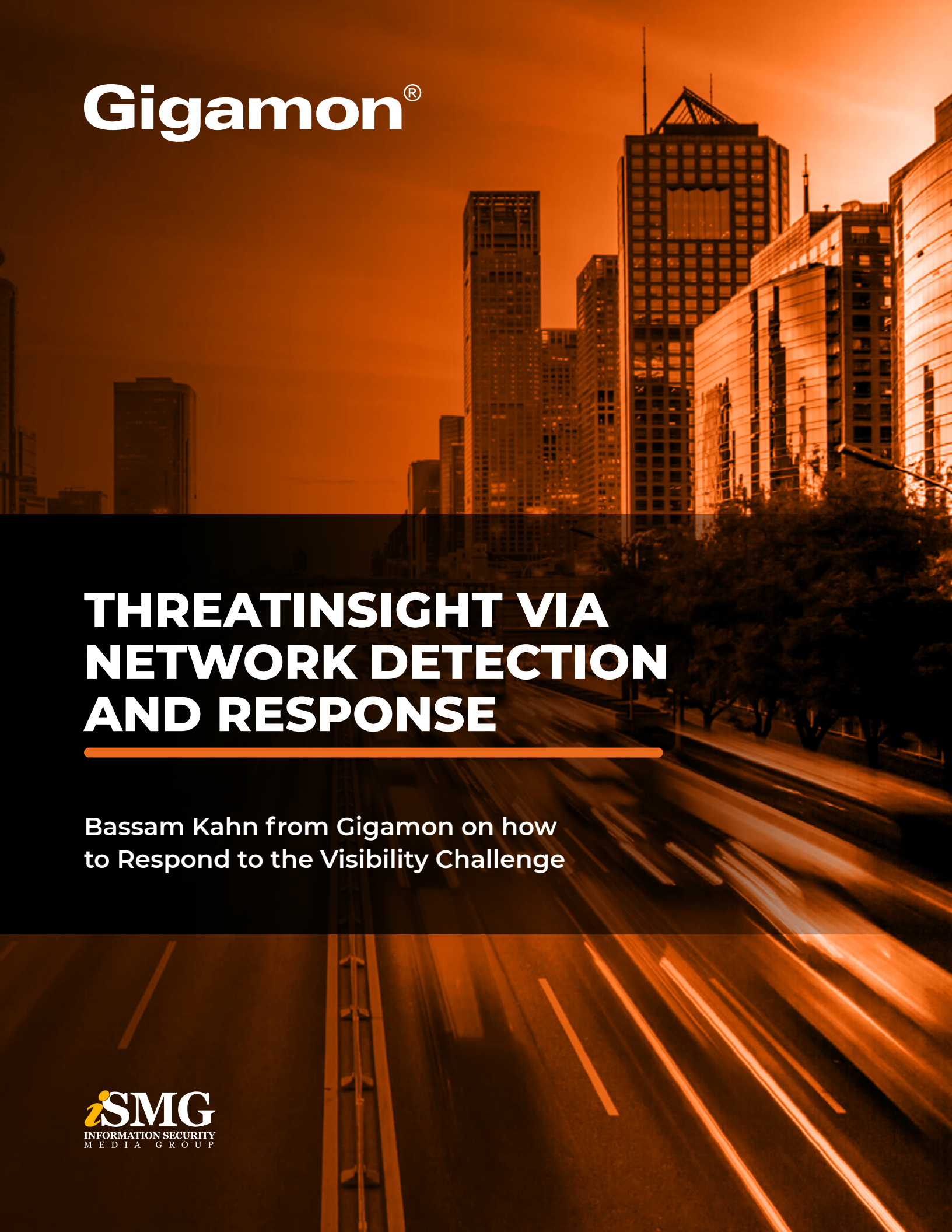


Gigamon®

THREATINSIGHT VIA NETWORK DETECTION AND RESPONSE

Bassam Kahn from Gigamon on how to Respond to the Visibility Challenge

ISMG
INFORMATION SECURITY
MEDIA GROUP

Bassam Khan

Khan is the vice president of product and technical marketing engineering, responsible for positioning and promoting company products and solutions and corporate and go-to-market strategy. He has 20 years of experience managing products for security, cloud and collaboration technology companies. Prior to Gigamon, he held executive positions at ControlUp, AppSense, PostPath, Cloudmark and Portal Software.

