

Security

ADVISOR

MIDDLE EAST



INTERVIEWS:

SOPHOS
JOHN SHIER

CYSIV
**PARTHA
PANDA**

ARMIS
**CHRISTOPHER
DOBREC**



UNDERSTANDING CYBERSECURITY

AS THE CYBERSECURITY AND ATTACK LANDSCAPES
BECOME MORE COMPLICATED, WE TRY TO CAPTURE
THE REAL PICTURE AND BRING YOU THE ENTIRE STORY.

Cyberattacks don't stop at your email perimeter. Your security can't either.

Phishing campaigns and business email compromise (BEC) grew by 54% and 67% respectively this past year proving that email continues to be the #1 attacked vector by cybercriminals.

Prevent Malicious Emails with DMARC

- Gain full visibility and governance across all email channels
- Authenticate email messages and improve deliverability
- Block inbound attacks and protect brands against abuse
- Publish a policy that instructs ISP's to deliver or delete emails



**DMARC
Resources
& Free Trial**

info.mimecast.com/dmarc-resources



mimecast



06 NEWS
We bring you up-to-date with the latest developments in the world of cybersecurity

INTERVIEWS

10 Christopher Dobrec, Vice-President Product Marketing, Armis, discusses the evolution of IoT, the convergence of IT & OT and how Armis is positioned to add value.

12 John Shier, Senior Security Advisor, Sophos, explains how Sophos adopts a comprehensive, collaborative and innovative approach to cybersecurity.

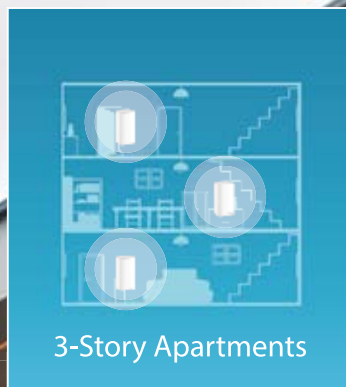
16 Partha Panda, CEO and co-founder of Cysiv, Inc, discusses how Cysiv's 24/7 SOCaaS solutions help organisations reduce the risk of costly & damaging breaches and business disruptions.

INSIGHT

18 Tamer El Refaey, chief cybersecurity strategist, emerging markets, Micro Focus, says that with the right technical capabilities, nextgen SoCs can help filter out 'noise' and overcome the major challenges surrounding cyber security.

Simple. Yet Flexible

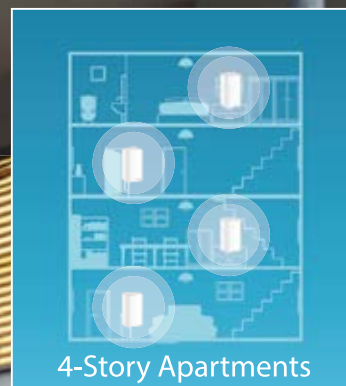
Wi-Fi 6



3-Story Apartments



**COVR-X1873
(3-pack)**



4-Story Apartments



**COVR-X1874
(4-pack)**

AX1800 Whole Home Wi-Fi 6 Mesh System



Smart
Roaming



MU-MIMO
Technology



Smart
Steering



Simple
Setup



Profile-based
Parental Controls



Expandable
Network



WPA3™
Encryption



Works with your
existing router
or gateway



Connect to more...

D-Link®

EDITORIAL



Talk to us:

E-mail:

anita.joseph@cpimediagroup.com

Anita Joseph
Editor

MAKING SENSE OF CYBERSECURITY

The cybersecurity landscape is evolving, but so are the threats—which is what makes the entire ecosystem fascinating and complicated. Research shows that hackers and cybercriminals are always a step ahead and that breaches and attacks are continuing into 2021 with increased vigour and sophistication. While threats such as ransomware and phishing dominate, subtler yet more serious threats are looming large on the horizon, all set to decimate organisations that don't have a solid cybersecurity strategy in place.

So, what can we do? How can we understand our security loopholes and address them in order to put up a strong defence? Experts vary in their opinion: some say that a collaborative approach is the best way forward, while others are of the opinion that 24/7 Security Operations Center-as-a-Service (SOCaaS) is the need of the hour. Some advocate a predictive approach to hacker behaviour and attack patterns, while others point out that an increased focus on

the human angle is the best defence tactic. Whatever it may be, one thing is clear: that cybersecurity must be the topmost priority for businesses if they hope to survive an increasingly mind-boggling deluge of cyberattacks aimed right at their weak spots.

This issue of your favourite magazine attempts to make sense of the whole threat/defence environment, especially now that the pandemic has accelerated digital transformation and shifted the whole world online. We speak to the who's-who of the cybersecurity industry to find out how they are interpreting the current scenario and where they see themselves in the future. We have insightful interviews with global players such as Sophos, Armis and Cysiv, as well as insights from industry frontrunners such as Fortinet and Mimecast, to bring you the whole picture, from every angle.

So, don't miss this issue—it's special—compact, focused and straight-to-the-point. Happy Reading!

**CYBERSECURITY
MUST BE THE
TOPMOST PRIORITY
FOR BUSINESSES
IF THEY HOPE
TO SURVIVE AN
INCREASINGLY
MINDBOGGLING
DELUGE OF
CYBERATTACKS
AIMED RIGHT AT
THEIR WEAK SPOTS.**

EVENTS



FOUNDER, CPI MEDIA GROUP
Dominic De Sousa (1959-2015)

Published by



Publishing Director
Natasha Pendleton
natasha.pendleton@cpimediagroup.com

**EDITORIAL
Editor**
Anita Joseph
anita.joseph@cpimediagroup.com

**DESIGN
Senior Designer**
Analou Balbero
analou.balbero@cpimediagroup.com

Registered at
Dubai Production City, DCCA
PO Box 13700
Dubai, UAE

**ADVERTISING
Group Sales Director**
Kausar Syed
kausar.syed@cpimediagroup.com

Online Editor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

**DIGITAL SERVICES
Web Developer**
Adarsh Snehan

Reception: +971 4 5682993
Operations: +971 4 5682994
Accounts: +971 4 5682995

Senior Sales Manager
Sabita Miranda
sabita.miranda@cpimediagroup.com

© Copyright 2021 CPI
All rights reserved

While the publishers have made every effort to ensure the accuracy of all information in this magazine, they will not be held responsible for any errors therein.

CISCO UNVEILS PASSWORDLESS FUTURE WITH STRONGER SECURITY FOR ALL

FADY YOUNES,
CYBERSECURITY
DIRECTOR, MIDDLE EAST
AND AFRICA, CISCO



Cisco Secure, the

leader in enterprise security, unveiled the future of simple and effective security with infrastructure agnostic, passwordless authentication by Duo Security. Integrated seamlessly into the existing Duo authentication experience used by more than 25,000 organisations globally, Duo passwordless authentication will enable enterprise users to skip the password and securely log into cloud applications via security keys or biometrics built into modern laptops and smartphones.

The consequences of using passwords are well known. Passwords are easily compromised and difficult to manage, costing enterprises billions of dollars annually. Users are inundated with passwords in their personal and professional lives. Password reset requests comprise a lion's share of IT help desk tickets, resulting in lost productivity for users and increased support costs for the business.

Duo passwordless authentication is part of Cisco's industry-leading zero trust platform, securing access for any user, from any device, to any IT application or environment. The product is designed to be infrastructure agnostic, paving the way to a passwordless future while ensuring that enterprises can seamlessly protect any combination of cloud and on-premises applications without requiring multiple authentication products or leaving critical security gaps. "Cisco has strived to develop passwordless authentication that meets the needs of a diverse and evolving workforce and allows the broadest set of enterprises to securely progress towards a passwordless future, regardless of their IT stack", said Fady Younes, Cybersecurity Director, Middle East and Africa, Cisco. "It's not an overstatement to say that passwordless authentication will have the most meaningful global impact on how users access data by making the easiest path the most secure," he added.

