E-BOOK

A TECHNICAL GUIDE FOR SECURITY PRACTITIONERS

Threat Actor Intelligence & Vulnerability Prioritization

Six major APT groups. 67 actively exploited CVEs. A technical framework for replacing CVSS-driven triage with threat intelligence–driven vulnerability prioritization.

21,500	3%	85%
CVEs disclosed in H1 2025 alone	Represent imminent risk to the enterprise	Of exploited CVEs rated Medium or Low

EXECUTIVE SUMMARY

The Volume Problem Has a Prioritization Answer

Modern vulnerability management faces a fundamental challenge: over **21,500** CVEs were disclosed in H1 2025, yet research shows only 3% represent imminent risk to enterprise environments. Traditional CVSS-based prioritization fails because 85% of actively exploited vulnerabilities are rated Medium or Low severity.

This guide examines six major threat actor groups responsible for the majority of current enterprise breaches, analyzes the 67 CVEs they actively exploit, and provides a technical framework for implementing threat intelligence–driven vulnerability prioritization.

Six APT groups

Six threat actor groups are responsible for most high-impact enterprise breaches across 2024–2025.

67 exploited CVEs

67 unique CVEs actively exploited — many rated Medium or Low despite active use in campaigns.

Edge-first vectors

Edge devices, zero-days, and supply chain attacks are the primary vectors across all actor groups.

Risk-based triage

Threat intelligence integration enables risk-based prioritization that focuses remediation on imminent threats.

KNOW YOUR ADVERSARIES

Six Threat Actors Dominate the Landscape

Understanding who your adversaries are and how they operate is fundamental to proactive defense. Six groups account for the majority of high-impact breaches — and the CVEs they actively exploit.

APT29 Cozy Bear

Russian state-sponsored

20 CVES

Targets: Government, defense, energy.

TTPs: Zero-day exploitation, LOLBins, sophisticated persistence.

APT41

Chinese dual-purpose · espionage + financial

16 CVES

Targets: Healthcare, telecom, high-tech.

TTPs: Supply chain attacks, Log4Shell exploitation.

Volt Typhoon

Chinese infrastructure-focused

8 CVES

Targets: Critical infrastructure, utilities.

TTPs: Living off the land, edge device compromise.

Clop TA505

Ransomware operator

8 CVES

Targets: Mass exploitation via file transfer apps.

TTPs: Zero-day access, double extortion, MOVEit campaign.

Silk Typhoon APT27

Chinese supply chain specialist

9 CVES

Targets: IT service providers, MSPs.

TTPs: ProxyLogon, downstream customer access.

UNC5174

Initial access broker

6 CVES

Targets: High-value enterprises.

TTPs: Rapid exploitation, access monetization to ransomware groups.

COMMON TTP PATTERNS

Shared Tactics Across the Threat Landscape

Each group has unique priorities, but common tactical patterns emerge — letting security teams build defenses that address multiple threat actors simultaneously.

100%

Living Off the Land

PowerShell, WMI, PsExec and legitimate admin tools used to evade detection.

83%

Edge Device Exploitation

VPN concentrators, firewalls, load balancers and network management tools targeted for persistent access outside detection zones.

83%

Rapid Weaponization

35% of exploited vulnerabilities are hit within 48 hours of disclosure.

67%

Supply Chain Attacks

Software vendors and MSPs compromised to reach downstream customers.

50%

Zero-Day Access

Both state-sponsored and financial actors now hold zero-day capabilities.

> **Critical insight:** zero-day capability is no longer exclusive to nation-states — Clop demonstrates financially motivated actors now have access. And Volt Typhoon's critical-infrastructure targeting signals pre-positioning for potential future disruption.

ATTACK VECTOR ANALYSIS

Attack Vector Preference Matrix

Which vectors each group favors — a map for prioritizing defensive effort against multiple actors at once.

ATTACK VECTOR	APT29	APT41	VOLT	SILK	CLOP	UNC5174
Edge Devices (VPN / Firewall)	●	●	●	●	○	●
Enterprise Applications	●	●	○	●	●	●
Cloud Platforms	●	●	○	●	○	○
Supply Chain	●	●	○	●	○	●
Zero-Day Capability	●	●	○	○	●	○
Critical Infrastructure	○	○	●	○	○	○

● Actively exploits vector ○ Not a primary vector

Persistent Access

Edge devices provide footholds outside traditional endpoint detection coverage.

Credential Harvesting

VPN and authentication systems process domain credentials enabling lateral movement.

Network Visibility

Compromised network devices reveal traffic and internal topology.

Patch Lag

Edge devices receive slower patch deployment than traditional IT assets.

EXPLOITED IN THE WILD

Actively Exploited CVEs to Prioritize Now

If these exist in your environment, they demand immediate remediation — regardless of CVSS score.

CVE	PRODUCT	CVSS	THREAT ACTOR
CVE-2025-61882	Oracle E-Business Suite	Zero-day	Clop, ShinyHunters, LAPSUS$
CVE-2023-42793	JetBrains TeamCity	9.8	APT29
CVE-2023-4966	Citrix NetScaler	9.4	APT29 — 'Citrix Bleed'
CVE-2021-44228	Apache Log4j	10.0	APT41, multiple actors
CVE-2018-13379	Fortinet FortiOS	7.5	APT29 — 6 years old
CVE-2023-34362	MOVEit Transfer	9.8	Clop — 2,500+ orgs hit
CVE-2024-3400	Palo Alto PAN-OS	10.0	Silk Typhoon
CVE-2025-11833	WordPress Post SMTP	6.5	Multiple actors, Nov 2025

CVSS scores do not predict exploitation. Attackers deliberately target lower-severity vulnerabilities because defenders aren't patching them — CVE-2018-13379 (7.5) has been exploited for 6+ years, and CVE-2025-11833 (6.5) is actively exploited despite a "Medium" rating.

