Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

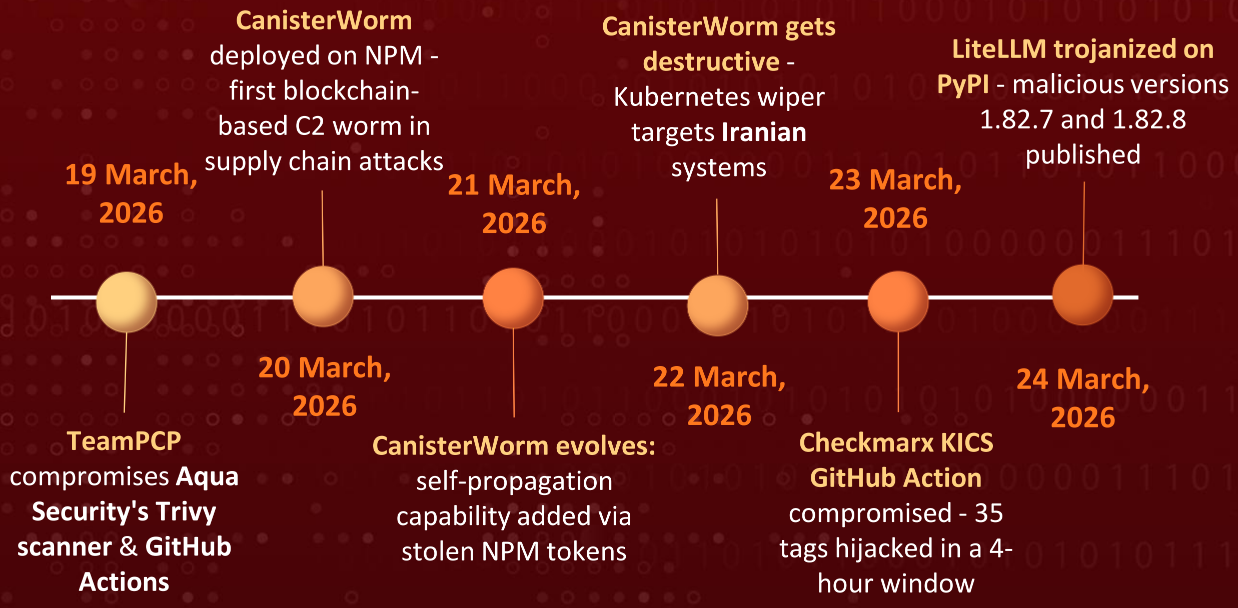
TeamPCP's Automated Supply Chain: From Trivy to LiteLLM in a Multi-Ecosystem Breach

Date of Publication	Admiralty Code	TA Number
March 26, 2026	A1	TA2026084

Summary

First Seen: December 2025
Targeted Regions: Worldwide (Primary focus on Iran)
Targeted Platforms: Docker APIs, Kubernetes clusters, and CI/CD pipelines
Targeted Industries: All
Threat Actor: TeamPCP
Malware: CanisterWorm