NUTANIX STUDY SHOWS GLOBAL PUBLIC SECTOR "CLOUD SMART" STRATEGIES VALIDATED BY COVID-19 RESPONSE

Nutanix, a leader in private cloud, hybrid

and multi-cloud computing, announced the global public sector industry findings of its third annual Enterprise Cloud Index Report, measuring organisations' plans for adopting private, hybrid and public clouds. The findings point to a concentrated modernisation effort throughout the sector over the past few months, with 70% of respondents saying COVID-19 has caused IT to be viewed more strategically in their organisations. This COVID-19-spurred push is especially notable, given that the public sector has struggled with IT modernisation efforts. Nearly half (48%) of global public sector respondents said their organisations had no employees working remotely one year ago. However, since the onset of the pandemic, the sector has scaled its number of remote workers, with only 15% and 11% of respondents reporting employing zero remote workers today. In order to effectively support this growing remote workforce, organisations have begun strategically evaluating their cloud models – with more than three-fourths (82%) of global public sector respondents identifying hybrid cloud as the ideal IT operating model for their organisation.

AARON WHITE, SR.
SALES DIRECTOR,
METI AT NUTANIX



Other key findings of this year's report include:

- **Modernisation is dependent on**

- decommissioning legacy architectures:** In

2019, 53% of global public sector organisations exclusively ran traditional, non-cloud-enabled datacentres. In 2020, that percentage dropped to 22%. Over the next five years, the public sector expects a 20-percentage-point drop in legacy datacentre installations and a substantial 43-point increase in hybrid cloud deployments.

- **Working from home remains top-of-**

mind: 43% of public sector respondents reported a direct increase in their public cloud investments as a direct result of the pandemic – eight points higher than the global average. These moves likely reflect an effort to quickly provide for home working employees, as past restrictions made them less capable of providing work-from-home solutions than other industries. Moreover, most entities in this sector are planning to maintain support for home working, with only 4% planning to go back to their pre-pandemic approach.

ANNUAL FIREEYE MANDIANT M-TRENDS REPORT REVEALS GLOBAL STATISTICS AND INSIGHTS FROM HUNDREDS OF INTRUSIONS

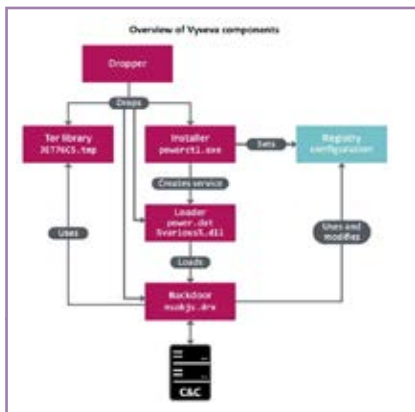
FireEye, the intelligence-led

security company, has released the FireEye®Mandiant® M-Trends® 2021 report. Now in its 12th year, M-Trends brings together the best of cybersecurity expertise and threat intelligence with statistics and insights gleaned from recent frontline Mandiant investigations around the globe.

This year's report outlines critical details on trending attacker techniques and malware, the proliferation of multifaceted extortion and ransomware, preparing for expected UNC2452 / SUNBURST copycat threat actors, growing insider threats, plus pandemic and industry targeting trends.

Additional findings are summarized below:

Over the past decade, Mandiant has observed a trending reduction in global median dwell time (defined as the duration between the start of a cyber intrusion and when it is identified). This measure went from over one year in 2011 to just 24 days in 2020 – that's more than twice as quickly identified in comparison to last year's report with a median dwell time of 56 days. Mandiant attributes this reduction to continued development and improvement of organizational detection and response capabilities, along with the surge of extortion and ransomware intrusions.



OVERVIEW OF VYVEVA COMPONENTS

ESET researchers have discovered a previously undocumented backdoor used to attack a freight logistics company in South Africa, which they have dubbed Vyveva. They have attributed the malware to the infamous Lazarus group due to shared similarities with the group's previous operations and samples. The backdoor includes several cyber-espionage capabilities, such as file exfiltration and gathering information about the targeted computer and its drives. It communicates with its Command & Control (C&C) server via the Tor anonymity network.

ESET telemetry for Vyveva suggests

LAZARUS ATTACKS FREIGHT COMPANY IN SOUTH AFRICA WITH A NEW BACKDOOR: ESET RESEARCH

targeted deployment as ESET researchers have found only two victim machines, both of which are servers owned by the aforementioned South African logistics company. According to the ESET investigation, Vyveva has been in use since at least December 2018.

"Vyveva shares multiple code similarities with older Lazarus samples that are detected by ESET technology. However, the similarities do not end there: the use of a fake TLS protocol in network communication, command line execution chains, and the methods of using encryption and Tor services all point toward Lazarus. Hence, we can attribute Vyveva to this APT group with high confidence," says ESET researcher Filip Jurčacko, who analysed the discovered Lazarus arsenal.

KASPERSKY: 32% OF UAE USERS UNDER THREAT FROM MALWARE HIDING WITHIN THEIR DEVICES



There is a common misconception that the most dangerous threats on the modern users' digital journeys are encountered during Internet surfing. The reality, however, based on the most recent analysis of cyberattacks in the United Arab Emirates in 2020 by Kaspersky experts, is that users are in fact more likely to face attacks from malware hidden within their devices.

Such threats are classified as 'local', which means they are detected either on users' devices or on portable data storage devices, such as flash drives. In 2020, 32% of Kaspersky private users and 24% of all corporate users in UAE were attacked by such threats. In comparison, web attacks affected only 12% and 8%, respectively.

Unfortunately, there has been an increase in the sophistication of such threats – which may be hiding on the user's device within a seemingly legitimate file for a while, to fly under the radar, and only strike later.

"The cyber threat landscape across the UAE is constantly evolving," says Denis Parinov, a cybersecurity expert at Kaspersky. "A few years ago, there were many more drive-by attacks –when different malicious software is downloaded and run while the user simply browses the Internet. Nowadays, most of the web-threats 'stays in browser': they specialise in content replacement, browser locking or clickjacking, online-skimming, cookie stuffing, etc., Now the situation when the user could download a malicious file directly is not too frequent. It's more common for a malware to be disguised as something else to hide from the security solutions, remaining an unseen threat to users. The good news however is that modern security solutions are too advanced for such malware to fly below radar – it is more likely to be blocked either during the initial scan of the file by a security solution that happens by default, or within the very moment such programs attempt to launch," he added.

FORTINET ENHANCES STUDENTS' CYBERSECURITY AWARENESS WITH AVAILABILITY OF FREE TRAINING AND BOOK RELEASE

Fortinet, a global leader in broad, integrated and automated cybersecurity solutions, has announced continued commitment to educate students and underrepresented groups on cyber awareness and safety. In addition to Fortinet's NSE 1 and NSE 2 training courses focused on fundamental cyber awareness providing an overview of threat actors and their tactics, Fortinet is releasing a children's book designed to increase cyber awareness amongst children ranging from 7 to 12 years old. The book "Cyber Safe: A Dog's Guide to Internet Security" was co-authored by Renee Tarun, Deputy CISO at Fortinet.

RENEE TARUN,
DEPUTY
CISO AND VP
INFORMATION
SECURITY AT
FORTINET



Renee Tarun, Deputy CISO and VP Information Security at Fortinet and Co-Author of "Cyber Safe" said, "With more children being online for prolonged periods of time as a result of remote learning, it's especially important to educate our youth about internet safety. The "Cyber Safe" book was written to help protect kids by teaching them from an early age how to behave and to keep themselves safe online."

MCAFEE SEES COVID-19 THEMED THREATS AND POWERSHELL MALWARE SURGE



McAfee Corp., the device-to-cloud cybersecurity company, released its McAfee Threats Report: April 2021, examining cybercriminal activity related to malware and the evolution of cyber threats in the third and fourth quarters of 2020. In Q4, McAfee Labs observed an average of 648 threats per minute, an increase of 60 threats per minute (10%) over Q3. The two quarters also saw COVID-19 related cyber-attack detections increase by 240% in Q3 and 114% in Q4, while Powershell threats again surged 208% due to continued increases in Donoff malware activity.

“The world—and enterprises—adjusted amidst pandemic restrictions and sustained remote work challenges, while security threats continued to evolve in complexity and increase in volume”, said Raj Samani, McAfee fellow and chief scientist. “Though a large percentage of employees grew more proficient and productive in working remotely, enterprises endured more opportunistic COVID-19 related campaigns among a new cast of bad-actor schemes. Furthermore, ransomware and malware targeting vulnerabilities in work-related apps and processes were active and remain dangerous threats capable of taking over networks and data, while costing millions in assets and recovery costs”.

