INTEL471

WHITEPAPER

EXTERNAL ATTACK SURFACE MANAGEMENT:

Intelligence-Driven Cybersecurity

Executive Summary

Digital transformation, multi-cloud, software-as-a-service (SaaS) adoption, and digital supply chain risks are driving the expansion of the external attack surface. The modern attack surface is also complex. Legacy IT systems, unpatched vulnerabilities, misconfigurations, shadow IT, forgotten third-party services, exposed cloud storage buckets, and leaked credentials are all potential points of exposure. And threat actors are prioritizing unpatched internet-facing assets to gain initial access, making it critical for defenders to remediate exposures before attackers move laterally in the network.

The purpose of External Attack Surface Management (EASM) is to reduce the complexity of defending this dynamic attack surface by continuously monitoring known assets and discovering new, unknown and unsanctioned internet-facing assets. Insightful, human-led and automation-assisted cyber threat intelligence (CTI) that contextualizes the threat landscape helps defenders see what assets are likely to be attacked and where to focus remediation. This white paper will look at why organizations are establishing CTI security programs, different EASM methodologies, the benefits of CTI-led EASM for asset remediation, and how to work with stakeholders to create a CTI program that reduces operational and third-party risk.

Regulations Point to a Future of CTI-led Security

New regulations aimed at lifting critical infrastructure cyber resilience with proactive threat detection and response are driving the adoption of CTI-led security.

The US Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) and the EU's Network and Information Systems Directive 2 (NIS2) bring closer scrutiny to how mid- and large-sized operators of critical infrastructure in the US and Europe manage cyber risks. CIRCIA will affect over 315,000 organizations. NIS2, the successor to the 2016 NIS Directive, affects more sectors, more mid-sized operators of essential services, and introduces higher fines for failing to manage risks for networks, IT and OT systems, incident handling, and supply chain security.

The 2024 SANS CTI Survey found that new critical infrastructure cybersecurity regulations, the SEC's material incident disclosures rules, and ISO 27001 standards will play a "very important" or "somewhat important" role in 74% of respondents' CTI planning.

Organizations with mature CTI programs have far better awareness of the threat environment to meet rapid incident reporting requirements and proactively mitigate emerging threats to their assets and supply chains.

Establishing a CTI program is complex, however a recent revision to the ISO/IEC 27001 standards for IT systems introduced CTI as a security control, which will help standardize how organizations implement CTI. The guidance reinforces that CTI should be relevant, insightful, contextual, and actionable. CTI should also incorporate strategic, tactical and operational threat intelligence to address the needs of management, SOCs, incident response, and other security teams. It also provides guidance on the planning required to build a CTI program, from selecting reliable sources to ensuring CTI is collected, processed, analyzed, communicated and then used to reduce risk. Later in this paper we offer an open-source methodology for designing a successful CTI program.

CTI SHOULD BE RELEVANT, INSIGHTFUL, CONTEXTUAL, AND ACTIONABLE

EASM is also an important tool for regulators to reduce attack surface exposures in critical infrastructure. CISA already provides non-intrusive vulnerability assessments and European national Computer Security Incident Response Teams (CSIRTs) may perform non-intrusive vulnerability scans on affected entities' attack surfaces.

Entities affected by CIRCIA and NIS2 should aim to reduce the risk of reportable cyber incidents by independently performing active, intrusive EASM scans on their own attack surface, and continuously mapping current CTI data to their exposures. Active EASM scanning enables security teams to identify known vulnerabilities, expired certificates, identifying shadow IT, and test for misconfigurations. This approach generates much more traffic to the target than passive-only EASM because it involves actively testing for vulnerabilities, querying application protocol interfaces (APIs), scraping web pages, screenshotting web pages, scanning ports, and running Domain Name Service (DNS) queries. While it is likely to set off security alarms at the targeted entity, the benefit is much deeper visibility. Additional passive scanning can help identify information exposures such as leaked credentials.

Taming Attack Surface Remediation with CTI

The number of disclosed vulnerabilities is rising significantly each year. The National Institute of Standards and Technology (NIST) assigned 28,831 new Common Vulnerabilities and Exposures (CVEs) to its National Vulnerability Database (NVD) in 2023 — a 560% increase since 2013 and 15% more than in 2022. Additionally, over half or 15,560 CVEs assigned in 2023 were "critical", contributing to the so-called alert fatigue problem. It's worth noting that recent NVD funding issues have complicated vulnerability management and make it likely there will be vulnerabilities not documented in the NVD.