Timeline



19 March, 2026
TeamPCP compromises **Aqua Security's Trivy scanner & GitHub Actions**

20 March, 2026
CanisterWorm deployed on NPM - first blockchain-based C2 worm in supply chain attacks

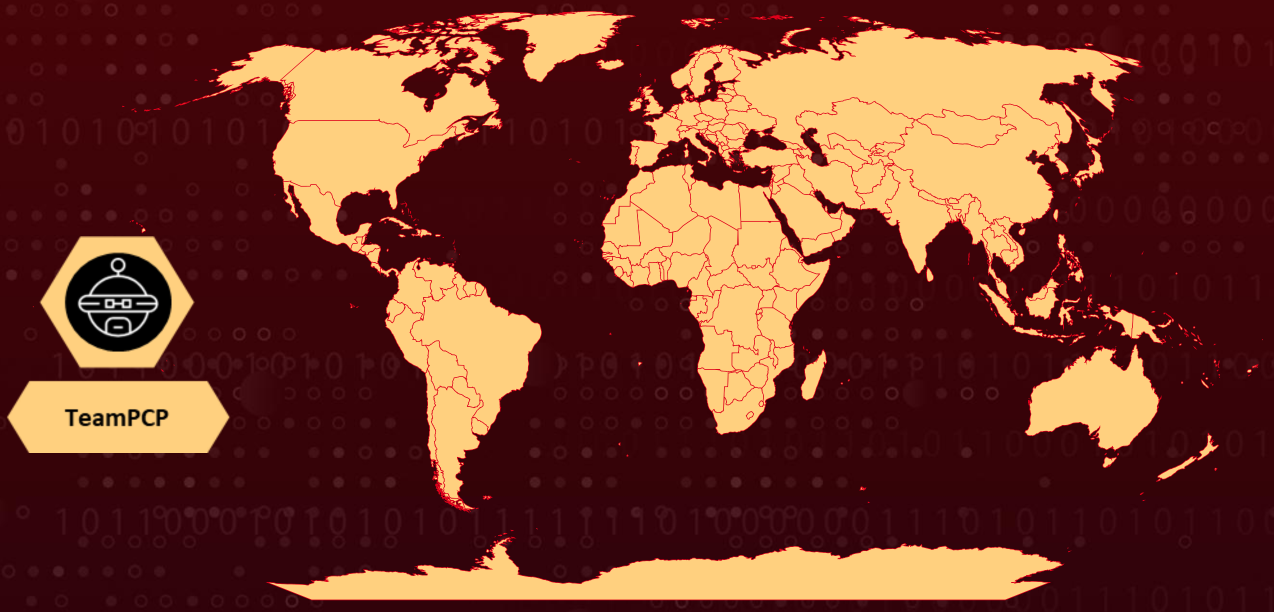
21 March, 2026
CanisterWorm evolves: self-propagation capability added via stolen NPM tokens

22 March, 2026
CanisterWorm gets destructive - Kubernetes wiper targets **Iranian** systems

23 March, 2026
Checkmarx KICS GitHub Action compromised - 35 tags hijacked in a 4-hour window

24 March, 2026
LiteLLM trojanized on PyPI - malicious versions 1.82.7 and 1.82.8 published

Actor Map



🟨	Targeted
🟥	Non-Targeted

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Actor Details

#1

TeamPCP is a cloud-focused threat group that has been active since at least late 2025. The group focuses on software supply-chain attacks, targeting widely used open-source security tools and developer infrastructure. Their operations show strong technical knowledge of CI/CD pipelines, container platforms, and distributed cloud environments.

#2

Before shifting to supply-chain attacks, TeamPCP carried out a large worm-based campaign in December 2025. They scanned for exposed Docker APIs, Kubernetes clusters, Redis servers, and Ray dashboards, compromising more than 60,000 servers worldwide. Most of the affected systems were hosted on Microsoft Azure and Amazon Web Services. The compromised infrastructure was used for proxy networks, scanning operations, cryptomining, ransomware, and data extortion.

#3

In March 2026, the group launched a new campaign that began with a single improperly rotated credential. This initial access quickly spread across multiple developer platforms, including GitHub Actions, Docker Hub, npm, OpenVSX, and PyPI. The attackers exploited trust relationships between these ecosystems to move laterally and expand their reach.

#4

One of the most significant incidents involved the compromise of the widely used LiteLLM Python package. Malicious versions of the package were uploaded to PyPI and included an information-stealing component designed to collect sensitive data from infected systems. The group also targeted other developer tools, including security scanners, by inserting credential-harvesting code into automated workflows.

#5

The malware used in these attacks focused on extracting secrets directly from CI runner memory. When a compromised workflow ran, it captured GitHub personal access tokens and other credentials from active processes. If those credentials had write access to additional repositories, the attackers used them to inject malicious code into other projects. This created a chain reaction in which one compromised component enabled the compromise of several more.