Each quarter, McAfee assesses the state of the cyber threat landscape based on in-depth research, investigative analysis, and threat data gathered by the McAfee Global Threat Intelligence cloud from over a billion sensors across multiple threat vectors around the world. The introduction of MVISION Insights in 2020 has made it

possible for McAfee to track the prevalence of campaigns, their associated IoCs, and determine the in-field detections. This month’s report is the first to feature statistics such as the top MITRE ATT&CK techniques observed in Q4 among criminal and APT groups, while sharing observations on the SUNBURST malware that rocked the cybersecurity world at the end of 2020.

COVID-19 Themed Threats

As organisations the world over adapted to unprecedented numbers of employees working from home, cybercriminals worked feverishly to launch COVID-19 themed attacks on a workforce coping with pandemic restrictions and the potential vulnerabilities of remote device and bandwidth security. As the pandemic began to surge around the world, McAfee saw a 605% increase in Q2 2020. These attacks again increased by 240% in Q3 and 114% in Q4.

Malware Threats

In Q3 2020, McAfee Labs observed an average of 588 threats per minute, an increase of 169 threats per minute (40%). By the fourth quarter, this average rose to 648 threats per minute, an increase of 60 threats per minute (10%).

- Powershell threats grew 208% in Q4 driven largely by Donoff malware. McAfee observed numerous Powershell attacks utilising Process Injection to insert code into legitimate running processes as a privilege escalation technique.
- Mobile malware grew 118% in Q4 in part due to a surge in SMS Reg samples. The HiddenAds, Clicker, MoqHao, HiddenApp, Dropper and FakeApp strains were the most

detected mobile malware families.

- Ransomware grew in volume 69% from Q3 to Q4 driven by Cryptodefense. REvil, Thanos, Ryuk, RansomeXX and Maze groups topped the overall list of ransomware families.
- MacOS malware exploded in Q3 420% due to EvilQuest ransomware but then slowed towards the end of the year.

Victims, Vectors & Vulnerabilities

Publicly Reported Incidents. McAfee tracked a 100% increase in publicly reported cyber incidents targeting the technology sector during the fourth quarter of 2020. Reported incidents in the public sector grew by 93% over the same period.

Attack Vectors. Malware was the most reported cause of security incidents in Q4 followed by account hijackings, targeted attacks and vulnerabilities. Incidents related to new vulnerabilities surged 100% in Q4, malware and targeted attacks each rose 43%, and account hijackings increased 30%.

Vulnerabilities Exploited. Among the campaigns McAfee monitored and investigated, the Eternal Blue exploit was the most prominent in Q4 2020.

MITRE ATT&CK techniques

The top MITRE ATT&CK techniques observed by McAfee in Q3 and Q4 included System Information Discovery, Obfuscated Files or Information, File and Directory Discovery, Data Encryption for Impact, Stop Services, Process Injection, Process Discovery, Masquerading Techniques, and Exploits of Public Facing Applications. 📌



ARE YOUR APPS READY TO PERFORM?



Software and applications are the backbone of modern business. High-performing applications are essential to deliver an enhanced experience and superior quality. Without it, you will be challenged to keep pace with digital natives and competitors alike.

Are you maximising your investment in application development with performance testing?

CONTACT MICRO FOCUS TODAY TO IMPROVE YOUR PERFORMANCE

Learn more at microfocus.com/loadrunner Or Scan this QR code:



PROTECTING THE CONNECTED LANDSCAPE

CHRISTOPHER DOBREC, VICE-PRESIDENT PRODUCT MARKETING, ARMIS, SPEAKS TO ANITA JOSEPH ABOUT THE EVOLUTION OF IOT, THE CONVERGENCE OF IT & OT AND HOW ARMIS IS POSITIONED TO ADD VALUE.

Five years ago, IoT was the 'next big thing' – what's the 'next big thing' that is beginning to emerge today?

The thing that's emerging now, and it's really a continuation of the trend, is really protecting all things that are connected to enterprise networks and the Internet. This is further enhanced by the various connectivity options that we're having, including 5G, but the notion that these devices are connecting to these networks—billions of them—and the enterprises that are deploying them are reaping the benefits, because they are becoming more efficient and more productive. The thing to consider as we move forward is that these products were designed to connect, certainly, but they weren't necessarily designed with built-in security in mind and so this has greatly expanded the overall attack surface and the risk landscape, and essentially these IoT and unmanaged devices they're all basically computers and have processors and memory and run applications, but they can't necessarily be managed or protected in the way traditional IT devices can, and so you need a really different approach for protecting them. So, the big thing, in my opinion, is nothing new emerging per se, but a continuation of the trend of an explosive growth of these things connecting by virtue of all the different connectivity options and the thing that we need to focus energy on, moving forward, is really how you protect them.

How are customers / CISOs preparing for that?

As with any emerging trends, there are varying degrees of recognition and preparedness here. But I think, there's a good news-bad news story here—in light of the recent attacks and breaches there's definitely an overall heightening of awareness that's bringing cybersecurity to the forefront of thinking at the C-level and board level in most organisations. So, the bad news is all these breaches, the good news is that it's front and centre of thinking and helping people manage their businesses. However, the challenge is really going to come down to, oftentimes, the skillsets and the budgets and from our perspective, the deeper visibility and what's actually going on in the network—in that say, complete visibility to every device, every asset—this still remains a key challenge for everyone, but I think customers and CISOs that I speak to are now beginning to prepare for that. This is actually where Armis comes in—the engagements that we have, most often begin by installing our platform and doing a complete discovery of what's actually on the network—managed, unmanaged and IoT devices—and giving that accounting and that visibility to those customers. So, I guess the recent events are heightening awareness and creating the need to get deeper visibility into what's going on. So, certainly, so the customers and CISOs that I'm speaking



to are getting ready for this and inviting Armis to the table to help them out.

How do you expect the IoT / unmanaged landscape to evolve in the next 3-5 years?

It's certainly not slowing down, that's for sure. We're not seeing any signs of these connected things going away-people are still deploying them for a variety of applications, mostly having to do with efficiency and productivity. But the real focus is going to be about how to deploy, manage and protect these systems at scale. Generally speaking, I would say security teams are reasonably prepared for that and that's the big challenge in the landscape for the next 3-5 years. Once again, I'd say it's exacerbated and enhanced by the fact that so many connectivity options are available now. I think 5G is going to have a major, major impact on that, moving forward.

So, it seems WFH is here to stay for the foreseeable future for many organizations? What is the biggest challenge organizations face with WFH?

The initial challenge at this point in time has been how to provide employees with access and secure access at scale. Recently, I spoke with a financial services organisation in the US and the CISO there told me that they went from about 15% of their workforce working remotely, to more than 90% of the workforce working remotely and working from home now. So, top of mind in that regard is: how do you provide the infrastructure that scaled to accommodate that? Of course, what comes along with providing that is providing access securely to all the tools that the employees need-whether those exist on-premise at the office or whether they exist in the cloud or whether they're in the home. Without a doubt, the visibility challenge remains a big issue, in the work-from-home use cases as well, and that comes down to having a complete visibility and understanding of the user,

"WE SEE NOT ONLY IT DEVICES & THE TRADITIONAL IT NETWORKS, BUT THE OT DEVICES AS WELL..."

their devices, their applications and being able to see all these things-this is definitely a challenge faced by most organisations I speak to when it comes to work from home.

We hear about the convergence of IT and OT - How is Armis positioned to help here?

The convergence is very real and it starts with the fact that the OT systems that have historically been air-gapped, now have connections to the Internet and often help out with connections to the Internet itself, for things like maintenance and monitoring. So, at first it started at the network level-the OT systems connecting to the Internet and the IT systems. Armis is very well suited to provide value here-we discover and protect all the devices and assets on both sides, if you will. We see not only IT devices and the traditional IT networks, but we see all the OT devices as well and we can provide our customers with their risk assessment and threat response for all those managed, unmanaged, IoT and OT devices.

