



Cybersecurity skalieren: Wachsende Anforderungen bewältigen und Risiken begegnen

Etienne Bottke, Senior Sales Engineer, CISSP

Security Operations

Angestrebtes Sicherheitslevel

Security Operations

Lücke

Die meisten Firmen stehen hier



BASIS

Passwörter / AD
Patch Management
Backups



PERIMETER

Firewalls
SPAM / Web Filters
WAF / Proxy



VERTEIDIGUNG IN DER TIEFE

Endpoint (NGAV, EDR)
DLP / SSL Inspection
Anti-DDoS / IPS / CASB



IDENTIFIZIEREN



SCHÜTZEN



ERKENNEN



REAGIEREN



WIEDERHERSTELLEN



WIDERSTANDS-FÄHIGKEIT

Proaktiv
Versicherbar
Konform (ISO, TISAX,
KRITIS, NIS2)



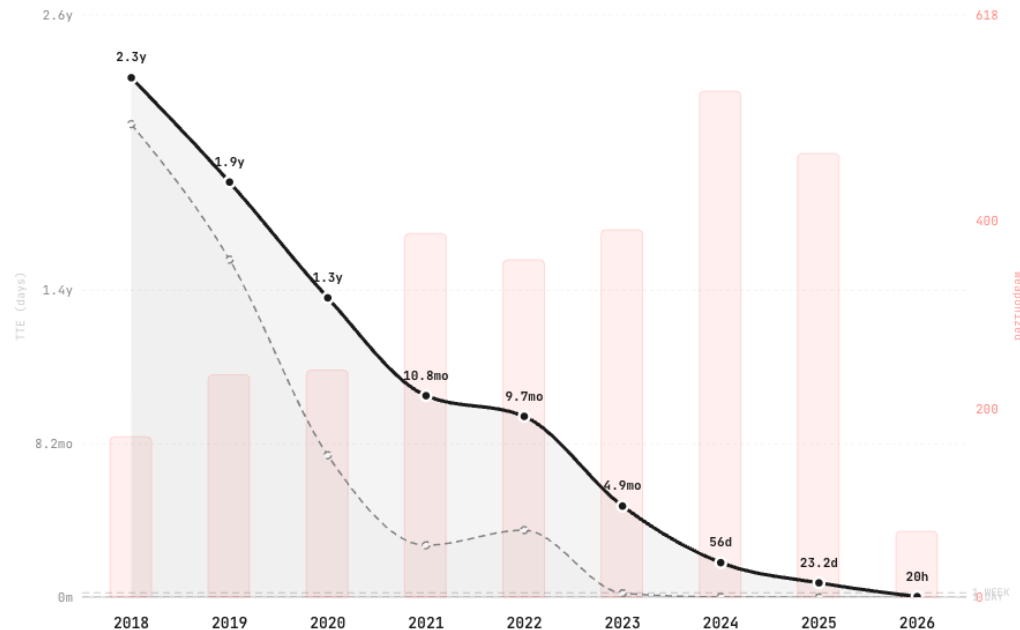
KI zwingt uns immer schneller zu werden

Dies ist kein theoretisches Problem mehr, Verteidiger müssen Schritt-halten

From Vulnerability to Exploitation

TTE (Time-to-Exploit) measures the gap between CVE disclosure and confirmed exploitation

— Mean TTE (10% trimmed, days) - - - Median TTE (days) ■ Weaponized Exploits (count)



Based on 3,530 CVE-exploit pairs from trusted sources (CISA KEV, VulnCheck KEV & XDB)

zerodaycLock.com

AI-Led Remediation Crisis Prompts Hacker Bug Bounties
Discovery used to be the bottleneck for open source bugs, but with automated discovery, which bounties don't fund.

Microsoft's massive Patch Tuesday: It's raining bugs
One CVE under attack, one already disclosed by angry bug hunter, and 163 more

Attackers exploited a spoofing vulnerability in Microsoft SharePoint Server before Redmond issued a fix as part of April's mega Patch Tuesday.

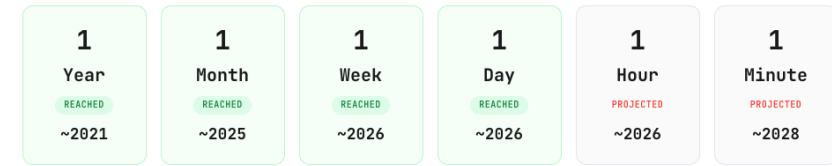
The monthly patch party included a whopping 165 new Microsoft CVEs.

And the bug under active exploitation, CVE-2026-32201, is due to improper input validation in SharePoint that allows an unauthorized attacker to perform spoofing over a network. This could allow someone to view sensitive information and make changes to disclosed information.

"By exploiting this flaw, an attacker can manipulate how information is presented to users, potentially tricking them into trusting malicious content," Mike Walters, president and cofounder of patch management provider Action1, told us, adding that this bug can be abused in phishing attacks, unauthorized data manipulation, or social engineering campaigns that lead to further compromise.