#6

In parallel, TeamPCP deployed malicious scripts against Kubernetes environments. Systems located in certain regions were wiped, while others were infected with a backdoor that allowed long-term remote control. This selective behavior showed that the group was capable of tailoring attacks based on geographic or operational targets.

#7

TeamPCP's main strength is not the discovery of new vulnerabilities but the speed and automation with which they exploit existing ones. By chaining together trusted developer services across multiple ecosystems, they were able to move from one compromised credential to widespread supply-chain damage in less than a week. Their use of decentralized infrastructure for command-and-control further complicates detection and takedown efforts, making this campaign both technically advanced and difficult to contain.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
TeamPCP	Unknown	Worldwide (Primary focus on Iran)	All
	MOTIVE		
	Espionage, Sabotage, Disruption, Financial Gains		

Recommendations

Enforce Immutable and Verified Dependencies: A core weakness exploited in the attacks was reliance on mutable version tags and unverified third-party actions. Attackers replaced legitimate tags with malicious code, which was automatically executed by downstream pipelines. All external dependencies, GitHub Actions, packages, and container images must be pinned to immutable commit hashes or digests rather than version tags. Verification of publisher identity and code provenance should be treated as a baseline requirement rather than an optional hardening step.

Reduce Trust in Third-Party CI Components: TeamPCP leveraged trusted automation tools, such as Trivy and KICS, to deliver malware. This reflects a broader pattern in modern supply-chain attacks where security tools themselves become attack vectors. Organizations should minimize reliance on external actions where equivalent functionality can be implemented internally and maintain an allow-list of approved CI components. Every new dependency introduced into a pipeline should undergo code review and risk assessment before adoption.

Isolate and Harden Build Environments: CI runners often operate with broad permissions and access to sensitive credentials. TeamPCP exploited this by extracting secrets directly from the runner memory. Build environments should be treated as high-risk execution zones and isolated accordingly. Ephemeral runners, network egress restrictions, and least-privilege permission models reduce the blast radius if a pipeline is compromised. Access to cloud resources from build systems should be limited to scoped, temporary identities rather than permanent credentials.

Audit Software Supply Chains End-to-End: The campaign spread across multiple ecosystems, GitHub, npm, PyPI, and container registries within days, demonstrating how modern software supply chains are deeply interconnected. Security reviews must extend beyond source code to include package registries, build pipelines, artifact repositories, and deployment environments. Maintaining a complete inventory of dependencies and generating a software bill of materials (SBOM) enables faster identification of affected systems when upstream compromises occur.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1195: Supply Chain Compromise	T1195.002: Compromise Software Supply Chain
		T1195.001: Compromise Software Dependencies and Development Tools
Execution	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
		T1059.006: Python
	T1204: User Execution	T1204.002: Malicious File
Persistence	T1543: Create or Modify System Process	T1543.002: Systemd Service
	T1053: Scheduled Task/Job	
Privilege Escalation	T1611: Escape to Host	
Defence Evasion	T1027: Obfuscated Files or Information	T1027.001: Binary Padding
	T1036: Masquerading	T1036.004: Masquerade Task or Service
		T1036.005: Match Legitimate Name or Location
	T1497: Virtualization/Sandbox Evasion	T1497.003: Time Based Evasion
Credential Access	T1528: Steal Application Access Token	
	T1552: Unsecured Credentials	T1552.005: Cloud Instance Metadata API
		T1552.004: Private Keys
	T1003: OS Credential Dumping	

