PALO ALTO NETWORKS

CYBERPERSPECTIVES

SPRING 2024

NAVIGATING THE COMPLEX THREAT LANDSCAPE

ARTIFICIAL INTELLIGENCE

A New Era of Cybersecurity with AI: Predictions for 2024

SECURITY AS A BUSINESS ENABLER

Limiting Remote Access Exposure in Hybrid Work Environments

CYBER LEADERSHIP

ARTIFICIAL INTELLIGENCE

SECURITY AS A BUSINESS ENABLER

HEALTHCARE

ZERO TRUST

LATEST RESEARCH

Navigating the Complex Threat Landscape — Key Takeaways for CISOs

By Michael J. Graven

Well, it looks like we cybersecurity defenders won't be getting a break any time soon. Unit 42 consultants and intelligence analysts have been busy, and a few trends have jumped out at us in the last few months. So, we decided to write them up. In our latest executive advisory, Navigating the Evolving Threat Landscape: Resilient Cybersecurity Tactics for CISOs,[1] we highlight a couple attacker trends, what they mean, and what you can do about them.

The bottom line: attackers are becoming more tenacious and resilient to defense. Defenders can take a few steps to match those changes and improve their own organization's resilience.

Criminals Are Committing Crime More Efficiently

One trend is improved efficiency. More attackers now use automation, organization, playbooks and repeatable operations. Certain actors have developed key expertise in modern IT infrastructure. And, they use it to move efficiently through the target environment – faster and more quietly than before.

Muddled Libra is a threat group that's exhibited these skills. The Unit 42 Threat Assessment on Muddled Libra[2] has an in-depth written analysis, and you can also listen to the Unit 42 Threat Vector podcast for expert insights and strategies to counter this threat actor group.

States Are Sponsoring Attacks on Non-State Targets

Nation-state attackers don't just conduct espionage. Lately, they have also been acting to destabilize other components of the states they target. One example is Trident Ursa,[3] an APT group with a history of creating access to its targets and gathering information from them. Their targets include most business sectors: financial institutions and government entities,[4] communications, manufacturing, information technology, education and more.

If you run operational technology (OT), you might also be interested in some of the insights in this OT Security Insights white paper[5] from our OT colleagues. It looks at the IT-OT interface and how attackers are crossing it.

What Unit 42 Recommends

A comprehensive defense strategy helps you frustrate attackers. And, they deserve to be. The advisory goes into more detail. Here are some quick takes to consider.

1. **Change How You Measure Success**: Define success as how effectively you respond to active threats, not how you prevented everything bad – nobody does that.
2. **Constrain the Attacker**: Deny them time and space, and give it to your defenders instead.
3. **Lather, Rinse, Repeat**: Run your response playbooks efficiently and repeatedly.
4. **Increase the Pressure**: Everyone makes more mistakes when they're rushed.
5. **Measure and Reduce Your External Attack Surface**: Almost half the organizations we surveyed had a Microsoft Remote Desktop server open to the internet.
6. Work Toward Being a Zero Trust Enterprise: Asset inventories and user identity are some of the first questions incident responders ask. »

Being Thoughtful About Defense

These changes in attacker behavior aren't all bad news. On the contrary, it means a comprehensive defense strategy is more valuable against more threat actors. Attackers are innovating, accelerating and becoming more tenacious. Your team should be, too.

Unit 42 and other Palo Alto Networks products and services can help. We provide Cyber Risk Management and Incident Response consulting services – from attack surface assessment to full-scope reactive incident response. We're familiar and experienced with responding to threat actors – from APT to ransomware – in environments that include the largest Global 2000 firms.

This is just the beginning of what you need to know. Read the executive advisory, Navigating the Evolving Threat Landscape: Resilient Cybersecurity Tactics for CISOs to learn more about key attacker trends and tactical steps you can take to improve your security defense.