As an example, in our product we've built some very specific capabilities that are targeted for OT environments but they're built on the Purdue model of access and so our product is geared to see all six levels-from level five to level zero and that means everything from managed IT devices and the enterprise network, all the way down to engineering workstations and PLCs and the backplanes of PLCs and even those physical connections at level zero, in those manufacturing environments. But the reason Armis is well suited in this space is that we see everything and have the ability to protect all those devices. This is where we're, quite frankly, being invited to quite a number

of large opportunities on a global basis, recognising this convergence of OT & IT.

What are some of the trends that will emerge in cybersecurity, going forward?

If you look at some of the recent threats-the points of entry have been greatly expanded by all the IT, OT, unmanaged, managed and IoT devices and the various connectivity options. The bad actors look for a way to get in and then they lie in wait and do the required reconnaissance and find their targets. Our research team has done some extensive research into vulnerabilities that impact these kinds of devices. Last year, they had divulged a set of vulnerabilities that we dubbed "URGENT/11"-at the time there were eleven zero-day vulnerabilities that impacted the networking software stack that's embedded in real-time operating systems. What that exposed was that now these devices, by virtue of being connected to the network, allow for the attackers to come in through a different route, because of these types of vulnerabilities. Earlier this year, we disclosed the vulnerability in CISCO's device discovery protocol, which we call CDPwn. This particular vulnerability impacts virtually all of the CISCO infrastructure-everything from switches and routers, to IP phones and IP cameras. But the key notion here I would point out is that it's not the traditional laptop or server any longer. It's the infrastructure pieces, the network-these are the things people need to be concerned about. We did a blog post recently that confirms what I've been saying-but our researchers did a follow-up on the "URGENT/11" and CDPwn research and we highlighted that over a year later, 97% of devices that are vulnerable to "URGENT/11" still remain unpatched. Further, 80% of devices that are vulnerable to CDPwn remain unpatched. This is concerning on the one hand, but these are the things we have to think about now-all these new entry points and how do we see them and stop them and protect the broader infrastructure. 🧑



John Shier, Senior Security Advisor, Sophos

SHARING & COMMUNICATING FOR A ROBUST CYBERSECURITY INDUSTRY

JOHN SHIER, SENIOR SECURITY ADVISOR, SOPHOS, TELLS ANITA JOSEPH IN AN EXCLUSIVE INTERVIEW HOW SOPHOS ADOPTS A COMPREHENSIVE, COLLABORATIVE AND INNOVATIVE APPROACH TO CYBERSECURITY.

How would you evaluate the global threat landscape today? What are the main areas of concern?

The obvious global concern is ransomware. Unfortunately, ransomware is often a symptom of an underlying security weakness. The reasons for ransomware's success are varied and speak to a broader set of causes. We find ourselves in a world where many cybercriminals have specialised and offer their unique services to others. Some focus their efforts on initial access by breaching companies with weak security on their externally facing services. Others are skilled at phishing which nets them valuable network credentials. Both these groups can resell their ill-gotten information to other criminals who are skilled at hands-on attacks and data exfiltration.

We also see malware, mostly in the form of droppers, that provide this initial foothold and offer compromised hosts

to other malware crews, like banking trojans. These banking trojans will, in turn, sell their access to ransomware crews once they have everything they need for financial fraud. Much of this world is automated, but it is supported by well-resourced criminals who have the time, money, and skill to deal with setbacks. What's worse are the groups that offer everything-criminal-as-a-service to unskilled, wannabe-cybercriminals.

Taken together, all these different threats and threat groups make it so that defenders need to be on constant high alert for potential problems in their environment. Just because you stopped an Emotet infection doesn't mean that Trickbot isn't hiding somewhere else. An exposed service, like RDP, can quickly turn into an entry point for an attacker. Once inside, they may drop clues to their presence, but these must be detected and investigated by security analysts. Failure to do so can, and often do, result in a ransomware attack. In the end, a lot must be done right so that one small misstep doesn't bring your company to its knees.

Multi-factor authentication, machine learning, application control-how can these technologies be effectively used to respond effectively to modern-day sophisticated cyber-attacks?

Protection technologies are particularly effective when they excel at a narrow set of capabilities. For example, application control allows administrators to divide applications into allowed and blocked. This simple division means we can authorise known-good applications from those we want to keep off our endpoints, thus reducing our attack surface. It doesn't mean a "good" application can't do "bad" things but at least now we have fewer applications capable of doing bad things.

"DEFENDERS NEED TO BE ON CONSTANT HIGH ALERT FOR POTENTIAL PROBLEMS IN THEIR ENVIRONMENT."

Machine learning is designed to deal with large volumes of data and can identify hidden patterns. To that end, we use it for blocking the hundreds of thousands of threats we see every day. But, to take our first example, we can also use it to spot suspicious patterns in behavior. If a "good" application starts behaving badly, machine learning can override application control and provide a backstop for catching novel threats. This layering of technologies, each with a specialised focus, is key to protecting modern environments.

Multi-factor authentication (MFA) is another backstop to an existing technology. Password-only authentication is fine provided the passwords are unique, long enough, stored properly, and kept secret. Failing any one of those criteria can lead to unauthorized access. MFA has been designed to provide an additional layer of security for when those criteria aren't met. Whether the failure happens to be password re-use, easily guessed or brute-forced, or disclosed by breach or subterfuge, MFA can stop an attacker dead in their tracks.

How can the security industry become collaborators and inventors to respond to evolving threats?

I'd argue that we're already doing this,

but it doesn't mean we can't do more. There are established groups, like the Cyber Threat Alliance (CTA), which aims to "improve the cybersecurity of our global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing among companies and organisations in the cybersecurity field." Other groups such as industry focused ISACs can get more focused with industry-specific threat information and protection strategies. Constant sharing and communication are key to developing a robust cybersecurity industry that pushes itself to continually improve and innovate in the face of ever increasing and sophisticated attacks. At Sophos, we value diversity and sharing which is why we participate in groups like the CTA and contribute to ISACs. We believe that our knowledge will help others make better decisions about how to protect themselves. We also benefit from the knowledge of others, especially those that look at the threat landscape from a different angle. It helps provide perspective and context that is incredibly important in this multi-dimensional fight with cybercriminals.

How is Sophos helping companies stay cyber-resilient and minimize the impact of complicated hacking techniques?

Sophos helps companies fight cybercrime in a few ways. First, we provide companies with products that prevent threats and unwanted software from infecting your devices and networks. Next, we provide a managed service that continuously monitors customer environments for those that don't have a security team, and a rapid response team to help companies who find themselves under active attack. Lastly, we provide insight into current threats and adversary tactics, and advice on how to best protect yourself through our various outreach channels. 📌

SOCaaS: THE NEED OF THE HOUR

PARTHA PANDA, CEO AND CO-FOUNDER OF CYSIV, INC, TELLS ANITA JOSEPH HOW CYSIV 'S 24/7 SOCaaS SOLUTIONS HELP ORGANISATIONS REDUCE THE RISK OF COSTLY AND DAMAGING BREACHES & BUSINESS DISRUPTIONS.

What is Cysiv all about?
Cysiv is a security software company. We provide 24/7 security operations center-as-

a-service (SOCaaS) that combines our cloud-native, next-gen SIEM software with a team of experts, to provide threat detection and active response. We deliver all of this, as-a-service, with simple subscription-based monthly billing.