Time-to-Exploit Milestones

When mean time-to-exploit crosses each threshold



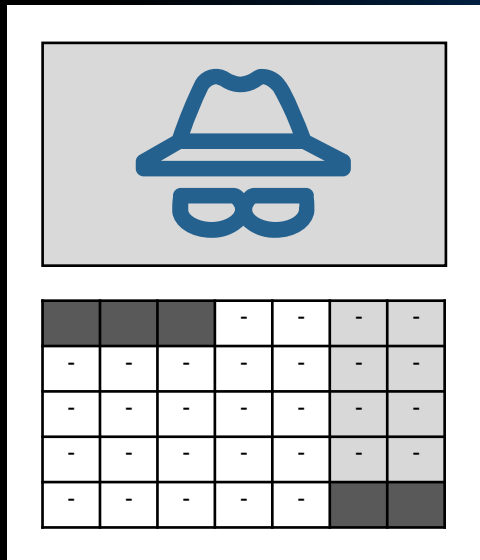
zerodaycLock.com

Maschinen-Geschwindigkeit muss das Ziel sein

Wie schnell sind Sie in Ihren IT-Security Abläufen?

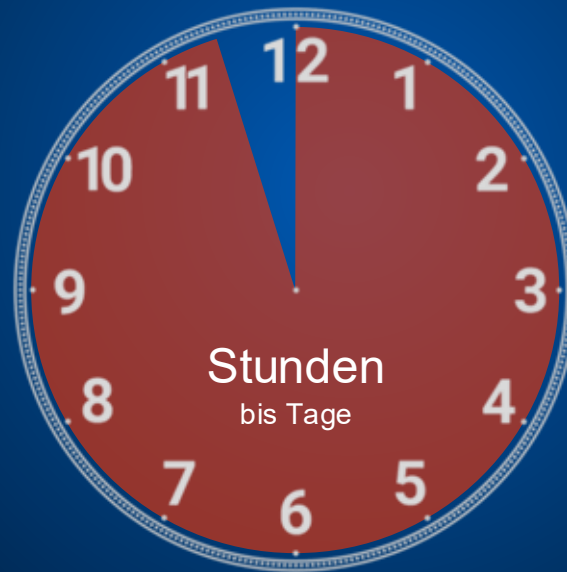
Traditionelle IT-Security

Die IT macht das irgendwie mit



Traditionelles SOC

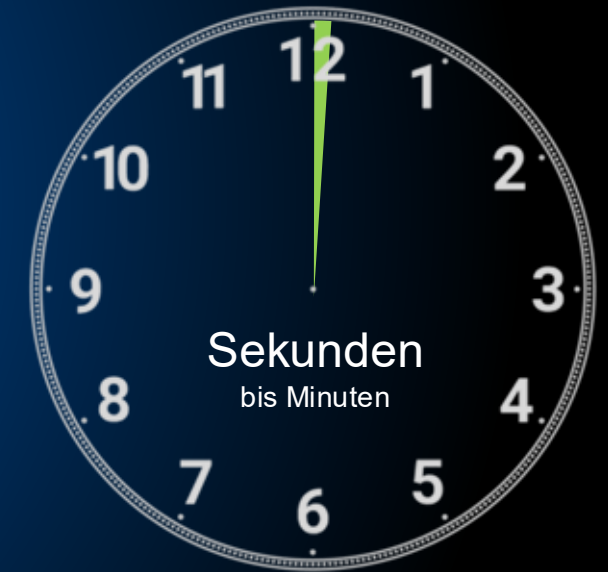
Menschen-geführte Prozesse



Typische SOC Timelines
Alert triage: 10–30 min je Incident
Analyse: 2–4 Stunden
Reaktion: Stunden bis Tage

Aurora Agentic SOC

Agenten-geführtes SOC, Menschen immer in der Prozesskette



Aurora Agentic SOC Timelines
Alert triage: Sekunden bis Minuten
Analyse: Minuten, parallelisiert durch den Swarm of Experts
Reaktion: Minuten bis zum Containment

Typische “Wir machen das Nebenbei”-Timelines*
Durchschnittszeit bis zur Detektion: 181 Tage
Durchschnittszeit bis zur Eindämmung: 60 Tage

* <https://www.ibm.com/reports/data-breach>



Was ist Superintelligence in Cybersecurity?

Die Fähigkeit, sowohl menschliche als auch rein KI-basierte Ansätze zu übertreffen und dabei sichere, zuverlässige und vertrauenswürdige Ergebnisse zu liefern.





Superintelligence Platform

Open Data Pipeline ermöglicht Herstellerunabhängigkeit.

Security Operations Graph Integriert unsere Sicherheitsexpertise in die Datenbasis.

Swarm of Experts deckt alle SOC-Aufgaben ab, während Menschen jederzeit in den Prozess eingebunden bleiben.

Trust Engine stellt sicher, dass alle Ergebnisse genau, zuverlässig und vertrauenswürdig sind.





Aurora Agentic SOC

Agenten geführtes SOC transformiert das Betriebsmodell, sodass es mit Maschinengeschwindigkeit läuft.

