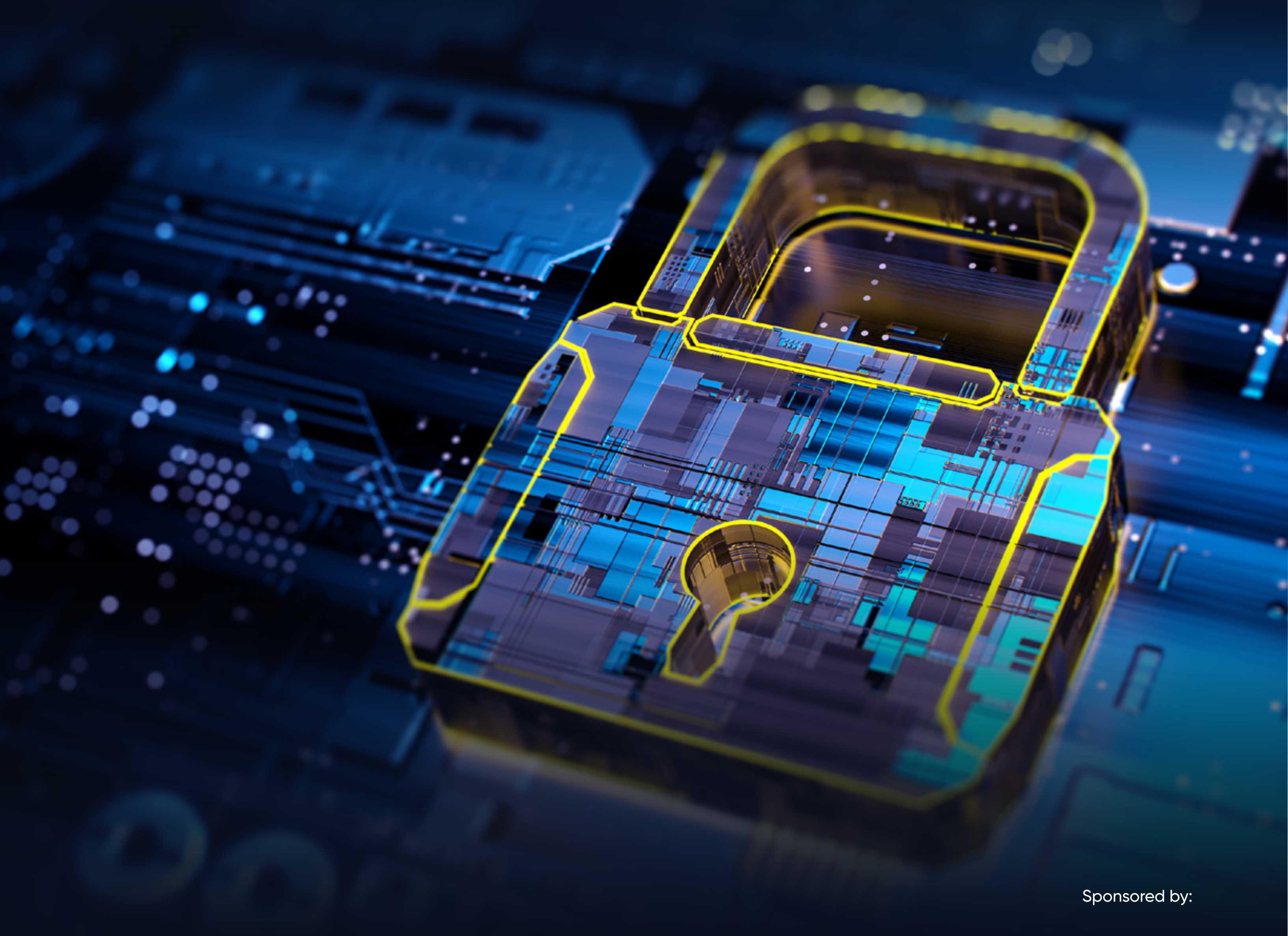
CYBER SECURITY HUB

THREAT INTELLIGENCE **EVOLUTION**



Sponsored by:

NETACEA

March 2021

EXECUTIVE SUMMARY

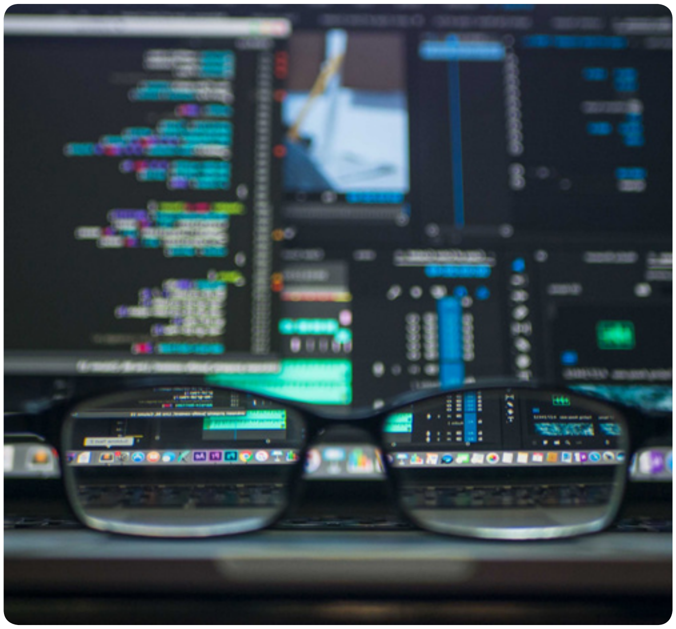
Cyber security threats are constantly evolving. Many organizations have learned the hard way that focusing on vulnerabilities alone is unmanageable and unproductive because there's no effective way of prioritizing which vulnerabilities need attention. As attack surfaces continue to expand, the number of potential vulnerabilities increases. As of March 4, 2021, NIST'S National Vulnerability Database (NVD) listed **149,901 Common Vulnerabilities and Exposures** (CVEs). The critical question for any organization is which of those vulnerabilities represent the biggest threats to the company and its customers? Although it is possible to narrow the search using keywords or an application vendor's name, businesses need a much faster way to prioritize them. One way to do that is through threat management which enables a company to understand where to focus its resources.

However, few organizations' threat management programs are addressing bot threats today, despite their growing use. While more organizations have engaged threat intelligence solutions, many of those solutions tend not include bot threat intelligence specifically. Without bot threat intelligence, it may appear as though a DDoS attack has been launched against the company's website or ecommerce site when the type of attack is far more nuanced than that. If the type of attack has been misidentified, then the time spent on remedial work will be wasted. Worse, hackers may have used the extra time to inflict additional harm.

Meanwhile, the pattern of attacks continues to shift as new tactics emerge. Traditionally, hackers have found a way into corporate networks and then navigate their way to sensitive data and other virtual assets. Modernly, they're compromising websites, web applications, and APIs using bots, targeting business logic as opposed to technical flaws. As the number of bot attacks continue to rise, enterprises cannot afford to defend themselves reactively, they must do so proactively.

This white paper explains in greater detail what bot threat intelligence is and why it's an essential part of an organization's security fabric.

TABLE OF CONTENTS



HOW THREATS ARE CHANGING

The COVID-19 pandemic was a gift for bad actors. Many companies were already in the process of digital transformation in direct response to digital disruption. When the pandemic hit, IT departments scrambled to enable virtual workforces within a matter of days so there wasn't adequate time to consider all the cyber security ramifications until later.

Meanwhile, hacker tactics adapted to the pandemic-stricken world. For years, they'd been compromising corporate networks, navigating their way to digital treasure troves. As businesses further engaged cloud architecture – some comparatively instantly as the result of the pandemic – hackers updated their tactics to focus on websites, web applications and APIs, and they're using bots to increase the speed and scale of their attacks. Yet, few companies are able to effectively thwart this evolving threat even now.