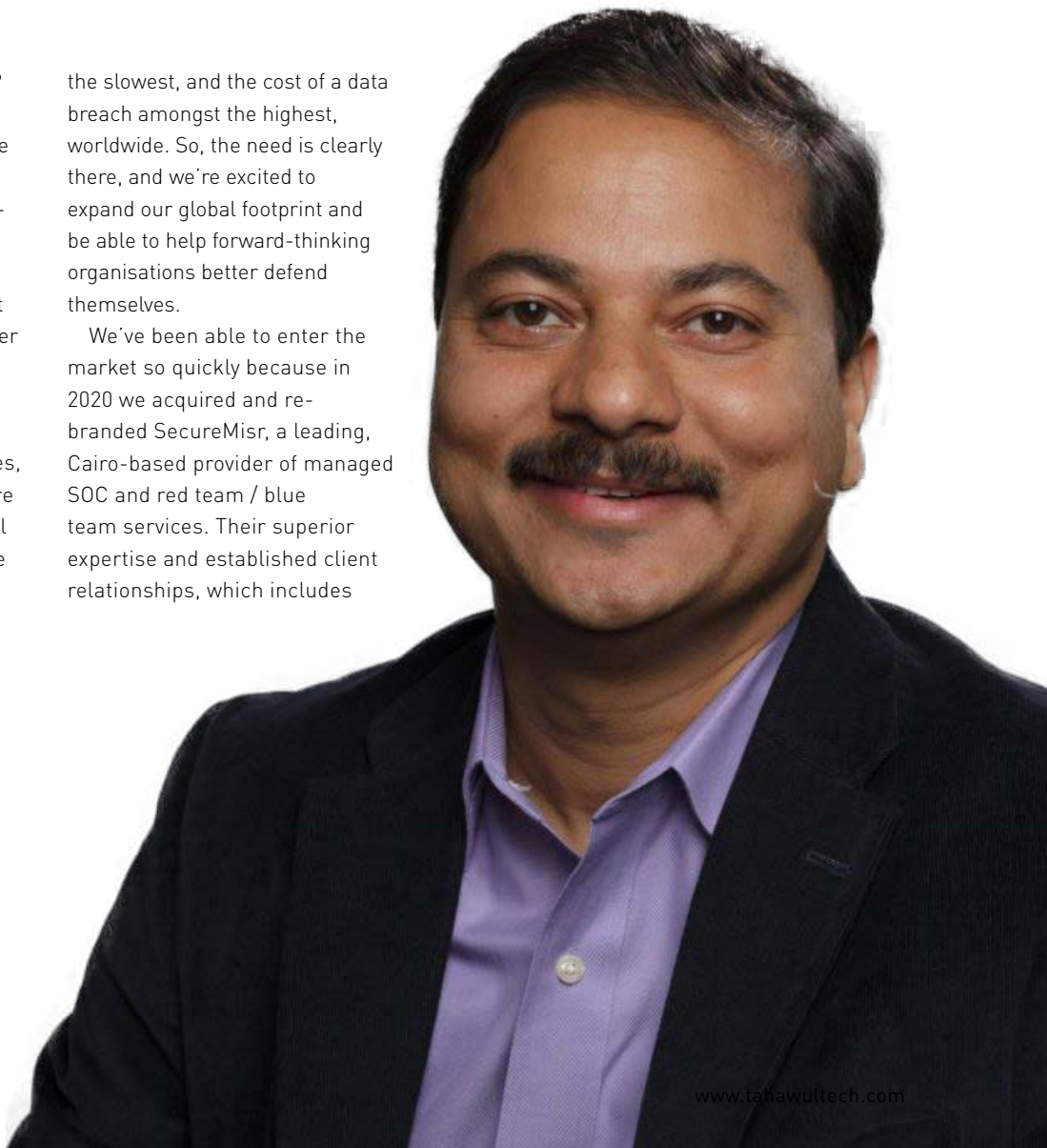
Cysiv is headquartered in Dallas, USA, and has offices in other countries, including now Egypt and UAE. We were incubated within Trend Micro, a global cybersecurity leader, and now operate as an independent company. We're backed by the largest VC firm that focuses exclusively on cybersecurity, and in addition to Trend Micro, have an important strategic alliance with Google Cloud.

Cysiv is entering the Middle East market in a big way. What does this mean for the company?

We believe there's a tremendous need for SOCaaS in the region. The average time to detect and contain a breach by organisations in the region is amongst

the slowest, and the cost of a data breach amongst the highest, worldwide. So, the need is clearly there, and we're excited to expand our global footprint and be able to help forward-thinking organisations better defend themselves.

We've been able to enter the market so quickly because in 2020 we acquired and re-branded SecureMisr, a leading, Cairo-based provider of managed SOC and red team / blue team services. Their superior expertise and established client relationships, which includes



many Global 2000 organisations in banking, financial services and telecommunications, has allowed us to accelerate our investment in the region.

What can the Middle East market look forward to, from Cysiv?

Cysiv's existing clients in the region will continue to receive the same expertise and service they've come to rely on over the past 12+ years. Our regional leadership team remains unchanged, and their deep knowledge, experience and understanding of the different industries and the regional threat environment, is central to our business and the value we provide. And we look forward to introducing them to the incremental benefits of SOCaaS. We'll also be investing heavily in the region, as we open additional offices, expand our regional SOC operation, and hire security experts, data engineers and sales professionals that further strengthen our local presence. We're very excited by the talent pool in the region, and we understand how important it is to serve Middle East clients with local experts.

Ultimately, with Cysiv, CIOs and CISOs can reduce the risk of costly and damaging breaches and business disruptions, and more readily support regulatory compliance requirements. This in turn will inspire greater trust and business confidence from their end customers.

What exactly is SOC-as-a Service and why is it relevant today?

SOCaaS provides enterprises with all the benefits of having their own world-class 24/7 SOC, but without the tremendous costs, complexity or time required to build, staff and operate one themselves. With our cloud-native,

“TRADITIONAL APPROACHES TO SECURITY SIMPLY HAVEN'T WORKED.”

next-gen SIEM, advanced use of data science and automation, and our ability to quickly and effectively leverage telemetry from across an organisation's entire IT environment, including on-premise and multi-cloud environments, we're able to deliver value that traditional MSSPs and MDR providers simply cannot.

The reason SOCaaS is relevant today is that traditional approaches to security simply haven't worked.

Despite all of the investments that organisations have made in firewalls, IDS/IPS appliances, endpoint detection and response and other security solutions, threat actors are still able to readily inflict massive damage by stealing valuable customer data and intellectual property and disrupting business operations.

An effective SOC—one that combines the right technology, experts and processes, and is able to deal with terabytes of telemetry and data from across the enterprise, and not drown its analysts in false positives and too many alerts—is tremendously expensive, complex and time-consuming to build, staff and operate. And until now, it's been beyond the reach of most organisations. Cysiv solves this problem.

How do you evaluate the threat landscape today?

Threat actors have gained the upper hand, and the proof is in the news headlines that have become all too common. Every industry in every country is under attack,

around the clock. Threat actors, including disgruntled employees, hackers and hacktivists, organized cybercrime rings, and nation states are more sophisticated and motivated than ever. The attack surface they can target has grown dramatically as enterprises adopt IoT, mobile and cloud computing, and try to support pandemic-driven work-from-home policies. And the weapons and techniques threat actors now have access to have made it increasingly difficult to quickly detect and actively respond to ransomware, advanced malware, business email compromise and other cyber threats, before it's too late.

What are the main cyber security challenges that the region is facing today?

They're no different than the key challenges faced by organisations in every other country. First and foremost, advanced threat detection and response is now primarily a big data problem: the signals of an attack or compromise are there, but finding, correlating and responding to them in a timely manner, is extremely difficult. To do this requires a team of highly skilled and collaborative data scientists and engineers, security analysts and incident responders, and threat researchers and hunters. Unfortunately, there aren't nearly enough of these people to go around. And operating a SOC is not a core competence for organisations. Nor should it be.

Cysiv overcomes these challenges by combining SOC technology—including a cloud-native next-gen SIEM, data science, machine learning, threat intel and automation—with a team of experts, and delivering them as a subscription-based service that can be quickly implemented, and that operates as an extension to your IT and security team. 🧑‍💻

COMBATING CYBERCRIME WITH AI-DRIVEN SECURITY STRATEGIES

BY **DEREK MANKY**, CHIEF, SECURITY INSIGHTS & GLOBAL THREAT ALLIANCES, FORTIGUARD LABS



As technology evolves, so too does cybercrime. The recent rise in remote work and the broadening of the attack surface that accompanied it have shown that cyber criminals are nothing if not resourceful and opportunistic. So, as bad actors advance their tool kits to include artificial intelligence (AI) and machine learning (ML) strategies, those who defend against cyber attacks must do the same.

AI-driven security technologies have the potential to anticipate attacks and counter them in real-time. Given that cyberattacks of the future are expected to occur in microseconds, the ability to react at machine speeds is crucial. The role of humans in defending against attacks will shift, focusing instead on ensuring that enough intelligence is fed into security systems to make them successful.

