CYBER RESILIENCE THINK TANK

# THREAT INTELLIGENCE:

## Far-fetched Idea or Must-have Security Tactic? How Every CISO Can Make it a Priority

SPONSORED BY

mimecast

# CONTENTS

# THREAT INTELLIGENCE ISN'T JUST FOR THE ONE-PERCENT

The truth is, the definition of "threat intelligence" will likely vary depending on who you ask. After all, there are a lot of factors at play. Things like budget, resources, skillset and industry all have great impact on how organizations approach threat intelligence—or whether they prioritize it at all. Though the technical definition can change, one factor remains constant: If threat intelligence isn't part of your cyber resilience strategy in some capacity, you have a massive gap on your hands. And you may be blindsided by a phishing attack, malware incident or worse.

Investing in third-party security vendors to manage data feeds will cover some gaps in your security strategy. But not everyone has the means to invest. Maybe it used to be okay to just accept this and fold. But today, you simply won't survive. Whether you're a large enterprise or a lean one, threat intelligence is the responsibility of every CISO. And budget isn't the only thing you need to be successful.

Here's how you can make threat intelligence a priority in your cyber resilience planning.

## BE ACTIONABLE.

Action. It's the thing that makes data useful to you. It's like a crystal ball for future threats, giving you a head-start on mitigating the bad stuff. Being actionable means understanding your data and using that information to increase your ability to be cyber resilient.

# THREAT INTELLIGENCE ISN'T JUST FOR THE ONE-PERCENT

So, when it comes to threat intelligence, where's all the action?

According to Stephen Ward, Chief Information Security Officer of a Fortune 100 financial institution, the security world is in a state of being reactive, and it needs to find the right balance of being reactive and proactive – to become actionable. "Good, actionable threat intelligence can tell you who is behind an attack, the tools and tactics used, and the who, how and what they're after. The contextual piece leads to true threat intelligence."

According to Marc French, Chief Trust Officer at Mimecast, true intelligence means turning information into action. "You don't truly get intelligence unless you get something on the other side."

Malcolm Harkins, Chief Security and Trust Officer at Cylance said, "As a security industry, we have to move away from being in a constant state of reaction. I want to minimize damage to my organization – I want prevention."

He continued, "I've always looked at threat intelligence broadly: What's my open source intelligence? What's my human intelligence? What's my signals intelligence? I want it all, because it all matters."

> ***As a security industry,*** *we have to move away from being in a constant state of reaction."*

**Malcolm Harkins**
CHIEF SECURITY AND TRUST OFFICER
CYLANCE

# THREAT INTELLIGENCE ISN'T JUST FOR THE ONE-PERCENT

## BE TACTICAL.

According to Gary Hayslip, Chief Information Security Officer at Webroot, the use of threat intelligence is a process that assists CISOs and security teams to better deploy their security controls and prioritize which known vulnerabilities should be mitigated first.

"Without using threat intelligence, you expend more time and resources, and you will miss issues that will leave your organization exposed to business-impacting risk," he said. "Through the use of threat intelligence, I can train my staff on incident response that pertains to our infrastructure, services and portfolio, making better use of my limited resources. I can also use this information to educate my executive staff and provide context into our current risk baseline and the adversaries that may look to interrupt our operations."

"Blocking and tackling threats is critical. It's something you just need to do. You need some form of threat data and a tactical intelligence strategy. Otherwise, you will let bad stuff in," said French.

> ***Without using threat intelligence,*** *you expend more time and resources, and you will miss issues that will leave your organization exposed to business-impacting risk ..."*

**Gary Hayslip**
CISO
WEBROOT

# THREAT INTELLIGENCE ISN'T JUST FOR THE ONE-PERCENT

## BEWARE OF DATA EXHAUST.

According to Ward, threat intelligence tends to produce a lot of data alerts that are irrelevant, and as a result, bog down operations teams and create exhaust. "We're still talking about bad URLs and hashes – those days are over. We should be focusing on the entire story of how something is done," he said.

Unfortunately, Ward said this is a problem outside the Fortune 250 companies who are getting the budgets to build hybrid disciplines. "If you throw money at threat intelligence, you'll do well at it. If you don't, it won't be a priority."

Big budget or not, any CISO can make threat intelligence a priority and learn how to focus on only the data that matters – data that will help mitigate future risks.