While only part of the NVD is relevant to an organization, many security teams — alert-fatigued or not — are uncertain about what CVEs to track and patch first. EASM can help make timely and contextualized CTI more actionable by continuously scanning the attack surface, which helps defenders map exposures to issues that must be addressed.

Intel 471's Vulnerability Intelligence team distills the NVD to a much smaller subset of CVEs that it believes are likely to be exploited. These CVEs are tracked by analysts across the globe in the Intel 471 TITAN Vulnerability Intelligence Dashboard. This CTI is also contextualized with information about the time a CVE emerged, where its risk level changed, how it changed, and its prevalence in similar organizations. The team's evaluation for their inclusion (or removal) on the dashboard is based on local language engagement with sources on cyber underground forums, assessments of claims by known threat actors, such as exploit brokers, security industry intelligence, vendors of compromised access credentials, cybercrime messaging groups, data leak blog posts, and other sources. This analysis also clarifies the evolving risk a vulnerability poses, based on whether the CVE has been:

- Researched for proof-of-concept exploit code development
- Discussed in underground forums or the open web
- Weaponized (integrated into an exploit kit for sophisticated users)
- Productized (integrated in tools such as a Metasploit module, Cobalt Strike, or Armitage for unsophisticated users)
- Actively exploited

By integrating CTI with continuous EASM scanning, security teams can immediately see when assets are at a higher risk from emerging threats, such as underground chatter about a CVE, or an immediate priority, such as when a CVE on the attack surface is weaponized. The Vulnerability Intelligence team also tracks and maps CVEs that are actively exploited to known malware activity, which is critical for decisions about prioritized remediation.

The external attack surface extends to the supply chain, such as contractors and managed IT service providers. CTI-led EASM enables security teams to combine CTI with EASM monitoring of third parties.

The need for CTI-enabled first-party and third-party EASM was demonstrated in the aftermath of CLOP data extortion gang's rapid exploitation of CVE-2023-34362, a SQL injection flaw in Progress Software's MOVEit managed file transfer (MFT) web application. CLOP compromised and exfiltrated data from over 2,700 organizations with vulnerable MOVEit servers. Several victim organizations that didn't directly use MOVEit suffered customer data breaches because their managed service provider used the application.

CLOP claimed to have compromised "hundreds" of victims before Progress Software released a patch on May 31. But on June 16, Intel 471 found another threat actor had

weaponized CVE-2023-34362 with a new exploit and was selling it in a hacking tool that significantly lowered the barrier for other actors to exploit it. Users of EASM solutions integrated with TITAN CTI data were immediately alerted to this new threat in reporting from scans of their IT environment and third-party environments.

The rapid exploitation by multiple actors of new critical vulnerabilities in internet-facing assets like CVE-2023-34362 is consistent with Intel 471's findings that threat actors are prioritizing new flaws for weaponization because they're less likely to have been patched. Threat actors weaponized 60% of CVEs tracked by Intel 471 in 2023, up from 47% in 2022. In 2023, there was also a 177.8% year-on-year increase in the exploitation of software and web application vulnerabilities.

Narrowing the Focus to High-Risk CVE Events

Real-world active EASM scans demonstrate how vast the attack surface is. For this paper, we examined all unpatched CVEs that customers using Intel 471's EASM solution Attack Surface Intelligence (ASI) found in the 12 months prior to June 13, 2024. ASI by default employs active scans and optional passive scans using API for services like Shodan for broader visibility.

ASI customers found 25,606 unique assets with at least one "critical" CVE and 315,985 unique assets with at least one CVE. The dataset of identified published vulnerabilities totaled 4,994 unique CVEs, of which 57 were assigned in 2024 as of June 13. The distribution of remaining CVEs was about 400 per year between 2023 to 2017, followed by a long tail of CVEs assigned between 2016 and 1999.

We can narrow down the 4,994 CVEs to a more manageable number using a small subset of a much larger CTI dataset from Intel 471's Vulnerability Intelligence. Since attackers are prioritizing newly disclosed flaws, we can, for example, correlate assets with CVEs that have been weaponized and were assigned in 2024 and 2023. Just 55 or 12% of 453 CVEs assigned in this period had been weaponized.