Tactic	Technique	Sub-technique
Discovery	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
Lateral Movement	T1021: Remote Services	T1021.004: SSH
	T1610: Deploy Container	
Collection	T1560: Archive Collected Data	T1560.001: Archive via Utility
Command and Control	T1102: Web Service	T1102.001: Dead Drop Resolver
	T1572: Protocol Tunnelling	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
Exfiltration	T1041: Exfiltration Over C2 Channel	
Impact	T1485: Data Destruction	
	T1496: Resource Hijacking	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	e9b1e069efc778c1e77fb3f5fcc3bd3580bbc810604cbf4347897ddb4b8c163b, 61ff00a81b19624adaad425b9129ba2f312f4ab76fb5ddc2c628a5037d31a4ba, 0c0d206d5e68c0cf64d57ffa8bc5b1dad54f2dda52f24e96e02e237498cb9c3a, c37c0ae9641d2e5329fcdee847a756bf1140fdb7f0b7c78a40fdc39055e7d926, f398f06eefcd3558c38820a397e3193856e4e6e7c67f81ecc8e533275284b152, 7df6cef7ab9aae2ea08f2f872f6456b5d51d896ddda907a238cd6668ccdc4bb7, 5e2ba7c4c53fa6e0cef58011acdd50682cf83fb7b989712d2fcf1b5173bad956, 65bd72fcddaf938cefdf55b3323ad29f649a65d4ddd6aea09afa974dfc7f105d, 744c9d61b66bcd2bb5474d9afeee6c00bb7e0cd32535781da188b80eb59383e0, 0d66d8c7e02574ff0d3443de0585af19c903d12466d88573ed82ec788655975c, 527f795a201a6bc114394c4cfd1c74dce97381989f51a4661aafbc93a4439e90, 887e1f5b5b50162a60bd03b66269e0ae545d0aef0583c1c5b00972152ad7e073, f7084b0229dce605ccc5506b14acd4d954a496da4b6134a294844ca8d601970d, 822dd269ec10459572dfaaefe163dae693c344249a0161953f0d5cdd110bd2a0, bef7e2c5a92c4fa4af17791efc1e46311c0f304796f1172fce192f5efc40f5d7, e64e152afe2c722d750f10259626f357cdea40420c5eedae37969fbf13abbecf, ecce7ae5ffc9f57bb70efd3ea136a2923f701334a8cd47d4fbf01a97fd22859c, d5edd791021b966fb6af0ace09319ace7b97d6642363ef27b3d5056ca654a94c, e6310d8a003d7ac101a6b1cd39ff6c6a88ee454b767c1bdce143e04bc1113243, 6328a34b26a63423b555a61f89a6a0525a534e9c88584c815d937910f1ddd538,

TYPE	VALUE
SHA256	0880819ef821cff918960a39c1c1aada55a5593c61c608ea9215da858a86e349, 8395c3268d5c5dbae1c7c6d4bb3c318c752ba4608cfcd90eb97ffb94a910eac2, d2a0d5f564628773b6af7b9c11f6b86531a875bd2d186d7081ab62748a800ebb, a0d229be8efcb2f9135e2ad55ba275b76ddcfeb55fa4370e0a522a5bdee0120b, 71e35aef03099cd1f2d6446734273025a163597de93912df321ef118bf135238
SHA1	0e22ec8d1e0dda3c62bf4beffcd4a8a5db1abda1, 45f3749467a6017cb4fb749054b498d149dd5924, 8e20c7a67bb95632e2040327a355fb97e6014d29, 93de85c910d859b759cf9185aa78d5a23a4b7000, 0e7343ba084735863db92b6f8ba2fa9dee604f7c, 2dc0fa613f6f4c15f26ad98225ad253475681616, f00191dd3352c0cd83c6cce4e6bf04b628214dd0, e0359b1a253ee66c8018586c3225e6e9cd2d8a4f, dc6dbf358998c0c64da83edc8fcd581c12656b19, 08b9ea97eb292d5e1f9ac2d8e21c0ba32f0fdff0, 005fb0837553de722f8bf11d98e905dbdde19861, a5471d37c656ecd4560e8e0b3977910f27025618, 3d49875ed47c6b8b4c8b50e0421418cf6b9f35f4, 121c38fb49c9fc82160245fb6e2a9119db636e4d, 1e9eeaba37fe0032deba133f598e74dab0ceb3b7, c5c07508527fc6a125855eebfb533e64f675bd8e, c999dbb9cc904e23675f9929f7e0e51d132879cf, 4ebf62dd8ff318412b38d19841fc3c8650e294bf, 3ae9f0d6f8139964635d411149f9b3e0a6eb935e, 96a0e8eb31c3cce6c495c9a49dd49c881cd17934, 31fbf5831a2e52429738fdc0cbaa20e57872b6fc, fca3a20afcb8ec7f9932c060a236d2a9021fdd2b, 0f81f132f9f09bb4976d403914a44a1a1eb6158d, c0e23718a5074f3b8ad286f37b532e02057af35f, d66f0657133bc42f8264458063999bf1910490db, e35c9d6a5faffc1c5b3450d0bf09006aa9b9e906, 2eee333d70fb6e14ce1d4aa73f12058bc5d70193, f9641eb512f5c6530d13275903e8a97baf0925f1, e8754eebc822b5122e96a6142b28dbc0e179c91c, 69b3f020390222a9fcb6029ba56533b2fb12f103, db942a0dd7e9d1aeac72bc675bdb67f39a688b63, 208813bf5feca5df9a935363cd426bc914614d0b, 3fdeadb81fbeddc1453163cc87bc173911fd47e2,