1. Unit 42. "Navigating the Evolving Threat Landscape: Resilient Cybersecurity Tactics for CISOs." *Palo Alto Networks*, 2 November 2023.
2. Russo, Kristopher, et al. "Threat Group Assessment: Muddled Libra (Updated)." *Palo Alto Networks*, 15 September 2023.
3. Unit 42. "Russia's Trident Ursa (aka Gamaredon APT) Cyber Conflict Operations Unwavering Since Invasion of Ukraine." *Palo Alto Networks*, 20 December 2022.
4. Rochberger, Lior, and Dan Yashnik. "GALLIUM Expands Targeting Across Telecommunications, Government and Finance Sectors With New PingPull Tool." *Palo Alto Networks*, 13 June 2022.
5. "OT Security Insights: Secure OT-IT Convergence to Keep the Production Lines Working." *Palo Alto Networks*, 16 October 2023.

Michael J. Graven is the director of Global Consulting Operations for Unit 42 at Palo Alto Networks

From Cybersecurity Webmaster to CISO

By Niall Browne

Navigating the Tides of Change & Building a Resilient SOC

Charting the course of my career, transitioning from a cybersecurity webmaster to chief information security officer (CISO), has given me unique insights (and scars) into the multifaceted nature of cybersecurity. Where prevention and incident response focus on what you need to do in order to avoid or handle cyberattacks in order to minimize fallout, a resilient SOC focuses on how to create efficient and repeatable processes. It not only ensures your ability to withstand an attack without catastrophic consequences, but also ingrains the idea of anti-fragility.

The transformation I've seen in cybersecurity over the past 15 years has been incredible. The idea of what to secure has expanded as the cloud, mobile devices and IoT has evolved. Multifactor authentication (MFA) and stronger encryption have become the norm rather than exceptions. And, more emphasis has been placed on continuous and holistic cybersecurity awareness, including through Zero Trust, real-time threat detection, attack surface management, vendor risk management and user education.

However, while the technology, adversarial tactics and security practices have changed quite a lot, the underlying philosophy within the security operations center (SOC) is still primarily focused on prevention and response alone. There needs to be a third pillar of cybersecurity philosophy – resiliency.

Every security incident should be a learning opportunity to build stronger defenses, and sometimes it may require a complete rethinking of how security works. »

The Cybersecurity Webmaster Era

When I began my journey as a cybersecurity webmaster, the internet was in its nascent stage. Websites were becoming digital storefronts, and the role of a webmaster was pivotal. Beyond ensuring the site was up and running, my task was to safeguard it from emerging cyberthreats.

Luckily for me, cyberthreats were relatively unsophisticated at this time. Simple distributed denial of service (DDoS) attacks, website defacement and basic malware were the primary concerns. The tools at our disposal were rudimentary. But, as online transactions and data sharing became more commonplace, the need for advanced security mechanisms became apparent.

The Transition to CISO

Taking the helm as a CISO, the strategic dimensions of cybersecurity came into sharper focus. Beyond merely ensuring technical safeguards, it became crucial to integrate cybersecurity into the very fabric of business strategy. The purview now encompassed risk management, crisis communication, regulatory compliance and, most importantly, aligning security imperatives with business objectives.

CISOs had to stop wondering whether security was strong enough if an attack happened. Instead, they needed to ensure processes were in place when an attack inevitably arrived. This is the foundation of building a resilient SOC – building efficient and easily automated processes to mitigate attacks as they come, minimizing the fallout, and finding ways to strengthen security with each hard lesson learned.

Monumental Industry Changes

Over the years, there have been instances where a new technology or strategy completely rethinks how security operates and greatly improves resiliency:

- **Shift to Zero Trust** – The traditional security model operated on the principle of "trust but verify," but verification methods always came with flaws and was replaced by the Zero Trust model. With Zero Trust, the default stance is mistrust, requiring verification for every user and device trying to access resources, irrespective of their location.
- **Cloud Security and Hybrid Environments** – With the surge in cloud adoption, securing hybrid environments that combine on-premises and cloud resources has become paramount. CISOs must ensure that data remains secure as it travels between these environments and as it resides in the cloud. Additionally, organizations need to be more diligent about attack surface management in the face of constant changes.
- **Automation and Intelligence** – SOCs today are flooded with data and alerts, and it is impossible to make sense of it all manually. CISOs must implement intelligent systems to ensure only critical tasks are seen by analysts and everything else is automated.