For one thing, cyber security teams are overwhelmed. Part of the reason is that they are still pursuing the impossible task of managing application vulnerabilities without the help of modern threat intelligence. Focusing on vulnerabilities alone is unwieldy and unproductive because there are too many that potentially apply to their expanding attack surface out of the 150,000 identified by NIST. Although it's possible to narrow a CVE search using an application vendor's name or keywords, vulnerability management is a time-consuming and costly process. Organizations need to understand which vulnerabilities are most relevant so they can be prioritized. That way, cyber security organizations can focus their limited security resources on what matters. To get there, they need modern threat intelligence which includes insights from bot attacks and associated automated remediation.

According to market and consumer data provider Statista, there were 109 million human-initiated and 442 million automated bot attacks in North America in the first half of 2020 alone.

Another challenge organizations face is that cyberattacks, including those executed by bots, are becoming more subtle and nuanced making them more difficult to detect. Threat intelligence must evolve accordingly to keep pace with hackers' changing tactics.

Finally, bad actors are becoming more organized and well-funded with many of them sponsored by nation states or other deep-pocketed organizations. They are targeting specific companies or groups of companies, sometimes spending millions or billions of dollars on a single project.

"You've always got to keep remembering the goal of automation, which was to make your team more productive, to free up your time so that you can minimize your opportunity costs so that you can spend the time with your precious resources on the things that matter the most. The key to automate things that keep reducing the noise, keep improving productivity, but do that in such a way that it's also not overwhelming the team."

Luke Steller

Cyber Security Operations & Threat Intelligence Head (Tribe Performance Lead), ANZ

PATTERNS OF BOT USAGE

Bot attack patterns differ from industry to industry, as well as among companies in the same industry.

For retail and ecommerce, bots will target a site with the goal of purchasing high-demand items, such as limited-edition products or concert tickets so they can be sold at a much higher price. When an instant sell out occurs, customers may become angry with the brand and complain on social media or stop doing business with that brand. Worse, the brand may also discover that the "successful" sellout of products was achieved by payment fraud. Sometimes, bots are used for sniping to ensure that no one else has time to bid or submit an offer.

In the healthcare sector, bots are bombarding provider websites with fake COVID vaccine appointments which are preventing some patients from getting immunized in a timely fashion. As the headlines reveal, the public is anxious about their individual ability to get a vaccine. Meanwhile, the healthcare providers are stuck with time-sensitive vaccine doses they may not be able to use and the revenue losses that come from fake patients failing to show up for their appointments.

Some of the threats bots represent include:

- Account takeovers which compromise PII and facilitate fraudulent transactions
- Card cracking which tests the validity of credit card numbers on websites
- Credential stuffing which automatically and continuously enters usernames and passwords into website login forms until the attack succeeds
- Fake account creation using fictional or stolen credentials
- PPC and other web-based click fraud that skews marketing analytics
- Sneaker/scalper bots which attempt to buy the entire inventory or a large inventory of high-demand or limited items so they can be resold at a much higher price
- Web scraping which steals website content without the owner's permission

An average account takeover involves between 50,000 and 200,000 attempts. Even if the attack succeeds only one percent of the time, as many as 2,000 accounts may have been compromised. The loss of PII could result in regulatory fines, lawsuits, reputational damage, customer attrition, and revenue loss. In addition, the dramatic traffic spikes may result in soaring infrastructure costs which are being squandered on malicious activity. These retail/ecommerce and healthcare examples are just two- nearly every sector is being hit with industry-specific attacks of their own.

WHAT THE BOT LANDSCAPE LOOKS LIKE

The use of bots allows hackers to accomplish more, faster and cheaper. Traditionally, bots have been deterministically programmed. However, an increasing number are using machine learning to make them more effective. Since most companies lack bot threat intelligence, they're easier targets.

Bot threat intelligence solutions must also take advantage of machine learning to defend against intelligent bots. That way, as the behavior of the bots changes, the solution can adapt. However, a strong defense requires more than just software. For example, the bot threat intelligence provider should be able to help protect customers against emerging threats that are targeting specific companies in their industry, such as high-end retailers, hospitals, or fintech companies.

Although bot intelligence platforms should be able to distinguish between attacks executed by humans or bots, some of them can even detect hybrid attacks involving humans and bots. For example, CAPTCHA was designed to prevent bots from posting spam on websites or harvesting data. However, well-funded groups hire humans to bypass CAPTCHA so the bots can succeed with their mission.