As enterprises adjust to the new threat landscape, how must they also adjust their approach to detection? Bassam Khan of Gigamon discusses the visibility challenge and the promise of new network detection and response solutions.

In a video interview with Information Security Media Group as part of its RSA Conference 2021 coverage, Khan discusses:

- Which threats are going undetected;
- Why common visibility tools miss the mark;
- The Gigamon ThreatINSIGHT approach to NDR.

THREAT TYPES

TOM FIELD: What types of threats are going through completely undetected today?

BASSAM KHAN: Many types of threats make it past the protection layers, including unauthorized attempts to access systems and

data, privilege escalations, insider threats, phishing, malware and targeted APT types. There is growth in the adoption of different types of tool sets for different types of attacks that wasn't there before. The ransomware that we've been seeing over the past couple of years has been built to conduct an enterprisewide attack rather than to attack individuals, because the payout is higher, particularly if the enterprise has cybersecurity insurance.

Some attack types are being recycled. For example, the first known widely spread ransomware was called the AIDS Trojan in 1989, the MS-DOS days. It would attach itself to the AUTOEXEC.BAT file, which reboots the machine. It had a counter that would increment every time the machine rebooted. And on the 90th reboot, the malware would kick in and rename all your files. When you paid the hackers $189, they would give you the code to restore the old file names back to the way it was. Waiting for the 90th reboot allowed your machine to act as a spreader for a long period of time.

All of malware since then has been instantaneously activated in encrypting your files until very recently, where it's trying to get to as many people from one organization as possible. So the loitering time goes up, which means you can apply detection technologies to an existing infrastructure, to see if that new ransomware that's using APT tools is trying to spread. The loitering time gives the defense team more time – maybe days or even months – to shut things down before the attack gets too prevalent.