The Cyber Transformation Journey Faltered at Detection and Response

However, in the ever-evolving world of cybersecurity, one glaring challenge that many organizations continue to face is the duration it takes to detect and respond to cyber breaches. Threat actors can live off the land, using legitimate system tools to maintain persistent access and avoid detection.

Despite advancements in technology, many breaches still go unnoticed for weeks or months and, subsequently, take as long to prevent and contain. Even worse, the evidence of these breaches can be pulled together easily, but only after the fact. In a resilient SOC, those indicators of compromise should be surfaced automatically before the impact occurs.

This transformation has been stymied, primarily due the existence of the legacy SIEMs that we have all been forced to rely on. These legacy SIEMs have numerous challenges, including scalability issues, limited analytics capabilities, integration challenges, slow search and query performance, alert fatigue and lack of cloud-native support, among others.

Last year, we decided to take up the challenge and transform our detection and response program with resiliency in mind. We discovered, you can build a more resilient SOC by rethinking automation, data analytics and where security analysts fit into the process. This meant building a SOC platform that was » automation-first, could intelligently filter through alerts to surface true threats and could adapt to detect and stop even novel attacks. So, a vital component was shutting down our legacy SIEM and moving to the newly launched Palo Alto Networks XSIAM SOC platform.

We were able to complete this XSIAM transformation journey in a short 6 months. This provided us with an in-depth picture by pulling data from endpoints, network, cloud and identity systems, then normalizing and stitching it all together. We then applied our machine learning models to reduce our alerts, achieve a mean time to detect (MTTD) of 10 seconds and a mean time to respond (MTTR) of 1 minute for critical and high alerts.

The Resilient SOC: Essential Reading for CISOs

Are you up to transforming your detection and response program? If so, start your journey with building your resilient SOC. This new asset is an interactive digital experience where we feature seven chapters on security issues, such as supply chain risks, ransomware, automation and more, including a chapter on our Cortex portfolio. The future looks bright, and we're proud to be creating a safer version of it with the innovation we're providing today.

Niall Browne is the SVP and CISO of IT at Palo Alto Networks

What Executives Should Know About SOAR

By Zachary Malone

Coined in 2015 and later updated in 2017 by Gartner,[1] SOAR (security orchestration, automation, and response) describes a platform that is designed to orchestrate the response to incidents, leveraging automated processes designed in decision tree mapping, typically called playbooks.

The value of a SOAR platform is focused on improving the accuracy, speed, and depth of data for responding to the litany of incidents that operations teams (especially security operations) are constantly dealing with. To deliver on these values, most SOAR platforms leverage the playbooks mentioned above.

These playbooks have a listing of all the surrounding tasks, data, and implications that are needed to respond to a specific type of incident, which can then be automated as much as possible for routine tasks. This includes (but is not limited to) the following:

- Create a ticket.
- Gather preliminary data into a single repository.
- Notify involved parties.
- Compare the incident to known attacks.
- Pause for user input.

How Did SOAR Originate?

Gartner® originated the term "SOAR" during a time when the huge growth of virtualization, containerization, "as a service," and cloud really hit their stride in automating growth. This brought overwhelming amounts of data, assets, applications, and services into a company,[2] which begets »

> "Approaching a SOAR adoption should be a step taken on a journey of improvement of the security organization."

the need to secure it all. SOAR was the concept that looked to bring automation growth to this explosively expanding security coverage need.

Why Is It Important in Cybersecurity?

The concepts of SOAR are designed to ease a growing pain point that security programs continuously encounter as the businesses they serve expand: event and incident overload.

This pain comes from a need to analyze any and every event to verify any level of impact or concern to the business. When humans have to handle event reviews manually, the maximum number of events manageable is relatively low and expensive, while also unable to keep pace with the ability of technology to grow and create more events that need review.

