacking

Campaign "JINX-0132"

June 2, 2025 – Gili Tikochinski, Danielle Aminov & Merav Bar

Wiz Threat Research uncovered a cryptojacking campaign dubbed JINX-0132 that targets publicly accessible and misconfigured DevOps applications — including Nomad, Consul, Docker, and Gitea — by abusing default settings and known vulnerabilities to deploy miners.

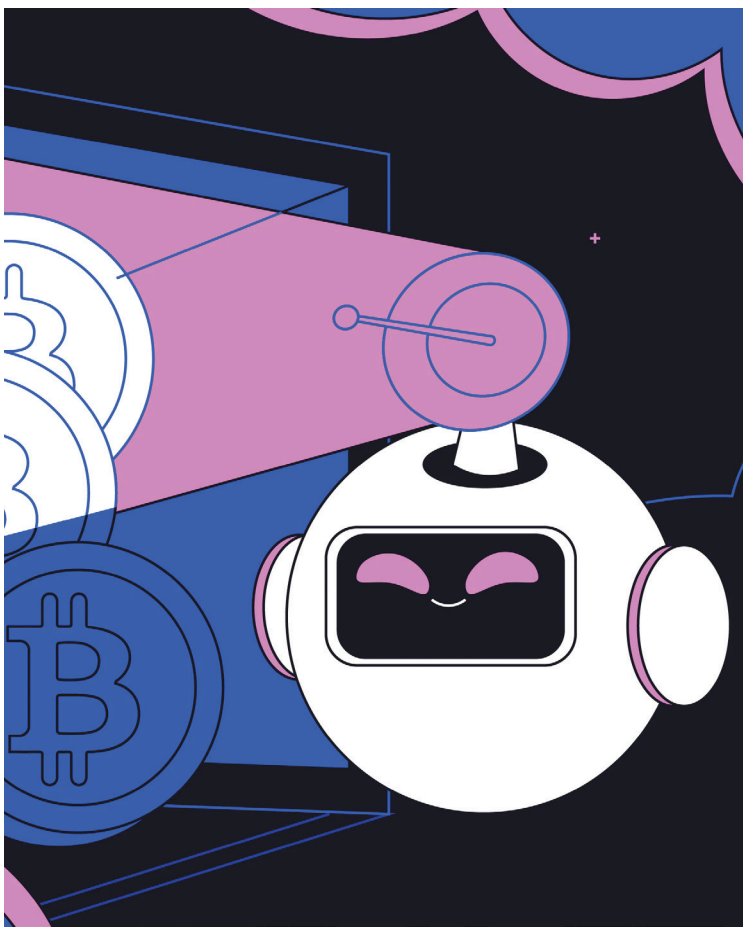
For Nomad, the team exploited unsecured default APIs that allow unauthenticated job submissions. On exposed Nomad servers, attackers submitted malicious jobs retrieving and executing the official XMRig miner binary from GitHub — with no need for attacker-controlled infrastructure or custom malware.

In cases involving Consul, attackers leveraged unsecured HTTP APIs to register malicious health checks. Because these health checks execute on agents, this allowed remote code execution and mining deployment across the infrastructure. For Docker, publicly exposed Engine APIs (e.g. tcp://0.0.0.0:2375) were abused to spawn containers with host-level privileges — enabling attackers to launch containers that mine cryptocurrency or mount the host filesystem.

