THREAT INTELLIGENCE USE CASE SERIES

VULNERABILITY MANAGEMENT ANALYST

VULNERABILITY MANAGEMENT ANALYSTS

Most IT organizations include analysts whose role is to track and prioritize vulnerabilities and help develop mitigation plans. They may be in the security operations or security engineering groups, or on the compliance and risk management team. Their tasks include:

- Discovering the servers, devices, endpoints and applications used by the enterprise, and identify the vulnerabilities that may be present.
- Identifying which new vulnerabilities pose serious risks to the enterprise and which are lower priorities, based on factors like the severity of the vulnerability, the systems and applications present in the enterprise, defenses and controls already in place, and whether the vulnerability is currently being exploited "in the wild."
- Helping determine optimal strategies for mitigation.
- Communicating with auditors, risk managers, and other IT groups about risks from vulnerabilities that cannot be mitigated immediately.

How Vulnerability Management Analysts Use Cyber Threat Intelligence

Vulnerability management analysts are using cyber threat intelligence to determine what vulnerabilities are critical, to help determine optimal mitigation strategies, and to communicate risks to managers and to other IT groups.

> Ideally, an organization would deploy every new patch immediately... However, in reality this is simply not possible because organizations have limited resources, which makes it necessary to prioritize which patches should be installed before other patches....
>
> —
>
> **NIST Special Publication 800-40 Revision 3**

CHALLENGES FACING VULNERABILITY MANAGEMENT ANALYSTS

The analysts and administrators responsible for tracking and prioritizing vulnerabilities face a variety of challenges, including:

- An ever-increasing flow of new vulnerabilities announced by software vendors, security consultants – and hackers and cybercriminals.
- The fact that a high percentage of entries in vulnerability databases have high risk scores (e.g., 41% of vulnerabilities in the National Vulnerability Database have a CVSS score of 7-8, 8-9 or 9-10), making it very difficult to identify the highest priority vulnerabilities.
- Little information is available to pinpoint which of the hundreds of vulnerabilities announced each month are relevant to a specific industry, geographic region or enterprise.
- It is difficult to determine when exploits have been developed to allow attackers to take advantage of new vulnerabilities, and what exploits are likely to be used as part of advanced attacks.

FireEye

Use Cases – Vulnerability Management Analyst

USE CASE	KEY OBJECTIVE	INTELLIGENCE NEEDED
Analysis of Vulnerabilities	Classify vulnerabilities by type, source and likely targets Understand how vulnerabilities are exploited as part of advanced attacks	Intelligence knowledge base of vulnerabilities, threat actors, attack techniques and likely targets Threat analysis reports customized for the industry or enterprise
Vulnerability Prioritization	Determine which vulnerabilities: • Affect systems and software in the enterprise • Are not mitigated by existing defenses and controls • Are actively being exploited by threat actors	Intelligence knowledge base Research on attack methods currently in use and exploit kits offered on hacker websites
Identification of Mitigation Techniques	Find patches for vulnerabilities Identify optimal alternatives to patching	Intelligence knowledge base with mitigation recommendations
Communication with Risk Managers and System Administrators	Identify high risk systems that need to be monitored until remediation is complete	Intelligence knowledge base Threat analysis reports customized for the industry or enterprise

How Cyber Threat Intelligence Helps

1. Understanding the Relevance and Severity of Vulnerabilities

Cyber threat intelligence can connect vulnerabilities with threat actors, their tactics, techniques and procedures (TTPs), and their targets. This information helps vulnerability management analysts determine which vulnerabilities affect the systems and software in the enterprise, and which are most likely to be exploited by attackers targeting their industry and region.

2. Information on Exploits and Exploit Kits

Researchers at cyber threat intelligence firms track exploits and exploit kits announced, discussed and offered for sale on the "dark web" frequented by hackers and cybercriminals. Vulnerabilities for which effective exploit kits are available are much more likely to be used in the immediate future. This information tells vulnerability management analysts which vulnerabilities need to be patched or mitigated immediately, and which are less urgent.

3. Mitigation Techniques

Cyber threat intelligence knowledge bases include data on patches that address specific vulnerabilities. They also contain information on mitigation techniques that can be employed when patches are not available or will take too long to deploy. Mitigation techniques can include creating rules for firewalls, application firewalls, and intrusion prevention systems, as well as changing the configurations of vulnerable systems, strengthening and enforcing access and password policies, and increasing monitoring of vulnerable systems and applications.

4. Clarity to Assess Business Risk

Cyber threat intelligence can provide descriptions of how vulnerabilities can be exploited as part of advanced attacks, and when combined with business context (local analyst for example), it can help assess a company's business risk. Those descriptions help analysts and administrators communicate with IT and business unit management in terms of business impact, and also about which systems need to be monitored until patching and remediation are complete.

The Bottom Line

Cyber threat intelligence can help your vulnerability management analysts:

- Better understand how and by whom vulnerabilities are likely to be used.
- Reduce risk to the business by better prioritizing vulnerabilities based on real threats to the industry and enterprise, lack of offsetting security defenses and controls, and the availability of exploits.
- Understand and apply optimal mitigation techniques.
- Communicate in business terms with auditors, risk managers, and other IT groups about the risks created by vulnerabilities.

For more information on FireEye, visit:
www.FireEye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com