What Is the Spin Around This SOAR Buzzword?

Far and away, the most egregious claim of SOAR is that it is the "only" tool a company needs to manage their security. This typically comes from the excitement of what a SOAR platform brings to a company's security and a lack of understanding and appreciation for how a SOAR platform is codependent on all the other tools included in a security strategy.

Another interesting claim is that "any programmatic process can be done via SOAR," which is not inherently wrong, it just misses the focus or the "S"/security and becomes OAR. This lack of focus creates the exact scaling and overwhelming issues as the amount of integration, processing, customization, and upkeep grow beyond any one department's ability to maintain.

Our Advice: What Executives Should Consider When Adopting SOAR

Approaching a SOAR adoption should be a step taken on a journey of improvement of the security organization. When your company is looking to improve the SOC in efficiency of time and error reduction, or streamline security processes to remove and reduce the risk blocking other business growth initiatives, then SOAR becomes highly compatible with that journey.

SOAR has incredible potential to solve massive scalability issues when properly adopted and maintained. Integrations should be simplified, robust, and prolific with a focus on the security tools and solutions that are already available.

Simplicity remains a key focus for implementation of the orchestration, automation, and response abilities of the platform, to avoid complexity merely expanding to this SOAR tool and not solving the removal/reduction of said complexity.

Here are some questions to ask your team for a successful SOAR adoption:

- If the business were to double or more in the size of our **D.A.A.S.**, how would the SOC be able to maintain our security posture without the ability to increase worker count?
- What are the routine processes and workflows that we continuously repeat to maintain our security integrity and what triggers can we define for initiating these workflows?
- What systems and security-specific **D.A.A.S**. will need to be integrated into our approach to this new automation of our orchestration and response strategy and how difficult will it be to achieve fully integrated status?
- What other IT-based operations would benefit from having an OAR platform and how well can we enable them from the SOAR platform to achieve new heights?
- How effectively and quickly will operations teams be able to understand, create, and update the playbooks and case management systems and how much product and/or coding knowledge will need to be known?

[1] Neiva, Claudio, et al. "Innovation Insight for Security Orchestration, Automation and Response." *Gartner*, 30 November 2017.

[2] National Security Agency. "Embracing a Zero Trust Security Model." *Defense.gov*, 25 February 2021.

Zachary Malone is a technical enablement architect at Palo Alto Networks

A New Era of Cybersecurity with AI: Predictions for 2024

By Dr. May Wang

Artificial intelligence (AI) has been table stakes in cybersecurity for several years now, but the broad adoption of Large Language Models (LLMs) made 2023 an especially exciting year. In fact, LLMs have already started transforming the entire landscape of cybersecurity. However, it is also generating unprecedented challenges.

On one hand, LLMs make it easy to process large amounts of information and for everybody to leverage AI. They can provide tremendous efficiency, intelligence, and scalability for managing vulnerabilities, preventing attacks, handling alerts, and responding to incidents.

On the other hand, adversaries can also leverage LLMs to make attacks more efficient, exploit additional vulnerabilities introduced by LLMs, and misuse of LLMs can create more cybersecurity issues such as unintentional data leakage due to the ubiquitous use of AI.

Deployment of LLMs requires a new way of thinking about cybersecurity. It is a lot more dynamic, interactive, and customized. During the days of hardware products, hardware was only changed when it was replaced by the next new version of hardware. In the era of cloud, software could be updated and customer data were collected and analyzed to improve the next version of software, but only when a new version or patch was released.

Now, in the new era of AI, the model used by customers has its own intelligence, can keep learning, and change based on customer usage — to either better serve customers or skew in the wrong direction. Therefore, not only do we need to build security in design – make sure we build secure models and prevent training data from being poisoned — but also continue evaluating and monitoring LLM systems after deployment for their safety, security, and ethics.

Most importantly, we need to have built-in intelligence in our security systems (like instilling the right moral standards in children instead of just regulating their behaviors) so that they can be adaptive to make right and robust judgment calls without drifting away easily by bad inputs.