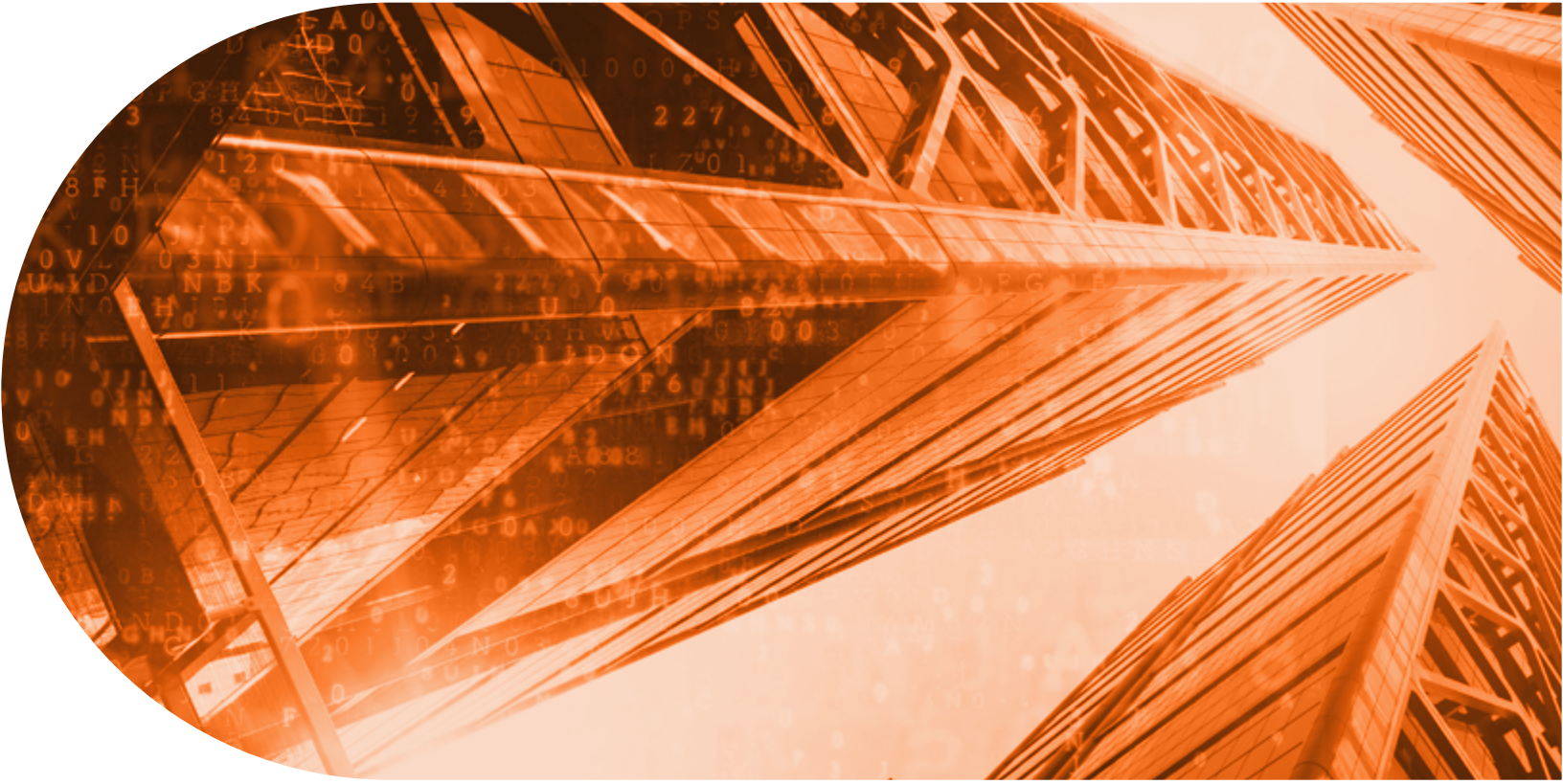
DETECTION CHALLENGES

FIELD: As enterprises adjust to this new threat landscape, how do they need to adjust their approach to detection?

KHAN: Attackers will get through any kind of prevention technologies and once they're in, they'll remain hidden. They'll carry out their mission – move around undetected, steal credentials, access systems, steal IP and exfiltrate data. The more advanced security teams have a very strong post-breach detection capability but SOCs that are not as advanced spend more time chasing phantom alerts from the frontline tools. They deal more with business interruptions and in the end, they have to deal with exfiltrated data and brand damage.

The less advanced organizations are alone, distracted, in the dark. They are alone because they don't get any outside help. They have to research every new attack that comes in. They are distracted because they spend a lot of time maintaining their systems, storage and servers, and fine-tuning and retuning based on new attacks. Analysts could be spending this precious time looking for threats. A Ponemom study showed that 43% of SOC analysts said their most time-consuming project is maintaining their systems. Less advanced organizations are in the dark because they don't have visibility into their environment and all the data in motion.

"ThreatINSIGHT has a lot of capability for advanced adversary detection. It uses a blend of machine learning and behavioral threat intel techniques for high-fidelity detections of hidden and emerging threats."



VISIBILITY TOOLS

FIELD: What tools are used for visibility, and why are they missing these threats?

KHAN: Most SOC teams have implemented the MITRE ATT&CK framework, which has many stages. But SIEM is a tool that's prevalent in every SOC that we talk to. Over the past five to 10 years, endpoint detection and response tools have taken a very strong foothold in SOCs as well. EDR tools are very powerful on the endpoint to identify, track and remediate for every stage of the attack. They are very important in the earlier attack stages. But there's a gap. The SIEM tool is getting its data from systems that let the attack through in the first place.

From an EDR perspective, there's a gap around hosts that are not being managed. We say, "All hosts, all traffic, all locations." What does that mean? All hosts means even hosts that are not managed, that don't have an EDR agent. That could be IoT devices, a surveillance camera, a printers or even a pump for a fish tank. All traffic includes traffic going in and out for north-south and east-west traversal. It includes not just all open traffic, but also encrypted traffic. We're seeing a steady increase in encryption by the good guys, but also by the bad guys, for both insertion as well as exfiltration.