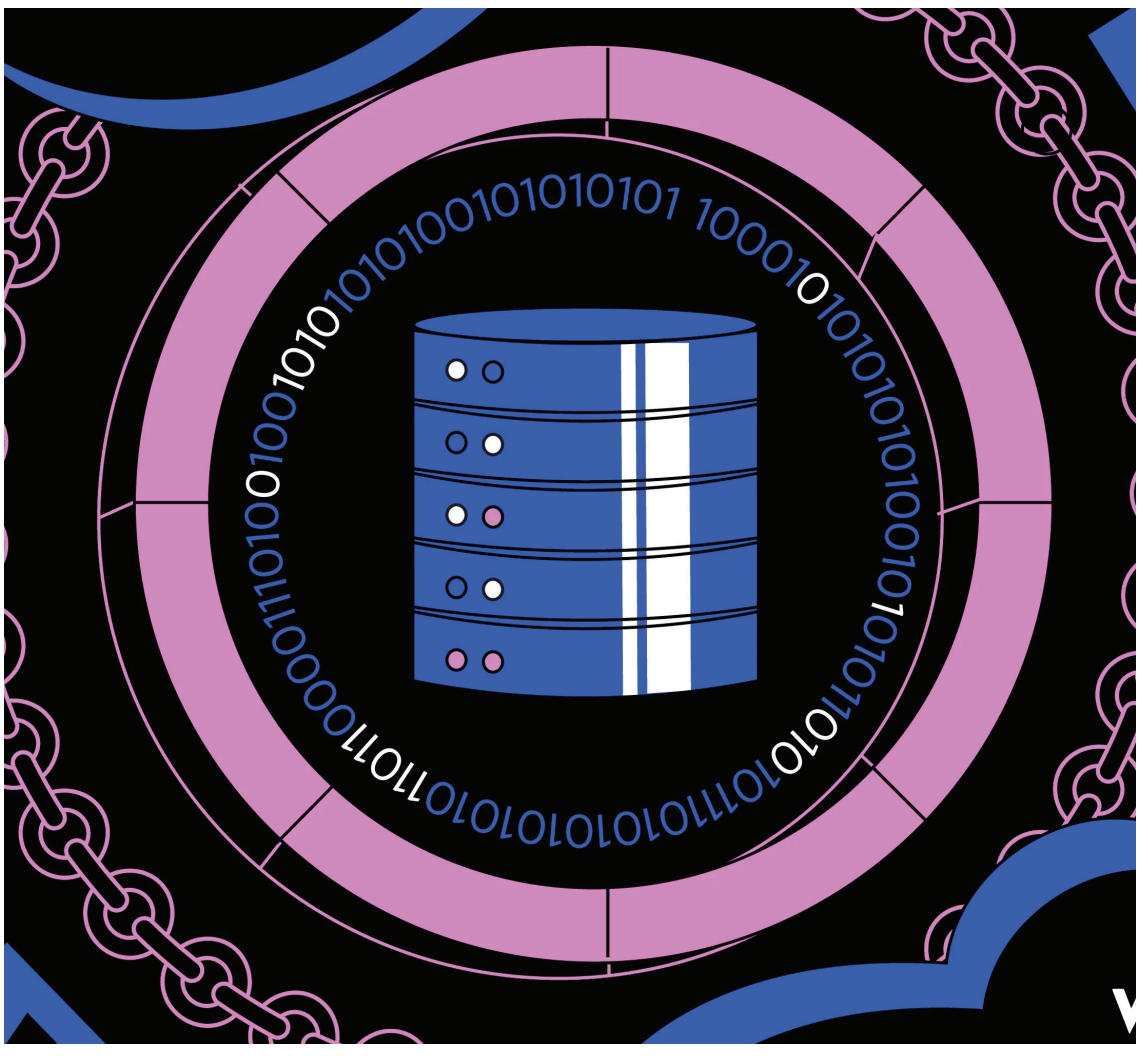
Gitea deployments were also at risk under several scenarios: outdated versions with known remote-code-execution vulnerabilities (e.g., CVE-2020-14144, vulnerable 1.4.0), insecure hook settings or unlocked installation pages. Publicly exposed Gitea instances could thus provide an initial foothold for mining campaigns or further exploitation.

According to Wiz's data, roughly 25% of all cloud environments run at least one of the targeted tools; among those, about 5% were exposed to the Internet, and of those exposed, approximately 30% were misconfigured — significantly expanding the potential attack surface.

Because the attacker used standard open-source tools (public XMRig releases) and legitimate infrastructure for payload delivery, traditional signature-based detection and attribution are complicated. To defend against JINX-0132, organizations should restrict API exposure, enforce appropriate access controls or ACLs, keep all services patched, disable unnecessary automation endpoints, and actively monitor for mining or abnormal container/job activity (for example using runtime-behavior tools or anomaly-detection sensors).