What have LLMs brought for cybersecurity, good or bad? I will share what we have learned in the past year and my predictions for 2024.

Looking Back in 2023

When I wrote The Future of Machine Learning in Cybersecurity[1] a year ago (before the LLM era), I pointed out three unique challenges for AI in cybersecurity: **accuracy**, **data shortage**, and **lack of ground truth**, as well as three common AI challenges but more severe in cybersecurity: **explainability**, **talent scarcity**, and **AI security**.

Now, a year later after lots of explorations, we identify LLMs' big help in four out of these six areas: data shortage, lack of ground truth, explainability, and talent scarcity. The other two areas, accuracy and AI security, are extremely critical yet still very challenging.

I summarize the biggest advantages of using LLMs in cybersecurity in two areas:

1. Data

Labeled data

Using LLMs has helped us overcome the challenge of not having enough "labeled data". »

High-quality labeled data are necessary to make AI models and predictions more accurate and appropriate for cybersecurity use cases. Yet, these data are hard to come by. For example, it is hard to uncover malware samples that allow us to learn about attack data. Organizations that have been breached aren't exactly excited about sharing that information.

LLMs are helpful at gathering initial data and synthesizing data based on existing real data, expanding upon it to generate new data about attack sources, vectors, methods, and intentions, This information is then used to build for new detections without limiting us to field data.

Ground truth

As mentioned in my article a year ago, we don't always have the ground truth in cybersecurity. We can use LLMs to improve ground truth dramatically by finding gaps in our detection and multiple malware databases, reducing False Negative rates, and retraining models frequently.

2. Tools

LLMs are great at making cybersecurity operations easier, more user-friendly, and more actionable. The biggest impact of LLMs on cybersecurity so far is for the Security Operations Center (SOC).

For example, the key capability behind SOC automation with LLM is function calling, which helps translate natural language instructions to API calls that can directly operate SOC. LLMs can also assist security analysts in handling alerts and incident responses much more intelligently and faster. LLMs allow us to integrate sophisticated cybersecurity tools by taking natural language commands directly from the user.

Explainability

Previous Machine Learning models performed well, but could not answer the question of "why?" LLMs have the potential to change the game by explaining the reason with accuracy and confidence, which will fundamentally change threat detection and risk assessment.

LLMs' capability to quickly analyze large amounts of information is helpful in correlating data from different tools: events, logs, malware family names, information from Common Vulnerabilities and Exposures (CVE), and internal and external databases. This will not only help find the root cause of an alert or an incident but also immensely reduce the Mean Time to Resolve (MTTR) for incident management.

Talent scarcity

The cybersecurity industry has a negative unemployment rate. We don't have enough experts, and humans cannot keep up with the massive number of alerts. LLMs reduce the workload of security analysts enormously thanks to LLMs' advantages: assembling and digesting large amounts of information quickly, understanding commands in natural language, breaking them down into necessary steps, and finding the right tools to execute tasks.

From acquiring domain knowledge and data to dissecting new samples and malware, LLMs can help expedite building new detection tools faster and more effectively that allow us to do things automatically from identifying and analyzing new malware to pinpointing bad actors.

We also need to build the right tools for the AI infrastructure so that not everybody has to be a cybersecurity expert or an AI expert to benefit from leveraging AI in cybersecurity.

Three Predictions for 2024

When it comes to the growing use of AI in cybersecurity, it's very clear that we are at the beginning of a new era – the early stage of what's often called "hockey stick" growth. The more we learn about LLMs that allow us to improve our security posture, the better the likelihood we will be ahead of the curve (and our adversaries) in getting the most out of AI.

While I think there are a lot of areas in cybersecurity ripe for discussion about the growing use of AI as a force multiplier to fight complexity and widening attack vectors, three things stand out:

1. Models

AI models will make huge steps forward in the creation of in-depth domain knowledge that is rooted in cybersecurity's needs.

