ISMG EXECUTIVE ROUNDTABLE
Sponsored by Cybereason

Indicators of Behavior: The New Way to Detect Advanced Attacks

Agenda

6:00 – 6:30 p.m.
Registration, Networking, Beer & Wine Service

6:30 – 6:45 p.m.
Introductions and Opening Remarks

- **Tom Field**, SVP Editorial, Information Security Media Group
- **Sam Curry**, Chief Security Officer, Cybereason

6:45 – 8:30 p.m.
Roundtable Discussion

8:30 p.m.
Program Concludes

ISMG INFORMATION SECURITY MEDIA GROUP

cybereason

Introduction

For many cybercrime investigators, it's all about indicators of compromise – hashes, URLs and other crime scene artifacts that can be gathered and compared to evidence from other crime scenes to determine what has occurred.

But what if you were to shift away from gathering evidence and toward cataloging behaviors – indicators of behavior - what people, applications and systems are doing that could indicate an attack is ongoing or imminent?

How does one make a strategic shift from IoC to IoB? What tools and skills are needed? What new standards and language must be developed?

If you're looking for answers to these questions, then welcome to this exclusive executive roundtable on **Indicators of Behavior: The New Way to Detect Advanced Attacks.**

Guided by insight from Sam Curry, CSO at event sponsor Cybereason, this invitation-only dinner will feature a case study and insights about IoB, and it will draw from the experiences of the attendees who will offer their views strategies to detect advanced cyberattacks. Among the discussion topics:

- What are indicators of behavior, and how must one gather and analyze them in proper context?
- How does your organization currently separate signal from noise when it comes to detection?
- What are your barriers – technical and nontechnical – to making this shift from evidence gathering to behavior monitoring?

You'll have the opportunity to discuss IoB with a handful of senior executives and market leaders in an informal, closed-door setting, from which you will emerge with new strategies and solutions you can immediately put to work.

Discussion Points

Among the questions to be presented for open discourse:

- How does your organization currently detect incidents and attacks?
- How effective do you believe these detection methods are?
- How does your organization currently separate signal from noise when it comes to detection?
- Where do you see your biggest detection gaps?
- To what degree are you currently focused on indicators of compromise vs. indicators of behavior?
- What are your barriers – technical and nontechnical – to making the shift from evidence gathering to behavior monitoring?
- What investments will you make in the coming year to improve detection?

About the Expert

Joining our discussion today to share the latest insights and case studies is:

Sam Curry

Chief Security Officer
Cybereason

Curry brings over 25 years of experience in security, with a focus on deep technology and solving practitioner problems, to his role as Cybereason CSO. He was previously CTO and CSO at Arbor Networks, senior vice president of engineering and CISO at Microstrategy, and held a number of significant senior roles at RSA, the Security Division of EMC. He has done work on national defense, public policy and establishing standards and protocols in security. He also founded two successful startups and is on three security organization boards. He is a frequent speaker appearing on BBC, CNN, MSNBC and other media outlets, a published author, a highly patented inventor and a widely quoted security expert.

About Cybereason
Cybereason, creators of the leading Cyber Defense Platform, gives the advantage back to the defender through a completely new approach to cybersecurity. Cybereason offers endpoint detection and response (EDR), next-generation antivirus (NGAV), and active monitoring services, all powered by its cross-machine correlation engine. The Cybereason suite of products gives you unmatched visibility, increases analyst efficiency and effectiveness, and reduces security risk. Cybereason is privately held, having raised $189 million from top-tier VCs, and is headquartered in Boston, with offices in London, Tel Aviv, and Tokyo.

About the Moderator

Leading our discussion today is:

Tom Field

SVP Editorial
Information Security Media Group

Field is an award-winning journalist with over 30 years of experience in newspapers, magazines, books, events and electronic media. A veteran community journalist with extensive business/technology and international reporting experience, Field joined ISMG in 2007 and currently oversees the editorial operations for all of ISMG's global media properties. An accomplished public speaker, Field has developed and moderated scores of podcasts, webcasts, roundtables and conferences and has appeared at the RSA Conference and on various C-SPAN, The History Channel and Travel Channel television programs.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

CONTEXT

Indicators of Behavior: The New Way to Detect Advanced Attacks

Q&A with Sam Curry of Cybereason

NOTE: In advance of this event, ISMG's Tom Field spoke about indicators of behavior with Sam Curry of Cybereason. Here is an excerpt of that conversation.

A Better Way

TOM FIELD: Why indicators of behavior?

SAM CURRY: Indicators of behavior will stand out regardless of how the bad guys act. They have the most longevity and are the hardest to dodge. They aren't a panacea, but they are where we need to go next.

Lessons Learned

FIELD: What have you learned about IoB from your own case studies and research?

CURRY: Classic telemetry and data structures don't tell us anything about behaviors or context. In an SIEM, it all has to be re-inferred and derived at great expense and difficulty. IoBs can be recorded in a directory, but they generally aren't. Some EDR products are doing it, and some network capture devices are recording a subset. IoBs persist regardless of whether rolling your own malware or living off the land.

The most interesting thing happens when we get out of the fetish of being able to trust something small and build on that — this trusted machine plus that trusted machine equal a trusted network. That's flawed. Instead of going micro-to-macro, we can look at chains of behaviors and go macro to micro. Go from detecting the kill chain to fixing the machine and not the other way around.

FIELD: How does this approach distinguish itself from indicators of compromise and indicators of attack?

CURRY: Locard's principle says "just get all the clues" and then work with those. This is slow and painful. The most recent attacks don't use the same compiles (and therefore different hashes) of the same attack in the same kill chain. If an IoC won't help you find two instances of the same thing in the same attack sequence, how will it help find it anywhere else? That's broken. IoBs on the other hand, if instrumented, will find the same nuances and chains of behavior concurrently, everywhere in an environment.

Sam Curry

Necessary Tools

FIELD: What are the tools and skills to enable the IoB approach?

CURRY: There are a lot. It could start with new telemetry recommendations, how to infer behavior in legacy telemetry and new data structures. Working straight on behaviors means new analytics and applications of machine learning.

I remember studying electromagnetism years ago and then finding Maxwell's equations. I was angry at first for having to learn the hard way and then finding the shortcut for a year of my life. However, knowing the basics did help me and continue to be useful, and the same is true of IoCs. Don't throw them out, but really, our energy in research, protocols, tools and so on should move on.

The Obstacles

FIELD: What are the obstacles – technical and non-technical – in the road?

CURRY: We have no sharing protocols for these yet or agreed on standards. We have a massive industry that pumps out IoCs that is a vested interest. We have technical hurdles and cultural ones to re-gear and develop this, but it has to happen if we're to accelerate the rate of improvement in defender capabilities. For the time being, the gap only widens.

"Much as in behavioral psychology, where we understand that we can't get into the heads of psychological pathology victims to understand motivation and we can't just look for physiological answers, we need to make the development of behavioral cybersecurity a new science and advance it."

Cybereason's Role

FIELD: How is Cybereason helping customers make this transition?

CURRY: At the moment, I'll pat us on the back for using and instrumenting behaviors. I will also give us a sound smack in the face for not advancing standards enough here or championing the cause of behavioral analysis.

Much as in behavioral psychology, where we understand that we can't get into the heads of psychological pathology victims to understand motivation and we can't just look for physiological answers, we need to make the development of behavioral cybersecurity a new science and advance it. ■

Notes

Notes

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach Prevention. Response. Notification. TODAY

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io