Critical Citrix NetScaler ADC Vulnerabilities Exploited in the Wild (CVE-2025-5349, CVE-2025-5777, CVE-2025-6543)



July 6, 2025 – Merav Bar & Amitai Cohen

Three critical vulnerabilities affecting Citrix NetScaler ADC and Gateway have been identified: CVE-2025-5349, CVE-2025-5777, and CVE-2025-6543—with some already weaponized in attacks.

CVE-2025-5777 (CVSS 9.3) is a memory-overread vulnerability triggered by crafted HTTP requests, potentially exposing session tokens and credentials—similar in impact to CitrixBleed.

CVE-2025-5349 (CVSS 8.7) arises from insufficient access controls on management interfaces, risking unauthorized administrative access.

CVE-2025-6543 (CVSS 9.2) is a memory-overflow flaw that may allow remote code execution. Citrix confirmed that CVE-2025-6543 was exploited as a zero-day prior to public disclosure.

According to Wiz data, approximately 3.5% of cloud environments contain vulnerable NetScaler resources. Proof-of-concept code for CVE-2025-5777 appeared on July 3, 2025, and exploitation of CVE-2025-6543 continues in the wild.

Security teams must urgently patch supported versions, upgrade end-of-life builds, terminate active ICA/PCoIP sessions after patching, rotate exposed credentials, and filter logs for non-printable characters that may indicate exploitation attempts.

The Lighter Side of **Cloud Security**

Unscramble these cloud security terms

Easy Level:

1. ARECBH = _ _ _ _ _ _ (Data incident)

2. IRNFMEOUGISDC = _ _ _ _ _ _ _ _ _ _ _ _ _ _ (Common cloud mistake)

Medium Level:

3. NBESUKERTE = _ _ _ _ (Container orchestration)

4. DBLMAA = _ _ _ _ _ _ (AWS serverless)

5. EIVKSCA = _ _ _ _ _ _ (Exploited vulnerability catalog)

Hard Level:

6. UERROTTSZ = _ _ _ _ - _ _ _ _ _ (Zero-trust security model)

7. PLHUCSAPYIN = _ _ _ _ _ _ - _ _ _ _ _ (Attack method)

8. SENAACGTMESERR = _ _ _ _ _ _ _ - _ _ _ _ _ _ _ (Key management)

(Answers: (from left to right): BREACH, MISCONFIGURED, KUBERNETES, LAMBDA, CISA KEV, ZERO-TRUST, SUPPLY-CHAIN, SECRETS-MANAGER)

Which Cloud Security Archetype Are You?

Answer these questions and tally your points:

1. It's 3 AM and your monitoring alerts go off. Your first reaction?

A) Jump out of bed and start investigating immediately (4 points)

B) Check if it's a real alert or just noise first (3 points)

C) Set a reminder to check it in the morning (1 point)

D) Hope someone else handles it (0 points)

2. Your ideal weekend project involves:

A) Building a home lab threat detection system (4 points)

B) Automating something that annoys you at work (3 points)

C) Reading the latest security research papers (2 points)

D) Actually taking a break from computers (0 points)

3. When a new vulnerability is announced:

A) You scan your entire infrastructure within hours (4 points)

B) You check if your systems are affected and patch accordingly (3 points)

C) You wait for your tools to flag it automatically (1 point)

D) You wait for IT to send an email about it (0 points)

4. Your approach to security documentation is:

A) Everything must be documented in real-time (4 points)

B) Document the important stuff, automate the rest (3 points)

C) Follow the company templates and standards (2 points)

D) Documentation is someone else's job (0 points)

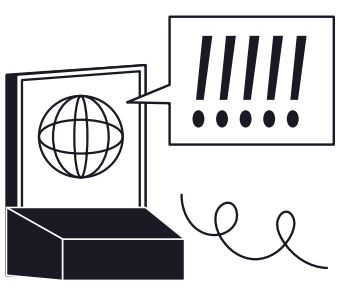
5. During a security incident:

A) You dive deep into logs to trace the attack path (4 points)

B) You coordinate teams and manage the response (3 points)

C) You follow the established playbook step by step (2 points)

D) You wait for instructions from your manager (0 points)



Results:

16-20 points:
The Threat Hunter
You live and breathe security. Anomalies in network traffic wake you up at night, and you genuinely enjoy hunting down IOCs. Your colleagues think you're slightly paranoid, but they're secretly grateful when you catch threats before they become incidents.

