WEBINAR SUMMARY

October 1, 2020

Heroku AbuseOps: Low-Value Indicators for High-Value Decisions

Spencer Cureton, Abuse Engineer, Salesforce
Allan Stojanovic, Abuse Engineer, Salesforce
Lori Smith, Product Marketing, Trend Micro

KEY TAKEAWAYS

- Salesforce uses Heroku to identify low-value indicators of abuse.
- Devaluation of loot and bad actor demotivation are the ultimate hunt goals.
- Lessons learned: Follow guiding philosophies and focus on the business.
- Trend Micro XDR enables quick security issue identification and response.

in partnership with

OVERVIEW

Traditionally, cybersecurity is interested in prevention, governance, and compliance. Abuse operations takes a wider view of the environment, looking for misuse, abuse, malice, and crime. Both security analysts and abuse engineers benefit from low-value indicators that, when combined with other indicators, identify likely problem areas.

The Salesforce abuse operations team has implemented Heroku, a code development and deployment tool, to help abuse engineers identify and resolve problems. Security analysts can take advantage of a tool built specifically with extended threat detection and response in mind: Trend Micro XDR.

CONTEXT

Spencer Cureton and Allan Stojanovic discussed how Salesforce's abuse operations team identifies and responds to abuse of the company's solution. Lori Smith discussed similarities between abuse operations and cybersecurity, and how Trend Micro XDR can help security analysts quickly identify and respond to threats.

KEY TAKEAWAYS

Salesforce uses Heroku to identify low-value indicators of abuse.

Salesforce uses Heroku to identify suspicious data that can indicate system security problems. Most initial indicators are low value; on their own they don't have enough context to support decision making, but combined with other indicators, they help identify likely problems.

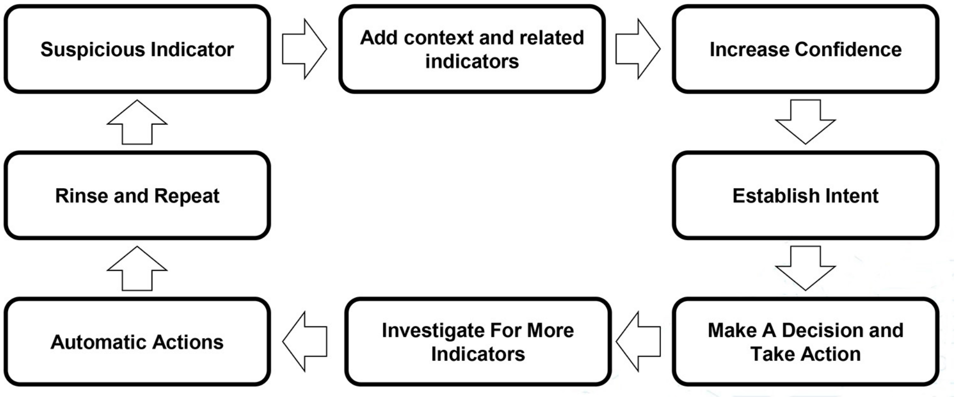
Abuse engineers begin the hunt for "badness" by looking at data as it builds on top of these indicators so they can resolve the current issue and prevent future similar problems.

Hunting for badness: Moving from low-value indicators to resolution and prevention	
1. Identify suspicious indicators	Derived from a combination of user-supplied data and data about that data. Most indicators are low value to start.
2. Add context	Using starting indicators, form a hypothesis about the intent of the actor and look for related indicators to prove or disprove the hypothesis. A collection of related low-value indicators becomes a good footprint for malicious activity.
3. Increase confidence	Ask "What else is going on?" and look for more indicators to further support the hypothesis.
4. Establish intent	Determine what the actor is trying to do. For bad actors seen in the past, determine what they are trying to do before they do it.
5. Make a decision and take action	Use the data and indicators to determine the path forward: – If the intent is bad, follow company policies for suspending or deleting the user or the application or escalating to legal or law enforcement. – If the intent is not bad, add the user and application to watch lists, allow lists, and other lists as necessary, and log as a false positive as appropriate. – If the intent is undetermined, do nothing and reassess the situation if or when it happens again.