The Need for AI-driven security and ML in the Modern Threat Landscape

Rich media services, increasingly intelligent endpoint devices, semi-intelligent IoT devices, and the emergence of 5G capabilities have combined to create new edge networks and fundamentally change how data is shared. This ongoing shift in how people work and live creates a host of new security concerns to address. Not only are AI-driven technology and ML useful in protecting against attacks, but when the prospective attackers are using that same technology, it becomes a necessity.

Bad actors are already using AI and ML to their advantage, building platforms to deliver

malware at unprecedented speeds and scale. And because humans alone cannot keep up with the increasingly complex techniques deployed by cyber criminals, those in the threat detection business must use AI, ML, and automation to maintain an edge over these malicious actors.

Proactive Security Using AI and ML

Staying ahead of cyber threats requires proactive strategies. As a general rule, it's much easier to have proper defense measures in place before something happens rather than having to undo the damage after an attack. Organisations can transition to proactive security strategies by using AI/ML techniques and sandboxing to analyse information gathered from global threat intelligence networks. Training systems using all three ML learning modes—supervised, unsupervised, and reinforcement learning—further increases accuracy over time.

A successful security-driven networking approach will be one that joins AI-driven security systems with modern threat intelligence and networking technologies to create a unified system. With this strategy, security becomes woven throughout the network in the form of segmentation, behavioral analytics, and zero-trust access. In addition, a distributed security system that replaces traditional sensors with learning nodes can both gather information and function as the first line of defense. In this way, it acts similarly to the human nervous system. Such a system is made possible by using

stored knowledge supplemented with ML for threat detection and coarse-grain response.

The Human Element in Modern Cybersecurity Practices

The use of AI and ML in cybersecurity solutions, along with automation, will also lead to a shift in the role of cybersecurity professionals. Next-generation cybersecurity technologies enable integrated, enhanced user interfaces that leverage task automation. This makes it easier to onboard new junior staff and requires less senior-level staff oversight. Moreover, these technologies can effectively compensate for the cybersecurity skills gap and leave more meaningful and high-value work for the humans involved, thereby increasing staff retention.

AI-driven Cybersecurity is the Future

Modern networks are increasingly complex, requiring inhuman levels of awareness and response to keep them safe. As cyber criminals deploy increasingly sophisticated attacks powered by AI and ML, cybersecurity professionals must use those same technologies in response. The threat landscape will continue to evolve, meaning AI-driven systems, trained and refined by humans with high-quality data, will grow more essential as a means to protect digital assets. 🛡️

Bringing IT together

ManageEngine crafts comprehensive IT management software for all your business needs.



Service Management | Identity and Access Management

Security Information and Event Management | IT Operations Management

Unified Endpoint Management and Security | Advanced IT Analytics

ManageEngine

a division of Zoho Corp.

www.manageengine.com

NextGen SOC: the key to cyber resilience

TAMER EL REFAEY, CHIEF CYBERSECURITY STRATEGIST, EMERGING MARKETS, MICRO FOCUS, TELLS *SAME* THAT WITH THE RIGHT TECHNICAL CAPABILITIES, NEXTGEN SOCS CAN HELP FILTER OUT 'NOISE' AND OVERCOME THE MAJOR CHALLENGES SURROUNDING CYBER SECURITY.

Proper security visibility is the dream of every organization. Knowing if something malicious is stealthily taking place in the environment and stopping before it causes a business impact is the ultimate goal of every security investment. Next-generation (NextGen) SOC was used and sometimes overused by multiple technology providers to give their customers hope to achieve that dream. In other situations, other security technology providers questioned the existence of the SOC, altogether.

Organizations are left baffled whether a NextGen SOC is a viable option or not. Is it technology? Can we buy a NextGen SOC? Can we transfer an existing SOC into a NextGen SOC?

The Need for a NextGen SOC

Today's security operation centres face significant challenges that prevent them from achieving the goal they were built for. The top three of those challenges are:

- 1. Security visibility.** According to statistics, 78% of chief information security officers (CISOs) are concerned about monitoring across a growing attack surface.
- 2. Alert fatigue.** Around 75% of SOC professionals reported that they are suffering from a massive volume of security alerts.
- 3. Skill shortage.** 62% of surveyed SOC

managers complained about analysts' availability and experience.

NextGen SOC promises to overcome these challenges by enhancing the ability to detect compromise attempts and gain insights that allow the analysts to navigate through the noise and focus on smaller high-fidelity alerts. Additionally, next-generation SOC is supposed to ensure resource optimization and efficiency.

Key Areas of a NextGen SOC

To build the next generation SOC, we must focus on four key areas within the

SOC: business, people, process, and technology. The business aspect deals with the SOC's mission, operating model, stakeholders, and services. The people aspect is related to the SOC leadership, the hiring process, skill assessment, and SOC resources retention. The process aspect focuses on the different processes and procedures within the SOC to execute the day-to-day activities, ensure SOC maturity and evolution, and prepare for the future.

For the remainder of this article, we will focus only on NextGen SOC's technology aspect.

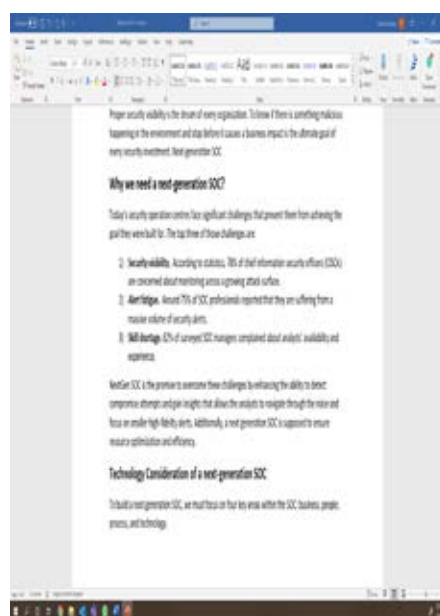


Figure 1: Different aspects to build a NextGen SOC.



Tamer El Refaey Chief Cybersecurity Strategist,
Emerging Markets, Micro Focus

Technology Aspect of a NextGen SOC

Technology plays a significant role in building a NextGen SOC. It is also the area where most of the investment is made. Multiple technology considerations should be considered when building a SOC, in general. The SOC architecture, the quality of data that is ingested, the technology ecosystem of the SOC, etc. are few examples of technical capabilities that should be carefully considered.

However, to capitalize on these foundations and mature into a NextGen SOC, five key capabilities make a big difference: metrics and KPIs, layered analytics, advanced content, improved context, and intelligent autonomy.

CLEAR METRICS

It is said that we cannot improve what we cannot measure. The same is true for

the NextGen SOC. Metrics and KPIs are the tools that allow management to know whether the SOC is delivering according to expectations, the areas of improvements, and where to focus efforts and time. Metrics and KPIs can help other cybersecurity teams make the right decisions to enhance the existing security controls.

NextGen SOC metrics fall, generally, into four categories; purpose, posture, performance, productivity. Most security operation centres focus on the last two; performance and productivity are more comfortable to measure and report. However, a NextGen SOC needs to ensure its alignment to business and role in enhancing the overall security posture of the organization

a.) Purpose. These are metrics and KPIs that measure the reason a SOC was formed. Some examples are avoided financial losses, reduction in customer fraud, prevented data breaches, etc. Better numbers show that the SOC is fulfilling its purpose.

b.) Posture. Metrics and KPIs related to posture are meant to measure how good or bad the organization's security. Examples may include the number of successful breaches, the number of open vulnerabilities, the percentage of failed security controls, etc. Reductions in these numbers show the organization's more robust security posture.

c.) Performance. Performance metrics and KPIs are meant to measure how good the SOC is in dealing with cybersecurity incidents. Examples may include mean time to detect (MTTD), mean time to respond (MTTR), breaches Vs incidents, etc. These indicators can provide SOC leadership with visibility on areas that need their attention.

d.) Productivity. Metrics and KPIs associated with productivity are designed to measure the efficiency of the SOC. Some examples include the false positive rate, the average time to close a ticket, the average number of alerts per analyst, adherence to service level agreements (SLA), etc. These indicators should be used to revise the workforce capacity, resources that require further training, and areas where automation would be much needed.

LAYERED ANALYTICS

It is the ability to look at the data in hand using different lenses that could lead to enhanced visibility, better insights, different outcomes, and high-quality decisions. The various analytics that can be used inside the SOC are:



Figure 2: Types of SOC metrics and KPIs.