WHY TRADITIONAL VM FAILS

Volume Overload

15,000–25,000 new vulnerabilities per quarter in typical enterprises.

Misaligned Risk

85% of exploited vulnerabilities are rated Medium or Low severity.

No Context

CVSS ignores active exploitation, asset criticality, compensating controls and business impact.

THE PRIORITIZATION MODEL

A Threat-Driven P0–P3 Framework

Replace CVSS-only triage with tiers built on active exploitation, asset criticality and business impact — each with a defined remediation SLA.

P0 CRITICAL	**Active exploitation + internet-facing + critical asset**	**24h** REMEDIATION SLA
P1 HIGH	**PoC available + targeted industry / region**	**7d** REMEDIATION SLA
P2 MEDIUM	**High CVSS + exposed asset, no active exploitation**	**30d** REMEDIATION SLA
P3 LOW	**Internal asset + no exploitation evidence**	**90d** REMEDIATION SLA

The shift: tiers are driven by what attackers are actually exploiting — not by the number on a scanner report. Active exploitation moves a Medium CVE to the top of the queue.

THE OPERATIONAL FRAMEWORK

Intelligence Sources & Six Steps to Operationalize

THREAT INTELLIGENCE DATA SOURCES

Active Exploitation Data | Threat Actor Intelligence | Zero-Day Tracking | Celebrity Vulnerabilities | IOC Databases

Effective prioritization integrates multiple sources to provide the context CVSS scoring cannot deliver — from real-time exploitation tracking to indicators of compromise for detection and response.

1 Automate Advisory Consumption

Ingest HiveForce Labs advisories and auto-correlate against your asset inventory.

2 Implement Continuous Validation

Use BAS to validate exploitability and test compensating controls against real TTPs.

3 Leverage Attack Path Analysis

Map how vulnerabilities chain for lateral movement; prioritize those that break critical paths.

4 Operationalize IOC Intelligence

Automate IOC ingestion (hashes, C2 infrastructure, URLs) into SIEM, EDR and network tools.

5 Extend Visibility to Edge Devices

Deploy discovery for VPNs, firewalls and load balancers — 83% of actors target them.

6 Track Supply Chain Exposure

Monitor third-party apps and SaaS; alert when vendors announce security incidents.

PROVEN OUTCOMES

What Intelligence-Driven Prioritization Delivers

Organizations implementing threat intelligence–driven prioritization with HiveForce Labs achieve measurable risk reduction.

97%

reduction in exploited vulnerability backlog through intelligent prioritization.

85%

faster mean time to remediation for critical threats — 72 hours vs 180 days.

60%

cost savings through tool consolidation and workflow automation.

Zero

successful exploits of known vulnerabilities in managed environments.

> Traditional vulnerability management prioritizes by CVSS. HiveForce Labs threat intelligence focuses remediation on the vulnerabilities attackers are actually exploiting — the ones that matter.

FROM THE FIELD

Security Leaders on the Shift to Exposure

> The impact of shifting from vulnerability to exposure management: night and day. I now could concentrate on those things specific to my organization. With Hive Pro, it's right there in front of us.

Matt Walker
Managing Director, IT Security & Compliance — Goosehead Insurance

> Before Hive Pro, it was kind of a game of whack-a-mole. CVSS scores don't always do a good job of telling you if it's something you really should pay attention to. That's where HivePro has solved a huge challenge for us in helping us prioritize properly.

David Malko
CSO — Direct Marketing Solutions

> For our security posture post-Hive Pro, I would say much more comprehensive. We have views and data and knowledge about our organization and our security posture much clearer. This is a 'Randy sleeps well at night' product.

Randy Potts
CSO — Real Time Resolutions

IMPLEMENTATION ROADMAP

From CVSS to Threat-Driven in 4–6 Weeks

A structured, phased transition to threat intelligence–driven exposure management.

01

Assessment

Week 1

Document existing tools, processes and backlogs. Map which systems are internet-facing, hold sensitive data or are business-critical. Review which threat actors target your industry and recent campaign exposure.

02

Platform Integration

Weeks 2–3

Connect existing scanners (Tenable, Qualys, Rapid7) to consolidate findings. Enable automated asset discovery across cloud and on-prem. Activate real-time threat intelligence feeds and automated correlation.

03

Operationalization

Weeks 4–6

Implement the P0–P3 tiers with remediation SLAs. Deploy BAS to validate exploitability. Connect ServiceNow / Jira for remediation workflows and push IOCs to SIEM and EDR. Shift the team from CVSS-driven to threat-driven.

04

Continuous Improvement

Ongoing

Monitor MTTR for P0/P1 exposures (target <72 hours), track backlog reduction and measure security-team efficiency gains. Adjust tier criteria to actual exploitation patterns in your industry and fine-tune asset criticality as priorities evolve.

Timeline: most organizations complete initial deployment within 4–6 weeks. The first week typically identifies 100–200 actively exploited vulnerabilities requiring immediate attention — immediate risk reduction while the full platform is configured.

SEE IT AGAINST YOUR OWN DATA

Prioritize What Attackers Are Exploiting Right Now.

See how threat intelligence integration works with your actual vulnerability data and threat landscape. A technical demonstration shows the specific threat actor activity relevant to your environment and industry.

Request a Technical Walkthrough

Or visit us to learn more: www.hivepro.com

Get Started →

HivePro Inc. | info@hivepro.com | www.hivepro.com