Of course, bad actors don't necessarily have to build bots when they can purchase them on the Dark Web. And increasingly, the bots sold on the Dark Web are being made available in multiple languages to increase their effectiveness in various parts of the world.

As organizations move further into the cloud, bot designs are adapting. Thus, bot threat intelligence is something today's enterprises clearly need.

> *"Once you know what attackers are targeting, their methods, and have an idea of the skill level of your adversaries, you can really start to make strategic-level security decisions to stay ahead of the attackers."*
>
> **Matthew Gracey-McMinn**
> Head of Threat Research, Netacea

HOW TO MINIMIZE THE MALICIOUS BOT THREAT

Data is critical. Companies must be able to understand how they're being attacked and how the threats are changing. To do that, organizations need comprehensive visibility into their web site traffic, web applications, and APIs to distinguish between bot and human interactions in each of those channels. Since more than 50% of web traffic is bot activity, businesses need a means of analyzing millions of requests, signals, and patterns in real time so they can take appropriate action in a timely fashion.

Armed with bot threat intelligence, cyber security teams can automatically block, redirect, or challenge attacks in real time or receive alerts notifying them of potential threats. However, the vendor's consulting arm should also provide additional insights that ensure the company is mitigating threats as early as possible.

A bot threat intelligence platform supplemented by a close, consultative partnership with the vendor can also help companies avoid attacks that have been launched against competitors or are planned against a group of businesses or the industry in which the company belongs.

Machine learning helps identify threat patterns and enables the bot threat management solution to adapt as threats evolve, becoming more sophisticated in the process. Different types of threats have different kinds of patterns that need to be defended against proactively.

Examples include:

- A high volume of fake account creations may camouflage an account takeover or the attack
- Obfuscation techniques such as placing random items in a cart like an actual customer would do may indicate carding
- Differing bot and human behavior over time, by path, or location within a website may reveal credential stuffing
- Registration page monitoring and user behavioral analysis may reveal the creation of fake accounts
- Changes in the number of new sessions, average session duration, average bounce rate, conversion rate, and direct and referral traffic may indicate click fraud that skews marketing results
- Monitoring site visits to a specific path and analyzing them in context relative to each of the visitors may indicate sneaker/scalper bots Information collection patterns may reveal web scraping

> *"The main focus is to leverage technical solutions which allow the users to gain insights and provide the ability to protect the information with the data-centric type of control."*

Mattieu Lahierre

Principal, Application & Data Security - Cybersecurity, Technology Risk & Compliance, BHP

›› HOW TO MINIMIZE THE MALICIOUS BOT THREAT (cont.)

A bot threat intelligence platform should be able to analyze the above scenarios in enough detail to distinguish between bots and real customers so that bot traffic can be stopped in its tracks and genuine traffic can continue to flow uninterrupted.

However, bot threat intelligence solutions are not a "set and forget" type of technology. Humans need to oversee and monitor them to ensure that the machine learning models are doing their job effectively and not "drifting" (becoming less accurate) over time. While the vendor is responsible for ensuring the accuracy of its bot threat intelligence solution generally, the vendor and its customer must work together to ensure the solution is protecting the specific company as effectively as possible since every company's attack surface and security posture is unique. Some vendors make a point of meeting with customers regularly, such as on a weekly basis, to ensure the two remain in sync.

All the while, the vendor should be monitoring the Dark Web and hacker forums continuously to gain insight into planned attacks, evolving hacker methods, the data that is available for sale, and emerging hacker tools so the intelligence gathered can be mapped to specific industries or groups of companies.

Using a holistic human-machine approach, it's easier to build proactive countermeasures that prevent or minimize bot-powered threats so that hackers are economically disincentivized from attacking protected assets.

"The future of detection and response I really believe is going to come down to technology, artificial intelligence, and machine learning."

Troy Wilkinson

Head of Cyber Security Data Analytics & Research, Interpublic Group (IPG)

EXECUTIVE Q&A

Matthew Gracey-McMinn - Head of Threat Research, Netacea

Bots aren't new. Why is their use in cyberattacks increasing now?

