Threat Management: Time to Go Beyond Vulnerabilities

Refreshed 19 May 2020, Published 21 February 2019 - ID G00447572 - 5 min read

FOUNDATIONAL This research is reviewed periodically for accuracy.

By Analysts Information Risk Research Team

Initiatives:Technology, Information and Resilience Risk

On January 17th, 2019, Troy Hunt announced his discovery of 773 million breached records. The discovery starkly illustrates the utter failure of vulnerability management to prevent — or even appropriately reduce — breaches. Leading CISOs recognize the current threat landscape requires a formally defined approach to managing threats, not just vulnerabilities.

On January 17 th, 2019, Troy Hunt announced his discovery of 773 million breached records. The data cache — dubbed Collection #1 — likely derives from multiple breaches over the past few years.

Collection #1 starkly illustrates the fact that vulnerability management is failing. Breach, after breach, after breach occurs regardless of Security's best efforts to manage vulnerabilities to an acceptable level.

Leading CISOs recognize the need for a formally defined approach to managing threats, not just vulnerabilities. These CISOs first define a formal threat management program and then iteratively mature the program over time. Managing threats — not just vulnerabilities — lets Security proactively protect, detect, and respond controls before threats are fully realized.

Defining Threat Management

Some CISOs use the combined term "vulnerability and threat management," but it's clarifying to consider threat management and vulnerability management as distinct activities.

> "*Threat Management: Collecting, processing, and using knowledge of threats facing the organization to proactively improve protect, detect, and respond controls before threats are fully realized.*"
>
> — ,

Threat management stands in contrast to **vulnerability management**, which focuses on mitigating known vulnerabilities — mainly through patching and updating controls.

Five Activities Within Threat Management

A threat management program consists of three core and two additional activities (figure 1).

Figure 1: Activities Within a Threat Management Program

Core Activities			Additional Activities	
Threat Intelligence	**Threat Modeling**	**Security Analytics**	**Hunting**	**Campaign Tracking**
Collecting and combining threat intelligence to gain deeper knowledge of adversaries' methods and intentions; these efforts encompass both technical and strategic intelligence, and they often draw from multiple risk disciplines.	Using the knowledge of vulnerabilities, adversaries, and the business to inform an understanding of how threats might affect the organization before those threats are actually realized	Acquiring, storing, and correlating large, diverse datasets to gain insight that helps achieve security and business objectives	Dedicating individuals within Security who use threat models and technical expertise to develop and validate new detection logic and scale these efforts using analytics and automation	Investigating past attacks and threat intelligence to sufficiently attribute, connect, and track attackers' campaigns against the organization; these efforts can reveal attackers' identities, locations, motives, methods, and objectives.

Source: CEB analysis.

A formally defined threat management program consists of three core activities: threat intelligence, threat modeling, and security analytics. Together, these three capabilities are required to proactively improve protect, detect, and respond controls before threats are fully realized:

- **Threat Intelligence** — Collecting and combining information to gain deeper knowledge of adversaries' methods and intentions.
  Intelligence sources include third-party indicator of comprise (IOC) feeds, Information Sharing and Analytics Centers (ISACs), news sources (e.g., our Daily Security Briefing), government agencies, and other corporate functions such as Legal, HR, Physical Security, or PR.

- **Threat Modeling** — Using the knowledge of vulnerabilities, adversaries, and the business to inform an understanding of how threats might affect the organization before those threats are actually realized.
  Common threat modeling methodologies include Microsoft's STRIDE Threat Model and DREAD risk rating model, Lockheed Martin's IDDIL-ATC Methodology, and other approaches.

- **Security Analytics** — Acquiring, storing, and correlating large, diverse datasets to gain insight that helps achieve security and business objectives.
  For example, security analytics can be used to detect signature-less attacks based on suspicious

activities, prevent customer fraud spanning multiple business units, or investigate the scope of current incidents by querying historical data.