11-15 points:
The Security Engineer
You balance proactive security with practical engineering. You automate what you can, investigate what matters, and know when to escalate. You're the person others turn to when they need both technical depth and common sense.

6-10 points:
The Compliance Professional You bring order to chaos through frameworks and processes. You might not write custom detection rules, but you ensure everything follows best practices and regulatory requirements. Your documentation game is unmatched.

0-5 points:
The Security Tourist
Security happens around you rather than through you. You're probably great at your main job, but when it comes to security, you prefer to let the experts handle it while you focus on other things.

Did You Know? Cloud Security Facts

Surprising statistics and esoteric cloud trivia

1. **Only 30% of global workloads** currently run in the cloud, meaning **70% of enterprise** computing still happens on-premises. Surprisingly, 83% of companies are now planning to move some applications back from cloud to their own servers.

2. The "**cloud computing**" was first used in a business context in 1996, but the concept dates back to the 1960s when computing was predicted to be sold like a utility.

3. **Cloud storage** processes over **100 trillion objects** globally and regularly peaks at millions of requests per second. Yet misconfigured storage buckets are still responsible for 70% of cloud data breaches.

4. **Streaming services** account for 15% of global internet bandwidth usage, all running on cloud infrastructure they don't own. Many companies run entirely without physical data centers.

5. The **average cloud environment** uses **5.2 different cloud platforms**, but only **23%** of organizations have consistent security policies across all of them.

6. **Cloud data centers** span **60+ locations** worldwide, each with different data sovereignty laws. Moving data between regions can accidentally violate multiple international regulations.

7. A single **typo in a cloud security policy** can expose entire systems. The most dangerous mistake? Using "*" (asterisk) instead of specific permissions - one character can grant access to everything.

8. **95% of cloud security failures** are due to customer mistakes, not problems with the cloud providers themselves. Experts predict this will increase to 99% by 2025.

Take a break.

Debug your mind. Smile a little.

Security Haikus

Patch Tuesday comes
Server refuses restart
Technical debt grows

S3 bucket
"Just for testing," they promised
Front page of the news

Zero-day alert
Cold coffee, endless phone calls
Long night lies ahead

MFA works great
Until your phone battery dies
Locked out, tears falling

Researcher Recipe Corner

Danielle's Fresh Pasta Carbonara

(Recipe by Danielle Aminov, Threat Researcher)

For 2 portions - comfort food after a long incident response**
Ingredients:
- Fresh pasta dough (1 cup flour, 1 egg, 2 yolks, salt) – already prepared
- Guanciale (150g), cut into small cubes
- Pecorino Romano (50-60g), finely grated
- 2 egg yolks
- Freshly ground black pepper

Instructions:

1. Prepare the guanciale
- Place diced guanciale in a cold pan, turn to medium heat
- Let the fat render and guanciale crisp up. No oil needed
- Once golden and crispy, turn off heat

2. Make the sauce
- Whisk egg yolks with grated pecorino and plenty of black pepper
- Add a spoonful of guanciale fat for extra flavor. Mix until creamy

3. Cook and combine
- Cook fresh pasta in boiling salted water for 2 minutes (al dente)
- Reserve ½ cup pasta water before draining
- Toss hot pasta with guanciale, add egg mixture and pasta water until glossy
- Serve immediately with extra pecorino and pepper

Alon's Banh Xeo (Vietnamese Crispy Crepes)

(Recipe by Alon Schindel, VP AI & Threat Research)

Makes 4-6 crepes - perfect for sharing after a successful threat hunt
Ingredients:
Batter: 1 cup rice flour, ½ cup coconut milk, ¾ cup water, ½ tsp turmeric, ¼ tsp salt, 2 green onions (sliced)

Filling: 200g shrimp (peeled), 200g pork belly or chicken (sliced), 2 cups bean sprouts, 1 onion (sliced), oil for frying
Serving: Fresh lettuce, herbs (mint, cilantro, basil), dipping sauce (lime juice, fish sauce, sugar, garlic, chili)