This has been caused by a combination of factors. First Covid-19 has driven a move to an online-first society, and while this move may decelerate with the end of Covid-19 we nonetheless anticipate it will continue. As more people and services move online this means there are more targets for bot attacks. More online services means more accounts and places with payment details stored, and more people using such services means more users whose information (from credentials through to payment details) can be attacked for profit. This has been compounded by an increasing interest in bot-based attacks; our Threat Research Team has observed a significant increase in both the number of bot attacks and the number of people joining bot groups and/or developing bots for attacks. More people being interested in bots means more bots, greater skill on the part of the bot developers and users, and more investment into their activities. They are thus advancing their capabilities quite rapidly. This combination has generated a feedback loop: there are more targets and more people doing the targeting, which means more money is being made by the attackers. This, in turn, encourages more people to become involved, which leads to more successful attacks, and so on.

What are bots capable of doing today? (E.g., they're not just deterministically programmed anymore so their capabilities have expanded. Explain the expanded capabilities AI/ML enable.)

Some of the more advanced bots we have seen are essentially collections of bots. A sort of "bot of bots". A collection of simple bots working together in sequence to perform a more complicated attack, with each bot performing its own stage of an attack before handing over to the next. This fully automates an entire attack and allows for readjustment to new methodologies based on what bots performing earlier stages have observed during their duties.

This includes having bots capable of bypassing defensive measures by being able to emulate human behavior on a website (and thus bypass detection methods based on behavioral analytics) or performing fully automated bypassing of CAPTCHA, which is commonly used to protect against bots. The most advanced bots can sell for prices in excess of $27,000 (USD). These are not cheap tools and for many developing bots is a business in and of itself – they simply build the tools used by others. These bots often have an ongoing development cycle with the developers adding new features at the customer's request and ensuring that the bot stays ahead of any attempts to mitigate against it.

Do bots always operate autonomously?

The bots perform actions autonomously. But they are not entirely autonomous with some stages of an attack being performed by humans. In some cases we see a back and forth between human and bot. The bot is essentially a tool for performing some (or in some cases all) of the stages of an attack. Generally speaking, the more advanced bots will automate more of these steps, while less sophisticated bots will require a more "hands on" approach from the human operator. Also, while it is tempting to think of this as an entirely automated attack, it is important to remember that the bot is a tool of a human operator who is using it to achieve an objective. While we may seek to mitigate against the tool, ultimately our objective is to thwart the adversary.

> *"The best start an organization can make is to take what they know and use it to look outwards. Examine the security incidents you have had and use this to understand and identify who is attacking you and how they are doing so."*
>
> **Matthew Gracey-McMinn**
>
> Head of Threat Research, Netacea

What are the biggest mistakes companies make when it comes to protecting their organizations against malicious bots?

It's not so much a mistake but rather an over-acceleration of the response. Many companies begin by saying "we want to stop bots" and start trying to block them. In my mind the first step is to really understand the bot threats facing that organization. Once you understand how the bots are attacking and what their objective is it is much cheaper, easier and quicker to implement an effective response. This understanding, of course, then needs to be kept up to date – it is no use maintaining a static defense in the face of a dynamic attacker.

What's the best way to shift from a reactive security organization to a proactive one?

I think the best start an organization can make is to take what they know and use it to look outwards. Examine the security incidents you have had and use this to understand and identify who is attacking you and how they are doing so. I recommend starting with methodology as attribution can be tricky. Once you know the sorts of attacks that are targeting you, you will be able to better recognize them immediately and implement protective measures against them. Then you can look at how advanced these attacks are. This should give some insights into the sorts of attackers that are targeting you and what they are after (i.e. are they low-skilled individuals/groups or high-skilled or somewhere in-between). Once you know what attackers are targeting, their methods, and have an idea of the skill level of your adversaries, you can really start to make strategic-level security decisions to stay ahead of the attackers.