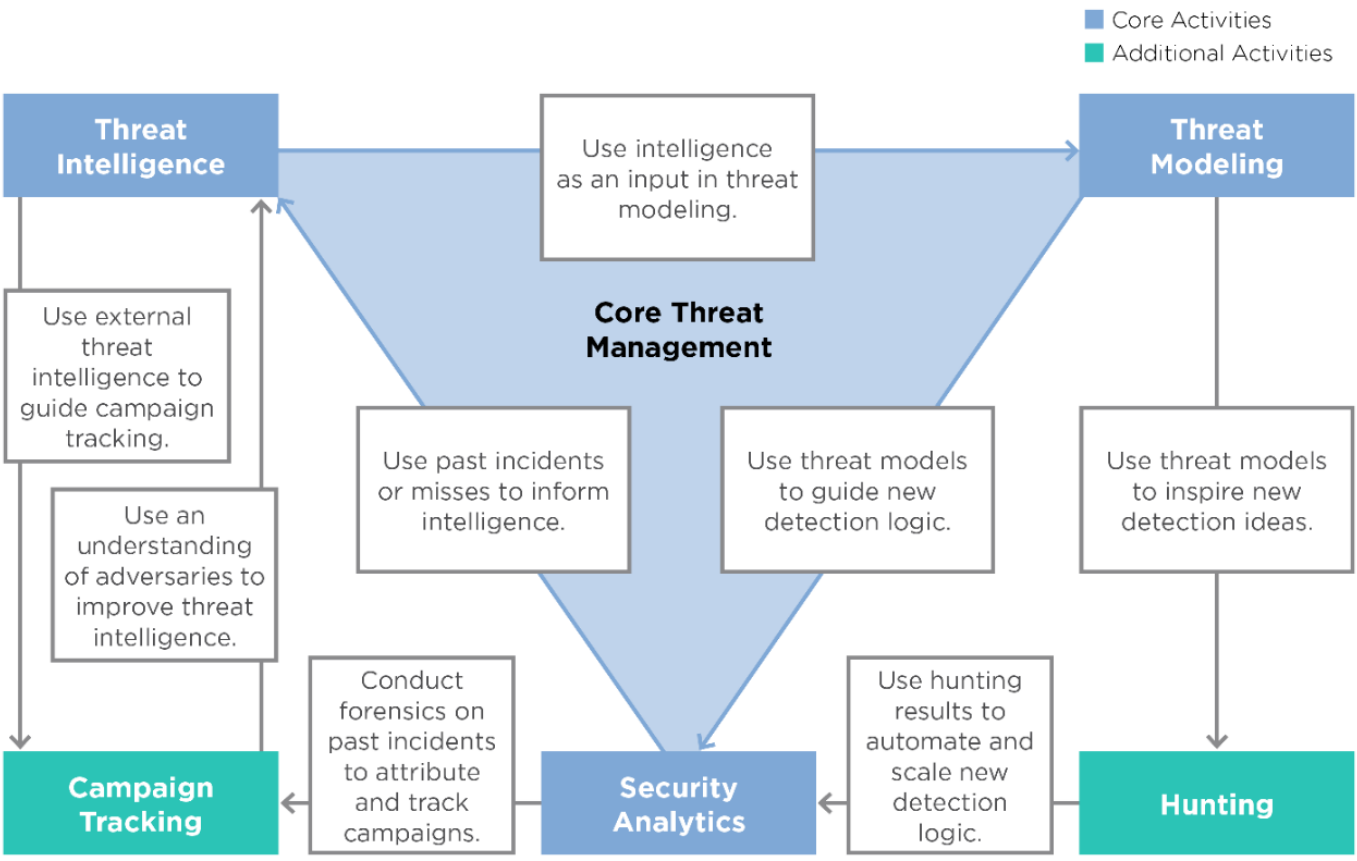
Our Security Analytics: Six Principles for Success research examines how leading organizations build and mature their security analytics programs. This includes case profiles of ADP, Pfizer, and UnitedHealth Group.

Read our full Issue Explorer to learn about additional threat management activities.

Visualizing Threat Management in Action

Threat management capabilities are not siloed. Rather, each capability should be part of a connected series of processes that together constitute threat management. Leading CISOs aspire to more formally define threat management processes (figure 2) — not just improve each individual capability.

Figure 2: Key Processes in a Threat Management Program



Source: CEB analysis.

Understanding the Core Threat Management Process

The core threat management process works as follows:

- First, information Security collects and aggregates raw **threat intelligence** from internal and external sources, such as IOC feeds, ISACs, and other corporate functions.

- Second, this intelligence then feeds into a formal **threat modeling** exercise that combines threat intelligence with knowledge of vulnerabilities and the business to better understand how specific threats might affect the organization.
- Finally, Security uses a prioritized list of threats and their potential impacts to inspire and prioritize new **security analytics** threat detection ideas. This includes writing new detection logic, guiding data access needs, and even directing new investment in analytics initiatives. Detected incidents or new insights from security analytics then inform threat intelligence collection, thus completing a single rotation around the core threat management process.

Read our full Issue Explorer to learn about the processes and connections between threat management activities.

Conclusion: Manage Threats, Not Just Vulnerabilities

The best CISOs formally define a threat management program to better anticipate and manage threats facing the organization. Managing threats — not just vulnerabilities — lets Security proactively protect, detect, and respond controls before threats are fully realized.

Such a program consists of at least three core activities: threat intelligence, threat modeling, and security analytics. Some Information Security functions also include hunting and campaign tracking in threat management. Collectively, these capabilities help Information Security functions:

- prioritize controls that address actual threats,
- detect incidents faster, and
- make threat intelligence more actionable to the organization.

Threat management also informs a range of security activities such as vulnerability management, strategic planning, employee awareness, and board reporting.

Recommended by the Authors

- Formally Defining Security's Threat Management Program
  Learn how leading CISOs define, run, and mature threat management programs.
- Security Analytics: Six Principles for Success
  Build Security's analytics program to detect threats while avoiding common and costly pitfalls.

by William Candrick

Recommended For You

Getting Serious About Insider Threats

GDPR Is Starting to Get Teeth

How Disinformation-as-a-Service Affects You

5 Ways to Keep your Company Safe This Thanksgiving

16 Tips to Enhance Your IT Disaster Recovery Program