Last year, there was a lot of attention devoted to improving general LLM models. Researchers worked hard to make models more intelligent, faster, and cheaper. However, there exists a huge gap between what these general-purpose models can deliver and what cybersecurity needs. »

Specifically, our industry doesn't necessarily need a huge model that can answer questions as diverse as “How to make Eggs Florentine” or “Who discovered America”. Instead, cybersecurity needs **hyper-accurate** models with in-depth domain knowledge of cybersecurity threats, processes, and more.

In cybersecurity, accuracy is mission-critical. For example, we process 75TB+ amount of data every day at Palo Alto Networks from SOCs around the world. Even 0.01% of wrong detection verdicts can be catastrophic. We need high-accuracy AI with a rich security background and knowledge to deliver tailored services focused on customers’ security requirements. In other words, these models need to conduct fewer specific tasks but with much higher precision.

Engineers are making great progress in creating models with more vertical-industry and domain-specific knowledge, and I’m confident that a cybersecurity-centric LLM will emerge in 2024.

2. Use Cases

Transformative use cases for LLMs in cybersecurity will emerge. This will make LLMs indispensable for cybersecurity.

In 2023, everybody was super excited about the amazing capabilities of LLMs. People were using that “hammer” to try every single “nail”.

In 2024, we will understand that not every use case is the best fit for LLMs. We will have real LLM-enabled cybersecurity products targeted at specific tasks that match well with LLMs’ strengths. This will truly increase efficiency, improve productivity, enhance usability, solve real-world issues, and reduce costs for customers.

Imagine being able to read thousands of playbooks for security issues such as configuring endpoint security appliances, troubleshooting performance problems, onboarding new users with proper security credentials and privileges, and breaking down security architectural design on a vendor-by-vendor basis.

LLMs’ ability to consume, summarize, analyze, and produce the right information in a scalable and fast way will transform Security Operations Centers and revolutionize how, where, and when to deploy security professionals.

3. AI Security and Safety

In addition to using AI for cybersecurity, how to build secure AI and secure AI usage, without jeopardizing AI models' intelligence, are big topics. There have already been many discussions and great work in this direction. In 2024, real solutions will be deployed, and even though they might be preliminary, they will be steps in the right direction. Also, an intelligent evaluation framework needs to be established to dynamically assess the security and safety of an AI system.

Remember, LLMs are also accessible to bad actors. For example, hackers can easily generate significantly larger numbers of phishing emails at much higher quality using LLMs. They can also leverage LLMs to create brand-new malware. But the industry is acting more collaboratively and strategically in the usage of LLMs, helping us get ahead and stay ahead of the bad guys.

On October 30, 2023, U.S. President Joseph Biden issued an executive order covering the responsible and appropriate use of AI technologies, products, and tools. The purpose of this order touched upon the need for AI vendors to take all necessary steps to ensure their solutions are used for proper applications rather than malicious purposes.

AI security and safety represent a real threat — one that we must take seriously and assume hackers are already engineering to deploy against our defenses. The simple fact that AI models are already in wide use has resulted in a major expansion of attack surfaces and threat vectors.

This is a very dynamic field. AI models are progressing on a daily basis. Even after AI solutions are deployed, the models are constantly evolving and never stay static. Continuous evaluation, monitoring, protection, and improvement are very much needed.

More and more attacks will use AI. As an industry, we must make it a top priority to develop secure AI frameworks. This will require a present-day moonshot involving the collaboration of vendors, corporations, academic institutions, policymakers, regulators — the entire technology ecosystem. This will be a tough one, without question, but I think we all realize how critical a task this is. »

Conclusion: The Best Is Yet to Come

In a way, the success of general-purpose AI models like ChatGPT and others have spoiled us in cybersecurity. We all hoped we could build, test, deploy, and continuously improve our LLMs in making them more cybersecurity-centric, only to be reminded that cybersecurity is a very unique, specialized, and tricky area to apply AI. We need to get all four critical aspects right to make it work: data, tools, models, and use cases.

The good news is that we have access to many smart, determined people who have the vision to understand why we must press forward on more precise systems that combine power, intelligence, ease of use, and, perhaps above all else, cybersecurity relevance.