CONCLUSION

Most enterprise security fabrics lack a bot threat intelligence element. Since bot traffic represents more than 50% of all web traffic, many security teams are missing an important part of the infrastructure that is necessary to protect their organization. Adding bot threat intelligence helps businesses save money, increase profitability and improve customer satisfaction and loyalty.

Like hackers, organizations should be combining technology, people, and processes to increase cyber security effectiveness. While a bot threat intelligence solution can help mitigate automated threats, security teams should also maintain a close relationship with the vendor's consulting team which has insight into the customers' website, web application, and API traffic as well as visibility across customers. By taking a partnership approach, the customer and the vendor are in a better position to protect the customer's assets against bot-powered attacks.

"If you look at the bad guys, they're happy to share information. They're happy to share the code. They collaborate a lot. Whereas good guys, they don't want to talk to each other. We don't collaborate. The good guys need to share information on what they're seeing so that we can collectively stop the bad guys."

Gopal Padinjaruveetil

CISO, AAA / The Auto Club

ABOUT NETACEA

Netacea provides an innovative bot management solution that solves the complex problem of account takeover and malicious bot activity for its customers, in a scalable, agile and intelligent manner, across websites, mobile apps and APIs. Our Intent Analytics™ engine is driven by machine learning to provide an in-depth analysis into all traffic to your site. This gives us an incredibly fast and comprehensive understanding of human and automated traffic behavior, enabling us to identify and block bots in real time with unparalleled accuracy. With machine learning at the heart of our approach, our technology provides an innovative and profoundly effective solution that is configurable to your environment and adapts to changing threats.

FOR MORE INFORMATION, VISIT NETACEA

ABOUT CYBER SECURITY HUB

CYBER SECURITY HUB

The Cyber Security Hub is an online news source for global cyber security professionals and business leaders who leverage technology and services to secure the entire perimeter in their enterprise.

We're dedicated to providing the latest industry news, thought leadership and analysis in the cyber security space. Cyber Security Hub's expert commentary, tools and resources are developed through obtaining data and interviewing end users and analysts throughout the industry to deliver practical and strategic advice.

Our editorial team surveys and monitors the latest trends in cyber security and creates news articles, market reports, case studies and in-depth analysis for a captive audience consisting of C-Level executives, VPs and directors of cyber security and information technology.

CYBER SECURITY HUB TEAM

Dorene Rettas
Managing Director
Dorene.Rettas@CSHub.com

Seth Adler
Editor-in-Chief
Seth.Adler@iqpc.co.uk

Tilak Antony
Director of IQPC
Digital Partnerships
Tilak.Antony@iqpc.com

Imran Shafi
Sales Director
Imran.shafi@iqpc.com

Rose Morishita
Director of Marketing
Rosecley.Morishita@iqpc.com

Desiree Santiago
Marketing Manager
Desiree.Santiago@cshub.com

SOCIAL MEDIA INFORMATION

Facebook:
CSHubIQPC

Twitter:
CSHubUSA

LinkedIn:
CSHub – Enterprise Security Professionals

JOIN US AT OUR UPCOMING ONLINE EVENTS:

CYBER SECURITY
DIGITAL SUMMIT FOR:
THREAT INTELLIGENCE 2021
AMERICAS

March 16 - 17

CYBER SECURITY
DIGITAL SUMMIT FOR:
THREAT INTELLIGENCE 2021
APAC

March 30 - 31

CYBER SECURITY
DIGITAL SUMMIT FOR:
HEALTHCARE 2021

April 13 - 14

CYBER SECURITY
DIGITAL SUMMIT FOR:
GLOBAL 2021

May 4 - 5

CYBER SECURITY
DIGITAL SUMMIT:
APAC 2021

July 13 - 14

CYBER SECURITY
DIGITAL SUMMIT FOR
FINANCIAL SERVICES 2020

September 14 - 15

CYBER SECURITY
DIGITAL SUMMIT FOR:
EMEA 2021

October 19 - 20

CYBER SECURITY
DIGITAL SUMMIT FOR:
NORTH AMERICA 2021

November 9 - 11

CYBER SECURITY HUB

Visit CSHub.com for more information from cyber security leaders for the cyber security community