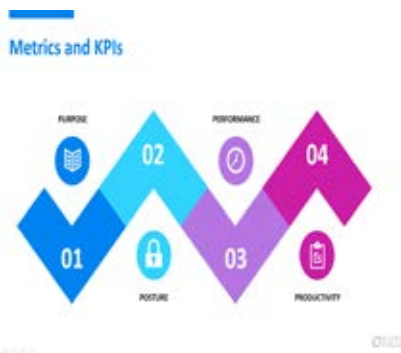


Figure 3: Layered analytics capabilities within NextGen SOC.

Real-time correlation. It works on detecting policy violations and meeting certain pre-defined conditions. This type of analytics is meant to detect document and well-known kind of attacks using traditional analytical tools.

Real-time correlation is still essential as it helps spot most of the conventional attacks that a SOC faces daily. Responses to these types of alerts should be, mostly, automated. A SOC analyst should not spend much time on dealing with alerts resulted from real-time correlation.

Big data analytics. This type of analytics builds relationships between different datasets that can provide an extra level of insights. Big data analytics can detect undocumented attacks using conventional analysis tools.

Supervised machine learning. Supervised ML is usually used to detect low and slow documented attacks by training the machine on previous attack models using pattern matching. It is instrumental in detecting known attacks that require unconventional analysis capabilities. Malware infection, spam

Unsupervised machine learning. This type of analytics is beneficial to detect unknown attacks that require advanced analysis capabilities. Mathematical data models are used to build behaviour profiles that would flag observed abnormality. The main benefit of unsupervised machine learning that you do not require training datasets. Yet, the behaviour profiles are continuously enhanced as more data is analyzed.

IMPROVED CONTEXT

Context is king. The bigger the picture we see, the accurate the decisions we take. To support the initiative of NextGen SOC, the following minimal context information must be integrated:



Figure 4: Examples of context information.

a.) Asset information. Not all assets are created equal. The SOC team needs to understand which asset is under attack, the asset criticality to the business, the information it handles, the asset network model, and any other information that quickly allows the analysts to make the right decision.

b.) Vulnerability information. Information like open vulnerabilities, compliance status, source code potential issues can provide the SOC analysts with security alerts with more prioritization.

c.) Identity information. Identity and access information add situational awareness that can help the SOC team prioritize alerts, decide on the abnormality of activity, and automate incident response in many cases. For instance, details of new joiners, leavers, privilege users, high-value targets, access details, etc. are critical to adding the analysts' proper understanding.

d.) Intelligence information. Threat intelligence has been a critical component of the NextGen SOC. Consuming different threat feeds and indicators of compromise have been proven helpful. NextGen SOC should expand in leveraging intelligence

information by integrating open-source intelligence, commercial feeds, and ensuring their awareness of world news that may impact their organization. The news of COVID-19 pandemic would alert the SOC to expect increased COVID-related phishing campaigns.

ADVANCED CONTENT

Content is needed to analyze the collected data into the SOC. Content can exist in the form of analysis rules, data models, reports generated, etc. When developing or selecting content, four key objectives need to be considered:

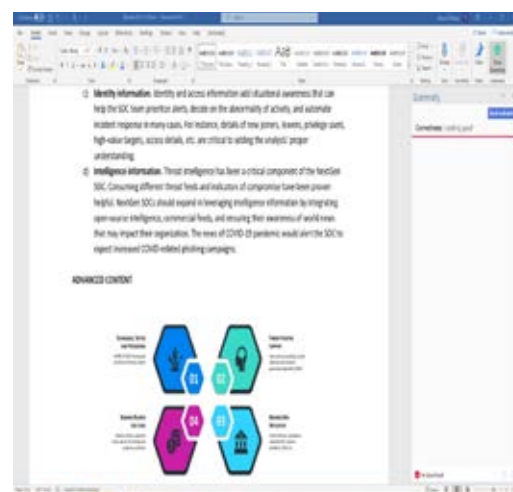


Figure 5: Categories of content used inside NextGen SOC.

a.) Techniques, tactics and procedures (TTP). SOC's can use known patterns of activities or methods associated with a specific threat actor or group of threat actors to detect threat actors while performing their attacks. Frameworks such as MITRE ATT&CK can provide great content that the SOC can use.

b.) Threat hunting support. NextGen SOC's should have the ability to develop or leverage content that can simplify and mature their threat hunting capabilities. Such content should be provided by the different technologies used or through reports or dashboards that can be created. Some examples of such content can be host and user profiling, outlier detection, domain generation algorithms (DGA), etc.

c.) Business risk mitigation. One of the main objectives of NextGen SOC is to enhance the security posture of the organization. Content that supports this objective is mandatory to ensure optimal risk mitigation. For instance, NextGen SOC should be able to pinpoint security control failures, regulatory compliance nonconformity, business process deviation, segregation of duty violations, etc. that could impact the

organization's data confidentiality, integrity, and availability

d.) Business-related use cases. A NextGen SOC is the one that supports and enable the business. A NextGen SOC should develop content that is business aligned and can provide early detection of attacks on the company. For example, content that monitors SWIFT, ATM, OT networks, telecom infrastructure is critical.

INTELLIGENT AUTONOMY

With the struggle to find qualified resources, NextGen SOC should work towards autonomy where the dependency on the human element is minimal whenever possible. Automation is one aspect of SOC autonomy. However, it is only focusing on orchestrating and automating the incident response. The term intelligent autonomy is meant to be wider than the incident response. It looks at the different non-intellectual activities that a SOC analyst does and move them to the machine. Examples may include SOC self-diagnosis and healing, leveraging robotic-process automation to mimic human actions, providing access to information using voice commands, etc.

NEXTGEN SOC SHOULD WORK TOWARDS AUTONOMY WHERE THE DEPENDENCY ON THE HUMAN ELEMENT IS MINIMAL WHENEVER POSSIBLE.

CONCLUSION

NextGen SOC is becoming critical for the success of organizations cyber resilience endeavour. The main technical capabilities that a NextGen should have are clear metrics and KPIs, layered analytics, improved context, advanced content, and intelligent autonomy. 🧑🏻

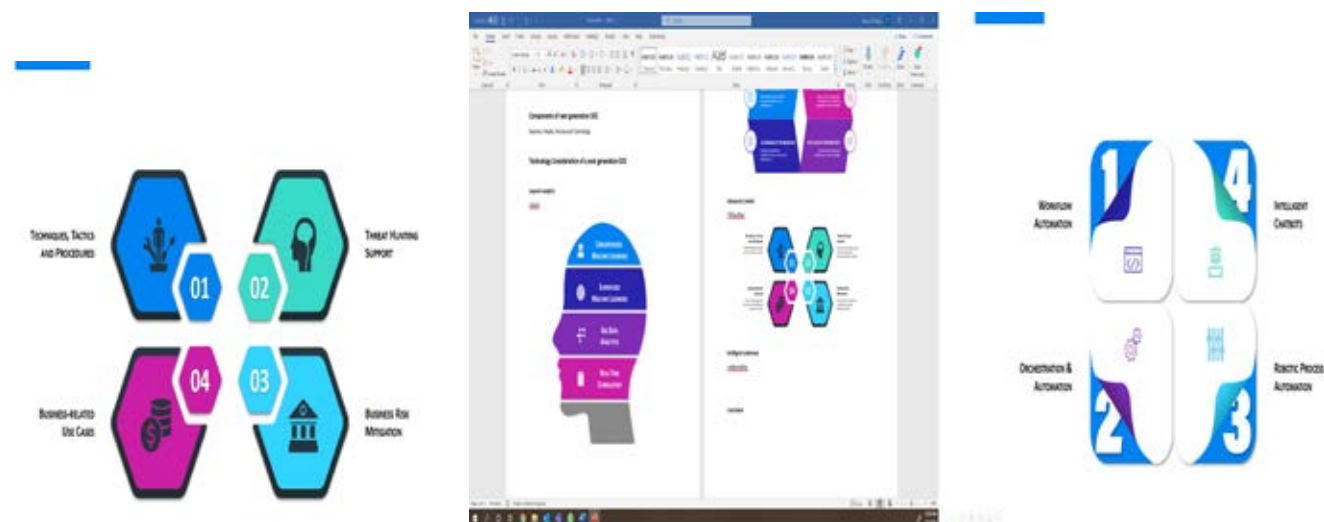


Figure 6: Evolution of automation capabilities.