I've been fortunate to work in this space for quite some time, and I never fail to be excited and gratified by the progress my colleagues inside Palo Alto Networks and in the industry around us make every day.

Getting back to the tricky part of being a prognosticator, it's hard to know much about the future with absolute certainty. But I do know these two things:

- 2024 will be a phenomenal year in the utilization of AI in cybersecurity.
- 2024 will pale by comparison to what is yet to come.

[1] Wang, May. "The Future of Machine Learning in Cybersecurity." *CIO*, 7 September 2022.

Dr. May Wang is the CTO of IoT Security at Palo Alto Networks

Securing Your AI-Powered Network Transformation: A Guide for C-Suite Leaders

By Anand Oswal

Complexity is the bane of all network security teams, and they will attest that the more dashboards, screens, and manual integration which they must juggle, the slower their response time. It need not be complex, it need not be disjointed, nor does it need to require adroitness in the art of juggling.

Your network makes engagement with customers, suppliers, and your workforce possible and must include a comprehensive security solution with consistent experiences across the board. Your workforce may be in any location, be it in the office, on the road, or working from home. The network security solutions being used by far too many are unnecessarily complex.

The time for change was yesterday, the opportunity for transformation is today. Artificial intelligence (AI) and generative AI capabilities have advanced, and this means that today enterprises that embrace the transformation and adopt platformization can look across their infrastructure through a single pane of glass and deal with security incidents in near-real time to meet the challenges of today's environment.

Today, criminal entities are able to mount their exploits quicker than ever before. Their ability to have their exploits work at machine speed, means that network security must also be working at machine speed. »

> **The time for change was yesterday, the opportunity for transformation is today."**

This puts tremendous pressure across your network's security stack to identify, isolate and remediate incidents as they occur. Now we must measure resolution in minutes or seconds.

Threats have historically been analyzed in a siloed manner, where the exploit was taken into a protected environment (sandbox) and analyzed and a solution produced and distributed. Clearly not machine speed.

Clearly, there is a need for change, for leveraging the advances provided by AI which increases visibility, accelerates identification of threats. By sending user traffic through the network security infrastructure, the application of AI and Machine Learning (ML) on the traffic makes it possible to find the threats and to block them inline.

Platformization Leveraging AI

The unified security stack, platform approach, brings to the forefront the knowledge afforded by the Palo Alto Networks global footprint. This obviates the myopic vision that the industry has historically embraced, point solution products.

The opportunity which AI presents is amazing, our ability to understand the risks and threats increases as the information becomes a part of our corpus. This corpus permits us to implement generative AI in a powerful manner across the entire suite of our offerings. In doing so, the accuracy of identifying threats is not only increased, the ease of use and understanding follows, with a single pane of glass view.

With the natural language processing provided by the AI/ML the expected acceleration of risk identification and remediation is evidenced. Your information security team no longer must be solely versed in the unique cybersecurity nomenclature, but they are also able to ask questions such as along the lines of "what is the risk or threat being presented" or "what are the recommended paths to remediation" or "what processes may need adjusting" and have the answer provided. It is important to emphasize, with the unified security stack, the implementation is ordered once and implemented across the infrastructure, addressing all areas affected. The power of natural language engagement and generative AI implementation in the correct manner provides visibility into root cause and pathways to remediation, which is the desired destination.

Yet not all security platforms are created equal. The platform must be innovative, it must be comprehensive, it must be integrated, and it must be able to operate in real time. These four components are key to the platform approach embraced by Palo Alto Networks.

Innovated Transformation

In sum, the time for transformation is today, the advances in understanding the power of AI have arrived, the ability to bring speed, clarity and address threats known and unknown are in hand. The ability to segment incidents and problems is now possible resulting in the reduction of information technology team escalations.

Leaders do not eschew innovation; indeed, they embrace it as it provides competitive advantage and the opportunity to leapfrog and disrupt one's sector. Adversaries are also innovative and their reduction of time from compromise to exploitation from 44 days to hours provides us with sufficient evidence of their level of innovation. We are not, however, operating in a vacuum and we at Palo Alto Networks are blessed with visibility which enables us to employ AI strategically and comprehensively into our solution.