Hunting for badness: Moving from low-value indicators to resolution and prevention	
6. Investigate for more indicators	Determine how widespread the activity is by retroactively looking at events to determine if they were related. This can identify additional accounts or applications that are also part of the abuse.
7. Automate	Automate to reduce the amount of manual work that occurs: – Automate the detection, collection of indicators, and action taken. – Automatically action the footprint retroactively. – Alert on a subset of activity. – Log actions by indicator for future consideration.

Once the automation phase is complete, the cycle begins again, continuously evaluating indicators to determine the potential for threat.

Figure 1: Hunting for abuse is cyclical


Suspicious Indicator
Add context and related indicators
Increase Confidence
Rinse and Repeat
Establish Intent
Automatic Actions
Investigate For More Indicators
Make A Decision and Take Action

What is Heroku?

Heroku is a container-based cloud platform-as-a-service (PaaS) that enables developers to build, run, and scale applications entirely in the cloud. The easy-to-use platform allows developers to focus on the design and craft of applications, so they can move quickly from idea to online application.

Devaluation of loot and bad actor demotivation are the ultimate hunt goals.

The ultimate goal of hunting abuse is to discourage bad actors from abusing the system again. Chasing off these abusers can be done by making loot less valuable and by using tactics and tools that demotivate the bad actors.

Hardening the platform makes it more difficult—and costlier—for bad actors to collect and use the loot, information, or systems they have collected. Resetting stolen passwords and reporting stolen credit cards make both unusable. Choking the central processing unit speed on a breached system slows down crypto-mining processes to the point where they provide no value. Forcing bad actors to rebuild pathways into the systems can ultimately cost more than the benefits a system can offer.

> Since our ultimate goal is to make loot less desirable without affecting legitimate customers, we really look to break [bad actor] spirits, as opposed to just their code.
>
> *Allan Stojanovic*

Lessons learned: Follow guiding philosophies and focus on the business.

Along with using Heroku, the Salesforce Abuse Operations team has learned that following a set of guiding philosophies, as well as keeping their focus on the business and its needs, has helped them keep up with the abuse their systems face.

Three key guiding philosophies are:

- **Relentless incrementalism.** Move within agility, fix one thing at a time, and fix it well.
- **Non-repetition.** Never see the same abuse pattern twice. This is the closest thing to prevention.
- **Hyper-automation.** Remove manual and system toil to enable relentless incrementalism and non-repetition. Automation gets the right information in front of an analyst quickly.

The team also focuses on understanding the business they serve and ensuring they are supporting the work the company does.

Three key guiding ideas behind serving the business to detect abuse are:

- **Break down silos.** Know teams, their data, and their alerts. This leads to identification of more indicators, improved situational awareness, and the ability to provide feedback to the business.
- **“Push left” to move security to earlier in the development process.** This includes hardening the platform, ultimately increasing the cost for abusers, devaluing loot, and demotivating abusers.
- **Focus on customer support and consider everyone a customer until they are determined not to be one (and instead deemed a bad actor/abuser).**

> We’re not here for the sake of technology or security whack-a-mole, even though for us it’s a lot of fun. We’re here to serve the business.
>
> *Spencer Cureton*

Trend Micro XDR enables quick security issue identification and response.

Security analysts are faced with numerous alerts and indicators from multiple systems across the organization, including endpoints, email, clouds, and network. Trend Micro XDR helps cybersecurity analysts work through the data and find and respond to threats quickly.