> ***We're still talking about bad URLs and hashes –*** *those days are over. We should be focusing on the entire story of how something is done."*

**Stephen Ward**
CISO
FORTUNE 100 FINANCIAL INSTITUTION

# NO BUDGET? NO PROBLEM.

## FIVE TIPS TO AVOID DATA EXHAUST

1. **FOCUS ON YOU FIRST.** Some CISOs don't have the budget to share, and that's okay. The few are here to protect the many – this is the moral obligation of bigger companies. Don't worry about sharing if you're a lean company.

2. **BE SELECTIVE** about the intelligence feeds you consume, whether they are paid or free.

3. **FOCUS ON ACTIONABLE DATA.** Data feeds can be exhausting. If only 10% of the information is valuable, going through the other 90% that doesn't matter will kill morale.

4. **AUTOMATE.** The goal is to have as much automation as you can to feed into existing technology to get good alerts.

5. **BE SMART ABOUT BUILDING REPORTS FOR EXECUTIVES.** The Board and executives want to know the details about threat data. Contextualizing and briefing them makes the money flow in and builds the case for making good business decisions.

# THREAT INTELLIGENCE ISN'T JUST FOR THE ONE-PERCENT

## USE OPEN APIs AND KNOWN THREAT PATTERNS.

Threat intelligence may be more accessible that you think. The most effective organizations know how to fuse the data they have in-house with the open APIs in different technology solutions to produce meaningful intelligence. Your own operations are likely the best place to start: This could be mining internal information that your security and operations teams have from experiences with previous vulnerabilities, malware incidents and data breaches. If properly documented, this information can provide you with meaningful content on how your enterprise networks were compromised, and if there were any recurring methodologies that worked against your deployed security program.

"This internal information, for most organizations, will probably be collected in some type of log management system or SIEM platform. If this information on incidents can be collected and used to properly document a history of attack paths, malware, vulnerabilities, and other patterns, it can provide invaluable insight into security gaps that can be remediated or help the company identify business processes or legacy issues that need to be addressed to prevent further compromise," said Hayslip.

Taylor Lehman, Chief Information Security Officer at Wellforce said, "I find that most of the intelligence I need is already in my infrastructure. It's the incidents that occur daily, the rate at which they are occurring, and who they are targeting. If you step back and classify your incidents in this context, you could learn a lot about what people want from you."

He continued, "It becomes a data analysis game, where you cluster incidents into interesting patterns then look at them to determine: What are the exploits? What's getting through and what isn't? And what countries are becoming more active?"

> ***I find that most of the intelligence*** *I need is already in my infrastructure."*

**Taylor Lehmann**
CISO
WELLFORCE

# **CHECKLIST:** HOW TO PROVE VALUE WITH LITTLE (OR NO) BUDGET

The struggle to prove value is real. Lack of budget, not enough staff and a skillset deficiency make it hard to build a solid business case for critical, but intangible, things like threat intelligence. But this doesn't mean it's a lost cause.

**Here are four ways to prove the value of threat intelligence to your executive team and the Board:**

- **CONDUCT AN INVENTORY OF ALL HARDWARE, SOFTWARE, CLOUD SERVICES AND DATA TYPES** to better understand which ones are required to keep the business running. Use this prioritized list to establish a data governance program, prioritize which vulnerabilities need to be remediated first and create/train your incident response and business continuity teams with a focus on the items in your prioritized list.

- **START MAINTAINING AN INCIDENT DATABASE OF INTERNAL ISSUES** from phishing emails to malware infections. Keep this up-to-date, and over time, you can use it for analysis to see what issues are common to improve the security stack, as well as improve training for employees to better prepare them for security incidents.

- **USE OPEN-SOURCE THREAT INTELLIGENCE** that is specific to your industry and technology portfolio with the understanding that it may not be current, but at least it's a start.

- **KNOW WHAT PARTS OF YOUR SECURITY STACK HAVE INTELLIGENCE FEEDS AND TURN THEM ON.** Keep a log of all the malware and threats that are blocked/remediated so you're able to show over time the amount of bad traffic that is removed, and the types of malware targeting the organization.

# TO OUTSOURCE OR NOT TO OUTSOURCE. YOU DECIDE.

Budget within an organization dictates how – and whether-or-not – threat intelligence is being performed. An organization with a big budget can create their own group and get augmentation from a third party. On the other hand, a small-to-no-budget will leave an organization to struggle.