TYPE	VALUE
SHA1	310734c0ffd29438f6195a24e2cbbacfdc33c9ab, b974e53df1e3a2cd22ea90f0ec01882394feede4, 8afa9b9f9183b4e00c46e2b82d34047e3c177bd0, 386c0f18ac3d7f2ed33e2d884761119f4024ff8a, 384add36b52014a0f99c0ab3a3d58bd47e53d00f, 7a4b6f31edb8db48cc22a1d41e298b38c4a6417e, 6d8d730153d6151e03549f276faca0275ed9c7b2, 99b93c070aac11b52dfc3e41a55cbb24a331ae75, f4436225d8a5fd1715d3c2290d8a50643e726031, f4f1785be270ae13f36f6a8cfbf6faaae50e660a, 0891663bc55073747be0eb864fbec3727840945d, 2e7964d59cd24d1fd2aa4d6a5f93b7f09ea96947, ddb9da4475c1cef7d5389062bdfdfbdbd1394648, 4209dcadeaea6a7df69262fef1beeda940881d4d, f5c9fd927027beaa3760d2a84daa8b00e6e5ee21, 18f01febc4c3cd70ce6b94b70e69ab866fc033f5, bb75a9059c2d5803db49e6ed6c6f7e0b367f96be, d488f4388ff4aa268906e25c2144f1433a4edec2, 3c615ac0f29e743eda8863377f9776619fd2db76, a9bc513ea7989e3234b395cafb8ed5ccc3755636, 8519037888b189f13047371758f7aed2283c6b58, 8cfb9c31cc944da57458555aa398bb99336d5a1f, 9092287c0339a8102f91c5a257a7e27625d9d029, 7b955a5ece1e1b085c12dac7ac10e0eb1f5b0d4d, 19851bef764b57ff95b35e66589f31949eeb229d, 61fbe20b7589e6b61eedcd5fe1e958e1a95fbd13, fa78e67c0df002c509bcdea88677fb5e2fe6a9b1, b7befdc106c600585d3eec87d7e98e1c136839ae, 7f6f0ce52a59bdfc5757c3982aac2353b58f4c73, ddb6697447a97198bdef9bae00215059eb5e8bc2, 3dffed04dc90cf1c548f40577d642c52241ec76c, ad623e14ebdfe82b9627811d57b9a39e283d6128, 848d665ed24dc1a41f6b4b7c7ffac7693d6b37be, ddb94181dcbc723d96ffc07fddd14d97e4849016, b7252377a3d82c73d497bfafa3eabe84de1d02c4, fa4209b6182a4c1609ce34d40b67f5cfd7f00f53, 2b1dac84ff12ba56158b3a97e2941a587cb20da9, 66c90331c8b991e7895d37796ac712b5895dda3b, fd429cf86db999572f3d9ca7c54561fdf7d388a4, 8ae5a08aec3013ee8f6132b2a9012b45002f8eaa, 2a51c5c5bb1fd1f0e134c9754f1702cfa359c3dd, 9c000ba9d482773cbbc2c3544d61b109bc9eb832, 91e7c2c36dcad14149d8e455b960af62a2ffb275, 4bdcc5d9ef3ddb42ccc9126e6c07faa3df2807e3,