> It's no surprise that security teams are overwhelmed with alerts getting triggered by different solutions. There's a lot of visibility, and not so much insight.
>
> *Lori Smith*

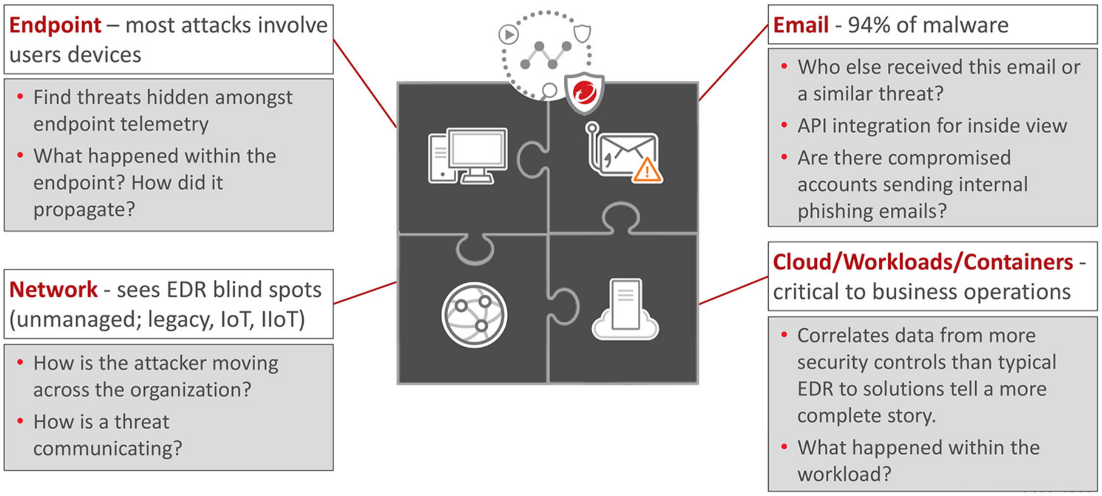
Trend Micro XDR understands that when hunting for threats and bad actors, cybersecurity professionals are using the same principles that abuse operations personnel use.

Shared abuse operations and cybersecurity threat principles when hunting for badness

- Use low-value indicators for high-value detections.
- Gather suspicious indicators and add context to increase the confidence of detection.
- Break down the silos to make the unobvious clear.

XDR breaks down the various silos across the business and builds a story an analyst can use to understand the potential threats and how to react. XDR goes beyond the single vector approach, allowing security analysts to quickly detect and respond to threats and attacks in their environment.

Figure 2: Each XDR Piece Adds Value



Endpoint – most attacks involve users devices

- Find threats hidden amongst endpoint telemetry
- What happened within the endpoint? How did it propagate?

Network - sees EDR blind spots (unmanaged; legacy, IoT, IIoT)

- How is the attacker moving across the organization?
- How is a threat communicating?

Email - 94% of malware

- Who else received this email or a similar threat?
- API integration for inside view
- Are there compromised accounts sending internal phishing emails?

Cloud/Workloads/Containers - critical to business operations

- Correlates data from more security controls than typical EDR to solutions tell a more complete story.
- What happened within the workload?

Learn More

www.trendmicro.com/XDR

BIOGRAPHIES

Spencer Cureton

Abuse Engineer, Salesforce

Spencer Cureton has a background in electrical engineering and started his career working in industrial control systems, providing services from support to live plant migrations. He managed to get into information security in 2016 and enjoys life as an Internet Mall Cop working on the Abuse Operations team at Heroku.

Allan Stojanovic

Abuse Engineer, Salesforce

Allan Stojanovic has survived IT for over 25 years. He has worked in nearly every vertical doing may different roles, mostly in the Information Security field. A jack of all trades, he tries to know a little bit about everything, and is a self-proclaimed expert at nothing.

Lori Smith

Product Marketing, Trend Micro

Lori Smith is part of the global product marketing team at Trend Micro. These days, Lori lives and breathes Trend Micro XDR, and is excited by her small part in helping to build an understanding and market momentum for extended detection and response. Boggled by the talents and expectations of security analysts, Lori has become a champion for trying to make their lives easier with tools that can solve their most pressing challenges. In those moments when Lori's not talking shop, she enjoys travel, starting (but maybe not finishing) home projects, and a good competitive game night! Reach out to Lori Smith at lori_smith@trendmicro.com