## TWO SCENARIOS: BIG ENTERPRISE VERSUS LEAN.

"A big company with big budget and a lot of resources typically has entire teams dedicated to threat intelligence," said Ward. "The in-house team pulls from the feed what they know is contextual and actionable. This requires a lot of money and a lot of effort. Then you need to decide how to communicate this information to the business. Threat intelligence is very valuable. The more people within the organization that have this information, the more valuable it becomes. If it sits only in the security team, it becomes far less valuable."

Ward continued, "If you're lean, you have to decide if you're going to dedicate one person to Google information, create situational awareness, analyze feeds (free and paid), look at the information and learn how to create firewalls and blocks. Most companies fall into the latter. Most outsource threat intelligence."

# TO OUTSOURCE OR NOT TO OUTSOURCE. YOU DECIDE.

## MOST THREAT INTELLIGENCE IS OUTSOURCED.

Maurice Stebila, Chief Information Security Officer at HARMAN by Samsung said, "I have various cybersecurity partners collecting intelligence on my behalf. All of their tools I have protecting the cloud, the network, the endpoint – they've taken those feeds and built them into their products so if there's a vulnerability, it's going to be blocked and captured. And I'll get an alert."

Stebila continued, "I really do expect my vendors to take all the threat intelligence, build it into their products, and integrate my different technologies so that I can protect my infrastructure."

Sue Lapierre, Vice President and Information Security Officer at Prologis said, "We are a public, $2.5 billion company, but we are a very lean security team. So, I have to rely on the vendors I have. I expect my security vendors to try to be the best, and to find the next threats that are out there."

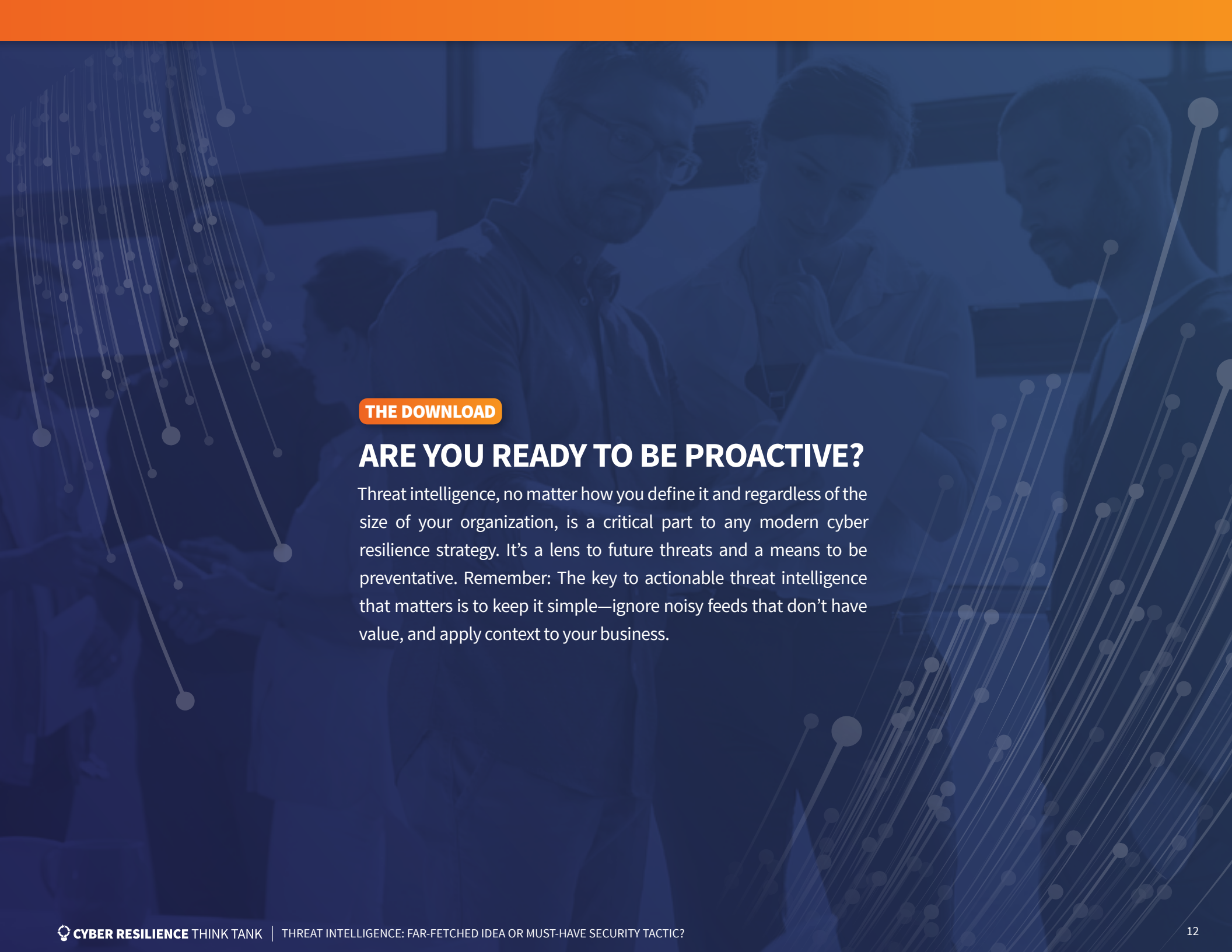
"I don't have the resources or the budget to do it myself. And I don't believe the ROI to hire a couple of threat intelligence people is going to be there. My ROI is better with contracting with security vendors," she said.

