INTEL471

471 Vulnerability Intelligence

KEY VALUE

- Informs vulnerability management and drives patch priorities with external threat intelligence
- Provides a live dashboard to track and alert on changes across the range of precursors of exploitation
- Delivers a regular stream of vulnerability reporting complete with sourcing for deeper context and background on vulnerabilities
- Drives all intelligence reporting and observations via actual analysts judgements versus monitoring volumetric keyword hits
- Tracks threat actor discussions and interest levels related to vulnerabilities, which often drives weaponization and productization
- Alerts when threat actors are selling, buying and trading proof-of-concept (POC) code signaling weaponization is imminent
- Identifies when patching is critical based on threat actors integrating vulnerabilities into exploit products, which vastly lowers the barrier to entry for exploitation
- Integrates using a RESTful API or one of our third-party integrations — SEIMs, Threat Intelligence Platforms (TIPs) and other security tooling

✉ sales@intel471.com

Vulnerability Patching and Business Requirements

Organizations are facing an ever-increasing list of applications and systems requiring regular patching to stay ahead of adversaries keen to exploit their vulnerabilities. However, even the notion that you can continuously take an enterprise offline to conduct patching is unrealistic and detrimental to daily business operations. An intelligent vulnerability management program must prioritize patching in relation to the business requirements of the organization, but without relevant and prioritized intelligence, this is a major challenge.

Driven by Intelligence

471 Vulnerability Intelligence provides both relevant and timely information about the adversary landscape and fills the void created by current vulnerability offerings, which focus mainly on existing exploits based on known attacks and open-source information. Our Vulnerability Intelligence closes this gap by including the precursors to such activity such as an increase in interest levels amongst threat actors, proof-of-concept (POC) code being developed, traded or sold, and ultimately the weaponization and productization of the code as it gets integrated into exploit kits, packs or other tools. This activity often takes place prior to attacks being observed in the wild and being alerted enables a more proactive approach to vulnerability management. Vulnerability Intelligence allows organizations to prepare for what's coming and patch accordingly, rather than hope that their system is robust enough based on historical/known attacks.

Precursors of Exploitation

471 Vulnerability Intelligence focuses on the precursors to exploitation of vulnerabilities in the wild via a regularly updated dashboard. It tracks the life cycle of significant vulnerabilities observed in the cyber underground from initial disclosure to exploit weaponization and productization. 471 Vulnerability Intelligence offers an analyst-driven assessment of priority vulnerabilities beyond volumetric keyword hits, which just isn't adequate in today's cybersecurity environment.

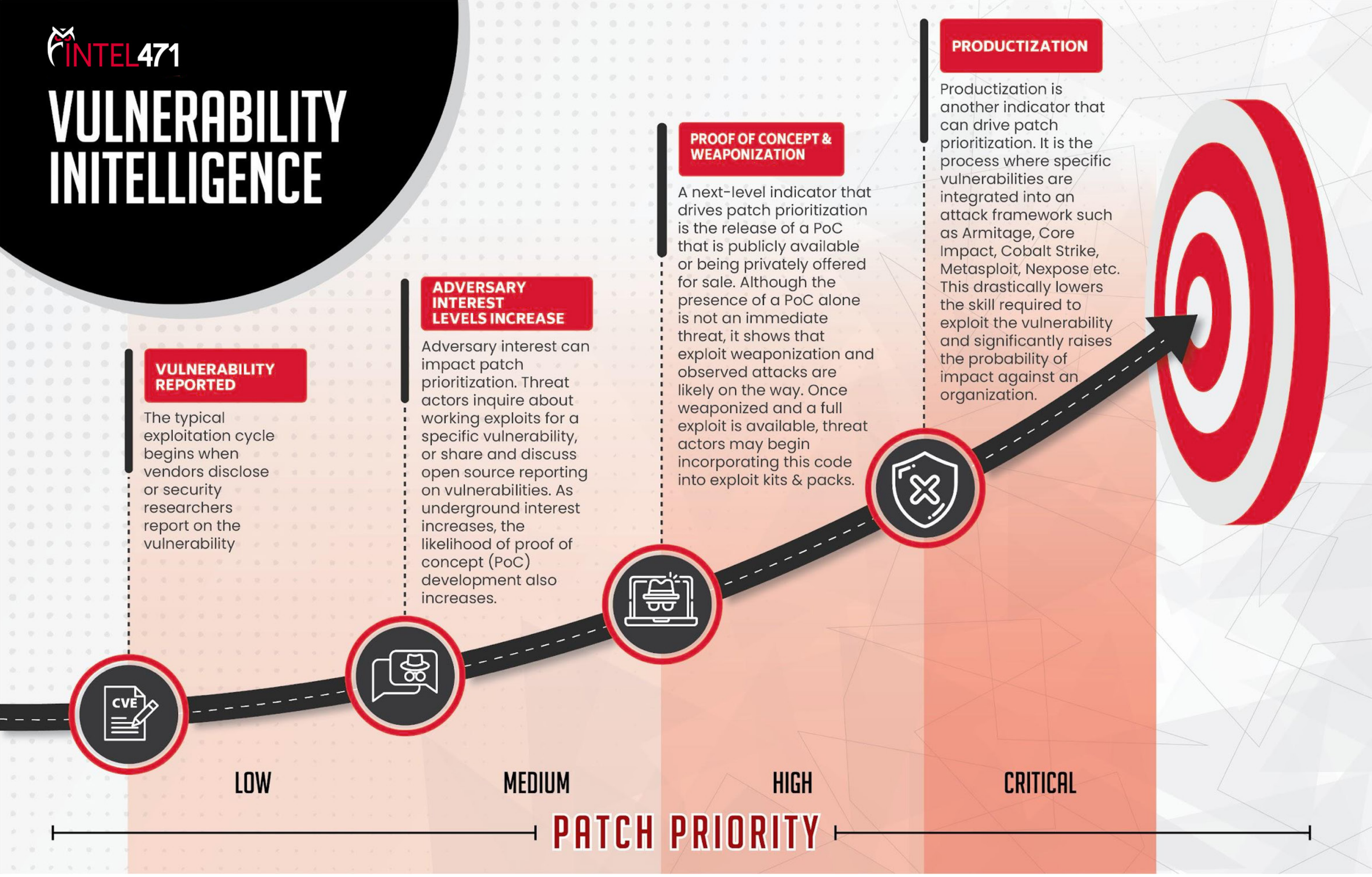
Precursors to exploitation include:

- Vulnerability publicized and patches released
- Threat actor interest levels start to orient toward specific vulnerabilities
- Proof-of-Concept (POC) code is made available amongst threat actors and researchers
- Weaponization is observed as exploits are bought and employed
- Productization occurs, lowering the barrier to exploitation significantly

Offering Something Different

Unlike many vulnerability offerings, Intel 471 bridges the gap between historical known attacks and those which are imminent. By gathering intel on the entire process, organizations can track threats as they develop, and then prioritize patching as the need arises. Resources within any CTI team are always stretched, so Intel 471 provides you with the most relevant intel, the progress of possible threats and the wider context from the cyber underground. With complete transparency of this process, organizations are no longer patching blindly, they have critical and timely intelligence that can be easily utilized to protect their organization.

VULNERABILITY INITELLIGENCE



VULNERABILITY REPORTED

The typical exploitation cycle begins when vendors disclose or security researchers report on the vulnerability

ADVERSARY INTEREST LEVELS INCREASE

Adversary interest can impact patch prioritization. Threat actors inquire about working exploits for a specific vulnerability, or share and discuss open source reporting on vulnerabilities. As underground interest increases, the likelihood of proof of concept (PoC) development also increases.

PROOF OF CONCEPT & WEAPONIZATION

A next-level indicator that drives patch prioritization is the release of a PoC that is publicly available or being privately offered for sale. Although the presence of a PoC alone is not an immediate threat, it shows that exploit weaponization and observed attacks are likely on the way. Once weaponized and a full exploit is available, threat actors may begin incorporating this code into exploit kits & packs.

PRODUCTIZATION

Productization is another indicator that can drive patch prioritization. It is the process where specific vulnerabilities are integrated into an attack framework such as Armitage, Core Impact, Cobalt Strike, Metasploit, Nexpose etc. This drastically lowers the skill required to exploit the vulnerability and significantly raises the probability of impact against an organization.

FREQUENTLY ASKED QUESTIONS

What is the purpose of 471 Vulnerability Intelligence dashboard?

Intel 471's Vulnerability Intelligence Dashboard is a quick reference tool designed to assist patch prioritization and vulnerability management decision-making. This regularly updated dashboard tracks the life cycle of significant vulnerabilities observed in the underground from initial disclosure to exploit weaponization and productization. It offers an analyst-driven assessment of priority vulnerabilities beyond keyword hits.

How are CVEs phased off 471 Vulnerability Intelligence dashboard over time?

To keep the dashboard current and concise, a vulnerability is removed from the dashboard after no significant state changes have been observed within two weeks. High risk vulnerabilities will continue to be monitored for up to an additional 30 days and re-published to the dashboard if a state change occurs.

Note: CVEs phased off the dashboard will still be searchable within TITAN.

What vulnerabilities are included in 471 Vulnerability Intelligence dashboard?

To help prioritize and track vulnerabilities likely to impact you, we regularly push individual vulnerabilities into dashboard view once an analyst manually reviews and validates any of the following criteria have been met:

- A significant CVE is discussed actively in the underground
- Requests for exploits are observed
- The CVE is weaponized or productized

How are vulnerabilities prioritized and ranked on 471 Vulnerability Intelligence dashboard?

Intel 471 analysts review and assess individual vulnerabilities and weigh them collectively against a number of factors including a proprietary Intel 471 risk level which factors in exploit status, actor interest level, patch availability, CVSS score, CVE ID and more.

What do the different "Interest Level" indicators mean?

- Disclosed publicly – applies to CVEs that have been publicly disclosed
- Researched publicly – applies to CVEs when they are observed in research publications (blogs, whitepapers, etc.)
- Exploit sought in underground – applies to CVEs when a threat actor is looking for exploits in the underground

These are contextualized indicators, not based on simply the number of observed underground discussions.

Why Intel 471?

Our experts operate across the globe, closely tracking sophisticated threat actors in the places they operate, speak their languages, and understand cultural references that expose and illuminate their underground activities. As a result, we can provide the most relevant and timely intelligence to our customers. Relevant intel refers to specific threats to your business or industry, and when CTI teams are often stretched to capacity, having the guidance on where to focus your team's finite resources is essential. The additional ability for organizations to understand and then implement necessary change is where the real value lies. We pride ourselves on helping organizations operationalize their intel so they are better protected against possible threats. As your organization and their CTI requirements grow, so too can our solution. Even for the most mature CTI teams, our intelligence will far exceed their most ambitious requirements.