TYPE	VALUE
SHA1	9e8968cb83234f0de0217aa8c934a68a317ee518, c5967f85626795f647d4bf6eb67227f9b79e02f5, b745a35bad072d93a9b83080e9920ec52c6b5a27, 38623bf26706d51c45647909dcfb669825442804, 555e7ad4c895c558c7214496df1cd56d1390c516, 2297a1b967ecc05ba2285eb6af56ab4da554ecae, 820428afeb64484d311211658383ce7f79d31a0a, f77738448eec70113cf711656914b61905b3bd47, 252554b0e1130467f4301ba65c55a9c373508e35, 22e864e71155122e2834eb0c10d0e7e0b8f65aa3, 405e91f329294fb696f55793203abf1f6aba9b40, 506d7ff06abc509692c600b5b69b4dc6ceaa4b15, 276ca9680f6df9016db12f7c48571e5c4639451d, aa3c46a9643b18125abb8aefc13219014e9c4be8, ea56cd31d82b853932d50f1144e95b21817e52cf, 0d49ceb356f7d4735c63bd0d5c7e67665ec7f80c, 7550f14b64c1c724035a075b36e71423719a1f30, da73ae0790e458e878b300b57ceb5f81ac573b46, 6ec7aaf336b7d2593d980908be9bc4fed6d407c6, cf19d27c8a7fb7a8bbf1e1000e9318749bcd82cf, ef3a510e3f94df3ea9fcd01621155ca5f2c3bf5b, 6fc874a1f9d65052d4c67a314da1dae914f1daff, b9faa60f85f6f780a34b8d0faaf45b3e3966fdda, ab6606b76e5a054be08cab3d07da323e90e751e8, a5b4818debf2adbaba872aaffd6a0f64a26449fa, e53b0483d08da44da9dfe8a84bf2837e5163699b, 8aa8af3ea1de8e968a3e49a40afb063692ab8eae, 91d5e0a13afab54533a95f8019dd7530bd38a071, 794b6d99daefd5e27ecb33e12691c4026739bf98, 9ba3c3cd3b23d033cd91253a9e61a4bf59c8a670, e0198fd2b6e1679e36d32933941182d9afa82f6f, 9738180dd24427b8824445dbbc23c30ffc1cb0d8, 3201ddddd69a1419c6f1511a14c5945ba3217126, 985447b035c447c1ed45f38fad7ca7a4254cb668, 3d1b5be1589a83fc98b82781c263708b2eb3b47b, fd090040b5f584f4fcbe466878cb204d0735dcf4, 85cb72f1e8ee5e6e44488cd6cbdbca94722f96ed, cf1692a1fc7a47120e6508309765db7e33477946, 1d74e4cf63b7cf083cf92bf5923cf037f7011c6b, c19401b2f58dc6d2632cb473d44be98dd8292a93
Domains	tdtqy-oyaaa-aaaae-af2dq-cai[.]raw[.]icp0[.]io, plug-tab-protective-relay[.]trycloudflare[.]com, scan[.]aquasecurtiy[.]org, checkmarx[.]zone
IPv4	45[.]148[.]10[.]212, 83[.]142[.]209[.]11