AVIENTEK

Distributor of Audio Visual & IT Products

Middle East | India | Africa



ENHANCE YOUR MEETING WITH PROFESSIONAL AV

ARE YOU ON THE RIGHT TRACK ?

- Video Conferencing
- Audio Conferencing
- Wireless Microphones
- Wireless Collaboration
- Interactive Display
- Professional Display
- Camera Extenders
- Video Wall Processors
- Media Streaming
- AV Mounting Systems
- AV Furniture
- AV Distribution Systems
- AV Racks
- Retractable Monitor
- Control Systems

 **CRESTRON**

EPSON

 **legrand** | AV

logitech®

NEC

ClearOne.

CLEVERTOUCH

 **DIGIBIRD**

 **DTEN**

 **OPTERNA**

PureLink

 **PureLink™**

SCREENLINE

 **SOLTEC**

 **WOLFVISION**

AVIENTEK LLC: Office#107, API Business Suites, Sheikh Zayed Road, Al Barsha 1, Dubai, UAE. Tel: +971 4 343 6216

AVIENTEK FZE: PO. Box-341290, Dubai Silicon Oasis, Dubai, United Arab Emirates

AVIENTEK TRADING WLL: Office# 26, Building-20, Street-940, Najma, C-Ring Road, Doha, Qatar.

MIMECAST REPORT: 78% OF ORGANISATIONS IN THE UAE WERE INFECTED WITH RANSOMWARE IN 2020

ANNUAL "THE STATE OF EMAIL SECURITY" REPORT ALSO FINDS 86% SUFFERED DISRUPTION OR FINANCIAL LOSS.



Mimecast Limited, a leading email security and cyber resilience company, has announced the publication of its "The State of Email Security" report. The report shows enterprises faced unprecedented cybersecurity risk in 2020 from increasing attack volume, the pandemic-driven digital transformation of work, and generally deficient cyber preparedness and training. The fifth annual "The State of Email Security," report is based on a global survey of 1,225 information technology and cybersecurity leaders, and supported by Mimecast's Threat Center data, which screens more than one billion emails per day.

Ransomware Looms Large

A full 86% of respondents indicated their companies had experienced a business disruption, financial loss or other setback in 2020 due to a lack of cyber preparedness. Respondents identified ransomware as the chief culprit behind these disruptions. Other insights include:

- 78% in the UAE indicated they had been impacted by ransomware in 2020, a massive increase from 66% of companies reporting such disruption in last year's "The State of Email Security" report.
- Companies impacted by ransomware lost an average of six working days to system downtime, with

29% of the companies in the UAE saying downtime lasted one week or more.

- 43% of ransomware victims paid threat actor ransom demands, but only 44% of those were able to recover their data. More than half (56%) never saw their data again, despite paying the ransom.

"The ransomware epidemic continues to rage, and the approaches to and results of remediation vary wildly. Many companies are choosing to pay ransoms rather than risking



extensive business downtime and expensive consulting fees to conduct self-remediation – but this introduces its own set of risks, including threat actors not holding up their end of the bargain. Paying ransom also makes companies an attractive target for subsequent attacks, since they’ve demonstrated they’re willing to pay.” Said Josh Douglas, Vice President of Threat Intelligence.

Threat Actors Exploit the Pandemic

While ransomware was a big problem for organizations in 2020, it wasn’t the only one. Mimecast’s “The State of Email Security” report also revealed additional threat trends, including:

- A 64% year-over-year increase in threat volume.
- An increase in email usage in seven out of 10 companies
- 40% of survey respondents noted they saw an increase in email spoofing activity.
- In the UAE, 88% said they are concerned about the risks posed by archived conversations from collaboration tools compared to the 71% globally.

All of these data points can be attributed to the pandemic: work-from-home increased email and collaboration tool usage, and threat actors sought to capitalise on the new “digital office” with massive waves of COVID-19-related social engineering attacks.

Cyber Preparedness is Lacking

Despite facing an elevated threat volume, the report found that companies aren’t doing well in the area of threat prevention. In addition to the 86% of local respondents who indicated a lack of cyber preparedness (compared to 79% globally), other notable findings include:

50% OF RESPONDENTS IN THE UAE SAID EMPLOYEE NAIVETE ABOUT CYBERSECURITY IS ONE OF THEIR GREATEST VULNERABILITIES.

- As many as half of those surveyed in the UAE said their organisations fall short in one or more critical areas of email security systems (compared to 40% globally), leaving employees open to phishing, malware, business email compromise and other attacks.

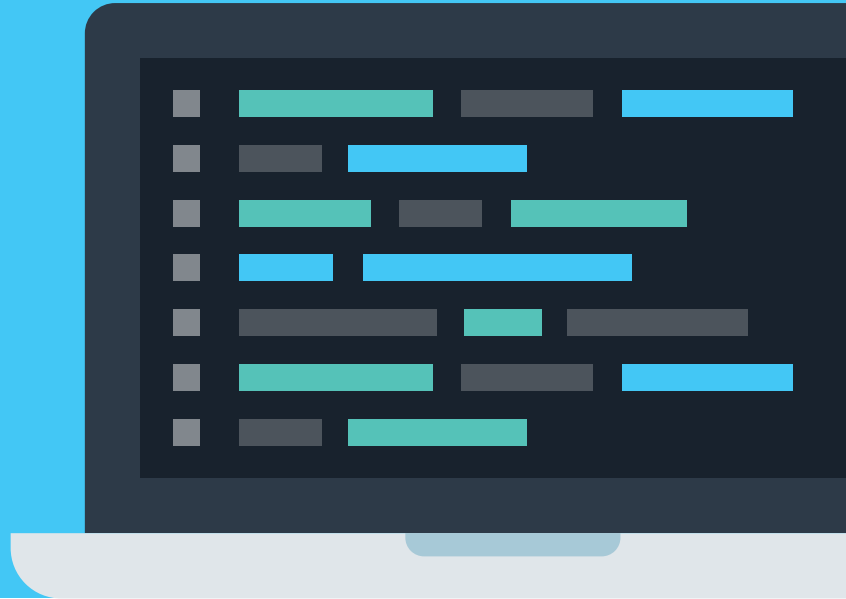
- 50% of the respondents in the UAE said that employee naiveté about cybersecurity is one of their greatest vulnerabilities, and yet only one in five respondents indicated they have ongoing (more than once per month) security awareness training in place.

“Companies know they are exposed but are not committing to the technology and training required to protect their environment. These exposure points are inflamed by so many companies rapidly adopting digital office models. Leaving employees untrained and unprotected in this highly distributed digital environment puts organisations at risk of digital deception,” added Josh Douglas.

Given these factors, it’s not surprising that 75% of survey respondents in the UAE believe their business will be harmed by email attacks in the next year. In 2020, 60% of respondents said they felt this way. 📌



Build Secure Software Fast with Fortify SAST



- ✓ **Find and fix** security vulnerabilities early and often with integrated SAST.
- ✓ **Launch fast, automated scans** from the Fortify platform or via your IDE and CI/CD pipelines.
- ✓ **Cover languages** that your developers love with support for 27 major languages and frameworks.
- ✓ **Protect against** open source component vulnerabilities with Sonatype software composition analysis.
- ✓ **Fix at the speed of DevOps** with machine-learning assisted auditing, rich analysis, filters, and issue templates.
- ✓ **Scale your AppSec program** with a static analysis farm that can be dynamically scaled to meet the changing demands of the CI/CD pipeline.

Learn more at microfocus.com/solutions/application-security

There's one thing even a
billion-dollar company can't afford:
a security breach

A person wearing a dark hoodie is holding a laptop in front of their face, obscuring it. They are standing in a dark, industrial-looking space with concrete pillars and windows in the background. The lighting is low, creating a mysterious and potentially threatening atmosphere.

Safeguard your IT
with
ManageEngine

Security Information & Event Management | Identity & Access Management
Network Security Management | Unified Endpoint Security & Management
Privileged Identity Management | Firewall Security Audit & Log Management

www.manageengine.com