Instructions:
1. Make the batter
- Whisk rice flour, coconut milk, water, turmeric, and salt until smooth
- Add green onions and rest 30 minutes

2. Cook the crepes
- Heat large pan over high heat with 2 tbsp oil
- Add onion (30 seconds), then shrimp and meat (2 minutes)
- Pour ½ cup batter, swirl to coat pan
- Add bean sprouts on one half, cover 2-3 minutes
- Fold in half when edges are crispy and golden

3. Serve
- Wrap pieces in lettuce with fresh herbs and dip in sauce
- The contrast of crispy, creamy, fresh, and tangy is perfection

Best enjoyed while discussing AI-powered threat models - or just savoring good food.

Take a break. Solve a puzzle. Laugh a little.

D	6	N	3	G	2	6	Z	V	L	Z	D	0	E	C	8	4	A	L	R	C	V	H
3	Q	I	M	C	A	5	S	V	8	M	4	J	L	I	U	B	G	P	0	K	4	3
5	G	6	5	F	0	P	K	0	E	Y	0	V	M	H	F	M	J	U	0	A	D	4
3	L	X	M	R	V	K	0	7	0	Z	L	G	8	3	F	R	S	9	7	G	0	P
R	I	5	P	3	C	7	R	3	4	0	Y	T	U	4	3	I	G	8	K	E	R	5
1	Y	3	M	G	F	D	S	N	7	5	4	R	M	R	R	G	8	P	L	I	3	P
4	X	R	E	G	2	8	5	A	W	Q	P	V	Q	7	0	9	I	K	7	V	Z	R
L	C	4	5	7	4	C	K	5	M	4	5	H	E	8	V	2	K	Q	T	K	L	4
L	H	W	S	Y	6	F	T	K	Q	8	8	8	0	L	3	X	9	4	3	A	P	Y
2	N	M	S	R	N	U	H	R	U	A	8	C	G	3	R	W	S	W	2	5	V	8
4	0	0	8	C	W	Q	T	J	9	0	J	E	H	3	F	H	6	H	0	5	7	W
7	1	5	9	4	A	U	5	W	3	9	R	P	D	D	L	8	1	5	T	D	H	U
1	7	N	9	N	0	L	7	U	C	3	X	3	3	D	0	C	3	T	0	M	3	R
0	C	4	Y	N	Y	I	T	8	6	C	8	J	P	9	W	Z	7	M	P	0	3	M
N	3	R	W	4	J	5	E	Y	Y	N	C	W	7	S	N	1	K	T	R	9	8	3
L	J	A	X	W	T	5	H	3	L	L	C	0	D	3	C	P	V	N	2	0	R	L
W	N	A	8	3	9	3	3	R	F	R	3	7	F	4	3	5	U	L	U	T	0	7
A	1	P	R	1	V	L	L	3	G	3	3	S	C	4	L	4	7	L	0	N	0	D
H	L	0	C	V	1	Y	4	U	F	G	R	U	4	F	K	M	8	8	G	H	D	0
9	Q	R	Q	K	C	0	H	5	L	L	3	H	5	9	Q	W	4	R	D	Q	K	W
X	5	A	W	0	L	F	R	3	V	O	R	3	6	3	7	N	1	4	9	L	C	N
H	G	J	1	3	F	E	Y	8	M	R	0	P	6	4	D	6	3	7	I	W	4	9
8	E	0	F	L	R	N	U	L	L	D	3	R	3	F	3	R	3	N	C	3	8	S

Find the following words in the puzzle. Words are hidden vertically (up and down), horizontally (left and right), and diagonally (from top-left to bottom-right).

REMOTECODEEXECTION
PRIVILEGEESCALATION
HEAPSPRAY
ZERODAY
NULLDEREFERENCE
USEAFTERFREE
SPECTRE
MELTDOWN
GHOST
HEARTBLEED
SHELLSHOCK
WANNACRY
BUFFEROVERFLOW
STACKMASH
ROPGADGET
SHELLCODE
PAYLOAD
INTEGEROVERFLOW
SQLINJECTION
RANSOMWARE
BACKDOOR
ROOTKIT
DESERIALIZATION