All locations includes all of the different hosts and everything that's under view on-premises, but it could also mean private cloud, public cloud and even home usage. Detecting all hosts, all traffic and all locations for all data in motion is where a network detection and response, or NDR, tool becomes valuable. Along with EDR and SIEM, it forms the SOC visibility triad.

GIGAMON THREATINSIGHT

FIELD: What is Gigamon ThreatINSIGHT, and how does it approach detection differently within this triad?

KHAN: ThreatINSIGHT is a Guided-SaaS network detection and response solution. We describe it in terms of effectiveness, efficiency and expertise. Effectiveness has three components to it: visibility, fast detection and informed response. Visibility is super important. It covers north-south and east-west traffic and plain-text as well as encrypted traffic, all the way up to TLS 1.3, which is being used more by the good people and the adversaries as well.

ThreatINSIGHT has a lot of capability for advanced adversary detection. It uses a blend of machine learning and behavioral threat intel techniques for high-fidelity detections of hidden and emerging threats. Also, when we give you an alert about a threat, we put that threat into context and make all the rich data around that threat accessible and searchable. We base all our detection on enriched metadata and use omnisearch, a hyper-fast search engine that lets you go back in history and investigative exactly what happened. Our detection also includes threat-specific guidance for every alert that you get, to tell you what to do with that alert. It helps with triaging and investigations.

Next is efficiency. You have an EDR and a SIEM in place, and you're bringing in a network detection and response tool. You've got two choices: You can buy the software, install it, run it, customize it and optimize it. Or you can outsource it and have a managed security service provider, or MSSP, take care of everything for you.

Each approach has its pluses and minuses. If you build it yourself, you'll have full control over it. But you'll have to spend a lot of time maintaining the system and fine tuning it as attacks come in. You'll also be working alone in the dark, with just a single-funneled view into your environment. An MSSP, which has multiple customers, has seen attack campaigns happen and knows the tools that the adversaries are using across companies. But because it has many customers, it has a generic system, not built just for you.

At Gigamon, we have combined the best of both worlds. The platform is hosted, so you're not spending any time maintaining it and updating the OS. We take care of that for you in a SaaS-like environment that is optimized for your environment. As for expertise, Gigamon's product and threat experts are mostly former incident responders. They support your team's ongoing proficiency with handling attacks and help make sure deployment, configuration and visibility are always optimized. This is important because a network is not a static entity; it's always changing. Our experts also make sure that your SaaS environment updates are done and that your system is always available.

ThreatINSIGHT closes the gaps in the SOC visibility triad. It arms teams with an NDR that's designed for them, improves their effectiveness by removing distractions and provides expertise when it counts.

CUSTOMER BENEFITS

FIELD: You said ThreatINSIGHT is built by incident responders for incident responders. Share some examples of how your customers benefit from this.

KHAN: Our customers, both the large and midsize enterprises, say they appreciate having guidance to detect active threats. We track threats remotely and reengineer and update our product based on attacks that we see on the customer side. Our technical success managers, or TSMs, directly contact the customers during a breach, tell them the indicators of compromise to look for and give them patches. Our applied threat research teams look at the knowledge that our TSMs shared with our customer base.

ThreatINSIGHT is a hosted SaaS solution. The customers don't have to deal with the platform, and they like that. They depend on ThreatINSIGHT on a daily basis. An organization with 70,000 employees said that ThreatINSIGHT is the only security product that they have deployed at every single network that they have. They don't have a SIEM in every single office or even an EDR, because EDRs are limited to hosts that they can run on or that agents can run on, while ThreatINSIGHT works for all hosts, all traffic and all locations.

Gigamon®

NETWORK VISIBILITY FROM CORE TO CLOUD

Gigamon helps the world's leading organizations run fast, stay secure and innovate. With visibility into network traffic across the entire hybrid cloud infrastructure, organizations eliminate security blind spots and helping improve SOC effectiveness. Close the SOC visibility gap with Guided-SaaS NDR and access expert advisory guidance when it matters most.

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.

(800) 944-0401 • sales@ismg.io

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

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY (Prevention. Response. Notification.) CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

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