Schlüsselfertige Lösung ermöglicht Kunden sofort den ROI der eingebauten Agenten zu realisieren

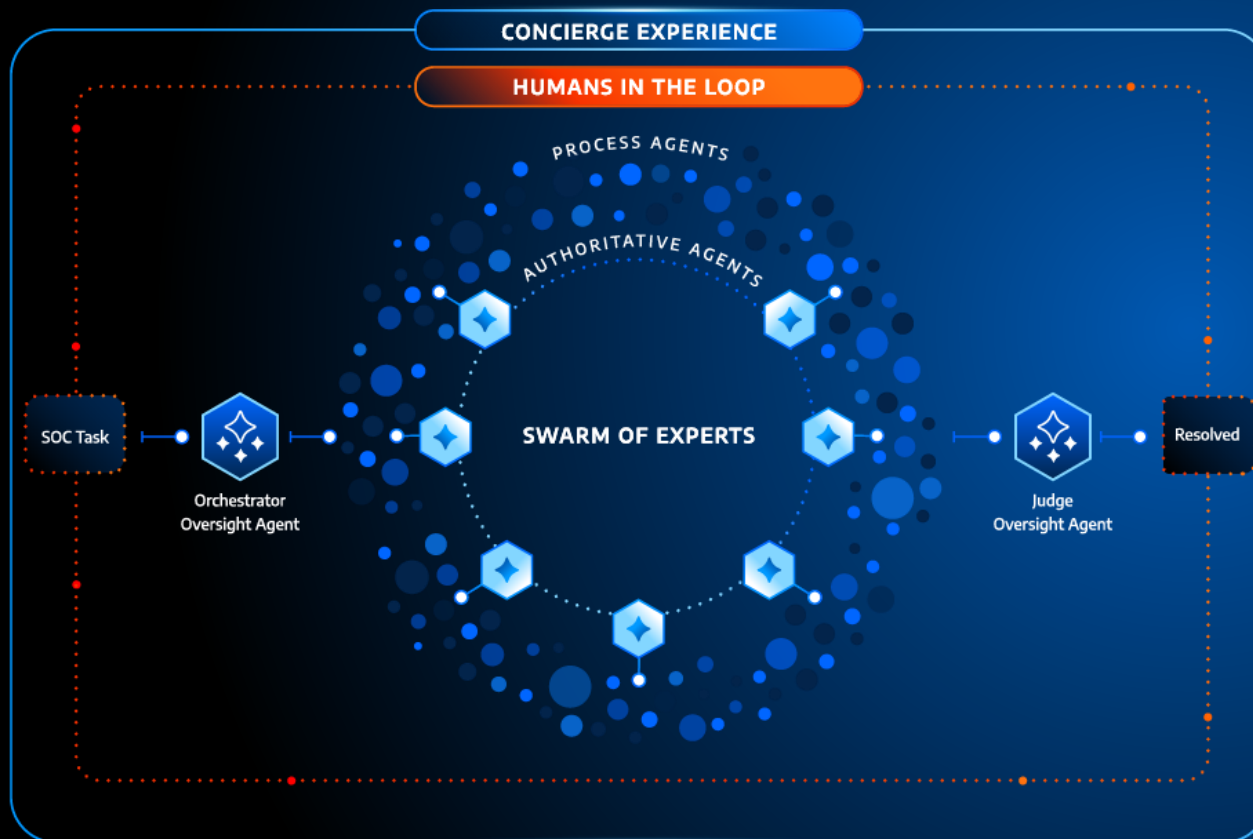
Unterstützt Concierge Integriert den jeweils kundenspezifischen Kontext konsistent in sämtliche Workflows.

Security Journey beschleunigt sich, indem Agenten repetitive Tätigkeiten eliminieren und Teams zu einem proaktiven Arbeitsmodus übergehen.



Wir schützen Sie mit Maschinen-Geschwindigkeit

Unser Swarm of Experts und das Aurora Agentic SOC arbeiten mit maschineller Geschwindigkeit. Der Mensch bleibt immer zur Aufsicht sowie für kritische Entscheidungsfindungen eingebunden.



Der Swarm of Experts wächst kontinuierlich durch neue Agenten und deckt mit maschineller Geschwindigkeit immer mehr SOC-Aufgaben ab.

Arctic Wolf Agent	Aufgabe
Triage Agent	Trennt Signale sofort vom Rauschen und priorisiert, was jetzt relevant ist.
Analyse Agent	Führt mehrstufige, domänenübergreifende Untersuchungen durch.
Response Agent	Steuert Eindämmungs- und Behebungsmaßnahmen schnell und innerhalb klar definierter Leitplanken
Threat Hunting Agent	Sucht proaktiv nach verborgenen Angreifern
Threat Intelligence Agent	Übersetzt globale Risiken in kundenspezifische Risiken
Detection Engineering Agent	Passt Erkennungen fortlaufend an die sich wandelnde Bedrohungslage an
Kontext Agent	Berücksichtigt durchgängig geschäftliche, technische und organisatorische Rahmenbedingungen
zukünftige Agenten	Kontinuierliche Erweiterung der Funktionalität durch neue Agenten



Vielen Dank

ETIENNE BOTTKE