Amongst this set of weaponized and actively exploited vulnerabilities was CVE-2024-3400, a critical command injection vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS disclosed publicly on April 12 with a CVSSv3 severity score of 9.8 out of 10. Intel 471 analysts discovered a threat actor had offered to sell an alleged exploit for this CVE on April 22. This was immediately logged in Intel 471's TITAN platform and automatically shared via 471 ASI alerting as an elevated risk. In this narrow use case, EASM is akin to CISA's Known Exploited Vulnerabilities (KEV) catalog of CVEs for priority patching by federal agencies, except that CVEs are mapped to the organization's external attack surface.

Another CVE in this set of weaponized and actively exploited vulnerabilities detected in 471 ASI scans as of June 13 was CVE-2024-4577, an remote code execution flaw with a CVSSv3 score of 9.8 affecting multiple versions of PHP running on Microsoft Windows. Patches were released on June 6. Within a day researchers reported attempted exploitation and within 48 hours of the exploit code becoming publicly available, operators of the TellYouThePass ransomware used it in attacks. Intel 471's Intelligence Summary for the week of June 3 to June 9 indicated the CVE had been weaponized, productized, and exploited in the wild. While CISA researchers had also observed exploitation at this point, the CVE was not added to the CISA KEV catalog until June 12. More importantly, teams using ASI to continuously monitor their attack surface were able to identify vulnerable versions of PHP on Windows servers in their environment with alerting about the CVE's evolving exploit status.

CVE-2024-4577 was among 12 vulnerabilities exploited in the wild in June that the Vulnerability Intelligence team were tracking in June, a month that the NVD gained 3,095 new vulnerabilities, of which 360 were rated as high or critical. Malware that the team mapped to these 12 CVEs included the Cardinal cybercrime group (aka Storm-1811, UNC4393), which operates the Black Basta ransomware, the well-known advanced threat actor IntelBroker, the Coathanger malware.

Ultimately, how well defenders can prioritize remediation depends greatly on the credibility and timeliness of CTI and each EASM solution's approach to data collection and scanning.

Where Does CTI-led EASM Go from Here?

Organizations of all sizes can use CTI-led EASM to reduce risk in their attack surface. That CTI should consist of open-source intelligence (OSINT) and closed source CTI data based on access to sources on underground markets and forums, continuous evaluation of threat actor tactics, techniques and procedures (TTPs) for initial access, persistence and lateral movement, in-depth malware analysis, and vulnerability and exploit status intelligence.

Organizations considering ingesting CTI should undertake an intelligence planning exercise to understand what key stakeholders — ranging from senior management, security operations, incident response, forensics, legal and risk management professionals — regard as the most important or valuable types of CTI.

Intel 471 has developed an open-source framework, the Cyber Underground General Intelligence Requirements Handbook (CU-GIRH) as a baseline tool to assist in organizing, prioritizing, measuring and producing cyber underground intelligence (for more information, see our blog post "Open Source Release of Intel 471 Intelligence Requirements Framework)."

Central to the CU-GIRH framework are General Intelligence Requirements (GIRs). GIRs describe threats and activities that pose risks to organizations — such as malware, vulnerabilities, access brokering, etc. — and the relevant questions around those activities that practitioners should focus on to create actionable intelligence products. These GIRs can be selected to narrow down Priority Intelligence Requirements (PIRs), which are specific to organizations based on their own threat modeling and assessments. PIRs are the most important intelligence requirements for an organization.

The Journey to Intelligence-led Security

Organizations of all sizes can establish an intelligence-led EASM practice not only to assess exposures. Large organizations with more resources and more mature CTI practices will find the approach easier, but there is also an opportunity for smaller organizations to prepare for new regulations and standards that cement CTI into security practices. Intelligence-led EASM can deliver a significant return on investment and help your security team prevent attackers gaining the initial foothold on the network that leads to a data breach or ransomware event. For more information about how to establish an intelligence-led EASM practice, please contact Intel 471.

About Intel 471

Intel 471 empowers enterprises, government agencies, and other organizations to win the cybersecurity war using the real-time insights about adversaries, their relationships, threat patterns, and imminent attacks relevant to their businesses. The company's platform collects, interprets, structures, and validates human-led, automation-enhanced intelligence, which fuels our external attack surface and advanced behavioral threat hunting solutions. Customers utilize this operationalized intelligence to drive a proactive response to neutralize threats and mitigate risk. Organizations across the globe leverage Intel 471's world-class intelligence, our trusted practitioner engagement and enablement and globally-dispersed ground expertise as their frontline guardian against the ever-evolving landscape of cyber threats to fight the adversary — and win. Learn more at intel471.com.

Our customers' eyes and ears outside the wire.