French noted only the organizations with the most sophisticated environments are performing threat intelligence in-house. "The ability to get true analysts is strained, it's a role that's hard to fill. In my opinion, intelligence is a mindset; not what a technical person does."

"However, there are cons to using a third-party vendor. You have no idea who is sitting on the other side – do they even know what they're doing? I can't tell if my vendor's intelligence team is good or bad – there's no vetting. There is no process for taking the intelligence process from fledgling to finished with third parties," he said.

> ***I expect my vendors to take all the threat intelligence,*** *build it into their products, and integrate my different technologies so that I can protect my infrastructure."*

**MAURICE STEBILA**
CHIEF INFORMATION SECURITY OFFICER
HARMAN



THE DOWNLOAD

## ARE YOU READY TO BE PROACTIVE?

Threat intelligence, no matter how you define it and regardless of the size of your organization, is a critical part to any modern cyber resilience strategy. It's a lens to future threats and a means to be preventative. Remember: The key to actionable threat intelligence that matters is to keep it simple—ignore noisy feeds that don't have value, and apply context to your business.

# CYBER RESILIENCE THINK TANK

An independent group of global industry influencers dedicated to understanding the cyber resilience challenges facing organizations across the globe, and together, providing guidance on possible solutions.

**SAM CURRY**
CHIEF PRODUCT / SECURITY OFFICER
CYBEREASON

**JOSHUA DOUGLAS**
CHIEF INFORMATION SECURITY OFFICER
TRC COMPANIES

**MARC FRENCH**
CHIEF TRUST OFFICER
MIMECAST

**JASON GUNNOE**
CHIEF INFORMATION SECURITY OFFICER
BRIDGESTONE TIRES

**MALCOLM HARKINS**
CHIEF SECURITY & TRUST OFFICER
CYLANCE

**GARY HAYSLIP**
VICE PRESIDENT & CHIEF INFORMATION
SECURITY OFFICER, WEBROOT INC.

**SUE LAPIERRE**
VP, INFORMATION SECURITY OFFICER
PROLOGIS

**NATHAN LARSEN**
DIRECTOR OF IT
SINCLAIR OIL

**TAYLOR LEHMANN**
CHIEF INFORMATION SECURITY OFFICER
WELLFORCE

**MICHAEL PRICE**
CHIEF TECHNOLOGY OFFICER
ZEROFOX

**DANA SANCHEZ**
SENIOR INFORMATION
SECURITY ANALYST
PROLOGIS

**ARI SCHWARTZ**
MANAGING DIRECTOR OF
CYBERSECURITY SERVICES, VENABLE, LLC

**JAKUB (KUBA) SENDOR**
SOFTWARE ENGINEER
YELP

**MAURICE STEBILA**
CHIEF INFORMATION SECURITY OFFICER
HARMAN

**STEPHEN WARD**
CHIEF INFORMATION SECURITY OFFICER
FORTUNE 100 FINANCIAL INSTITUTION

**MATTHEW WINTER**
VP, GLOBAL MARCETING
AND BUSINESS DEVELOPENT
LOGRYTHM


# Ready to Strengthen Your Defense?

Learn More

Mimecast (NASDAQ: MIME) makes business email, web and data safer for thousands of customers and their millions of employees worldwide. Founded in 2003, the company's next-generation cloud-based security, cybersecurity awareness training, archiving and continuity services deliver comprehensive controls for email and web risk management.