TYPE	VALUE
File Path	/var/lib/svc_internal/runner.py, /etc/systemd/system/internal-monitor.service, /tmp/pglog, /tmp/.pg_state, /var/lib/pgmon/pgmon.py, /etc/systemd/system/pgmonitor.service, ~/.local/share/pgmon/service.py, ~/.config/systemd/user/pgmon.service
URLs	hxxps[:]//souls-entire-defined-routes[.]trycloudflare[.]com/, hxxps[:]//investigation-launches-hearings-copying[.]trycloudflare[.]com/, hxxps[:]//championships-peoples-point-cassette[.]trycloudflare[.]com, hxxps[:]//tdtqy-oyaaa-aaaae-af2dq-cai[.]raw[.]icp0[.]io/

References

https://www.aikido.dev/blog/teampcp-stage-payload-canisterworm-iran

https://www.aikido.dev/blog/teampcp-deploys-worm-npm-trivy-compromise

https://www.elastic.co/security-labs/teampcp-container-attack-scenario

https://www.wiz.io/blog/teampcp-attack-kics-github-action

https://www.wiz.io/blog/trivy-compromised-teampcp-supply-chain-attack

https://www.wiz.io/blog/threes-a-crowd-teampcp-trojanizes-litellm-in-continuation-of-campaign

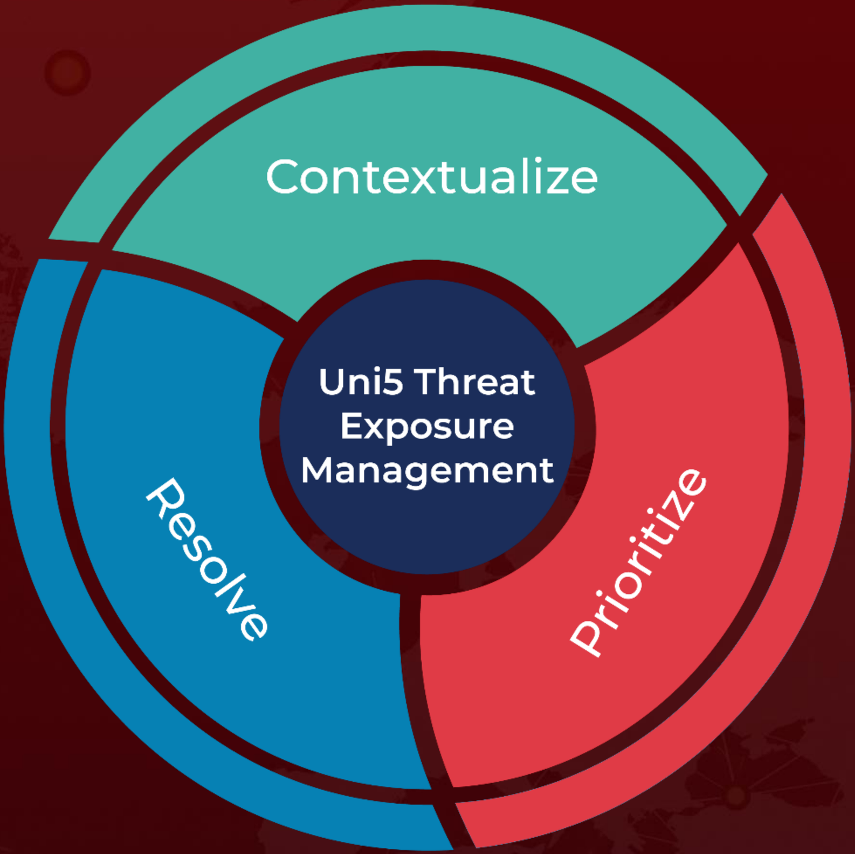
https://www.sysdig.com/blog/teampcp-expands-supply-chain-compromise-spreads-from-trivy-to-checkmarx-github-actions

https://www.endorlabs.com/learn/teampcp-isnt-done

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 26, 2026 • 9:00 AM

More at www.hivepro.com