Anand Oswal is the SVP of product for Network Security at Palo Alto Networks

SEC Rule Sparks Reimagining of Cybersecurity Operations

By Nikesh Arora

The U.S. Securities and Exchange Commission (SEC) has placed cybersecurity at the center of public company governance with its new cybersecurity incident reporting rule.[1] Companies must disclose not only information on their cybersecurity risk management processes in their annual reports but also any cybersecurity incident, or series of incidents, that are "material" to the company and must do so within four days of determining that the incident was material. Regulators around the globe are requiring that companies report more about cyber incidents in defined sets of time and, in doing so, are illuminating a truth we have long known – organizations must embrace a new approach to implementing security solutions to defeat motivated, well-financed and ever more sophisticated cyber attackers.

In finalizing the rule, the SEC observed that disclosure and reporting practices varied across publicly traded companies, and reasoned that a more standardized approach would better serve investors. Unfortunately, a standardized approach reflecting most companies' capabilities today would not yield impressive results. According to the up-to-date analysis of incident response from Unit 42, it takes companies an average of 5.5 days to initially contain an incident once discovered, and full recovery and remediation can take additional weeks or even months. These numbers are underwhelming, but they are not surprising given the flawed way too many organizations select and use their security solutions. Organizations are deploying disaggregated products to address discrete threats that do not provide a holistic picture of the threat landscape, unify data into actionable insights, or proactively hunt for potential attacks. The result is a 55% increase in vulnerability exploits in the wild from 2021 to 2022 (source: 2023 Unit 42 Network Threat Trends Research Report).[2]

We can do better and these regulatory trends should catalyze companies to consider how best to dramatically reduce their chances of ever having a material incident in the first place. The next generation of AI-powered cybersecurity solutions, such as Cortex XSIAM® from Palo Alto Networks, are built to meet and defeat the cyberthreats we see now and expect to see in the future and, in the process, drive significantly faster and better security outcomes. A common sense framework underpins the advanced capabilities of XSIAM, which will enable any company to reimagine its security operations.

1. A security architecture that employs an integrated, best-of-breed platform reduces risk, simplifies processes and provides better outcomes. According to Palo Alto Networks 2022 What's Next in Cyber survey,[3] over 65% of organizations want to consolidate their security solutions because existing point solution-based architectures are not sufficient to mitigate the kinds of threats that security operations centers (SOCs) confront today. A consolidated platform shares intelligence across data points, dashboards and user experiences to better prevent zero-day threats in real-time while reducing the risks inherent in integrating point »

products. You achieve better security when every part of your cyber stack works together. This isn't complicated calculus. It's common sense.

2. Effective threat detection and investigation requires access to significant amounts of data from varied sources. Cortex XSIAM natively integrates telemetry from any source, analyzes it and then stitches the resulting intelligence together into a single, comprehensive view of cyber incidents and threats. It integrates Unit 42 security research expertise with critical data from first-party sensors across endpoint, network and cloud to lay the foundation for high-quality analytics.

3. This rich data must be analyzed at machine scale, with automation driving the SOC. Doing so will dramatically improve two key metrics that determine the effectiveness of any SOC: mean time to detect (MTTD) and mean time to respond (MTTR). If your MTTD is on the order of seconds and your MTTR is on the order of minutes, you have the best possible chance of identifying an incident and assessing its materiality as soon as possible. This gives you the best chance to react to the incident and mitigate its effect. Yet all too often, we observe MTTD of hours to days and MTTRs of days to weeks or even months. Simply put, this is no longer a human-scale problem.

4. Companies should employ an integrated, single view of the cybersecurity landscape that triages every alert and incident at a machine scale, delivering a causality chain and an automatic determination of severity and impact. Most companies manage to assess 30-50% of alerts. In this threat environment, a partial solution is usually no solution.

XSIAM employs every element of this framework today. It is an AI-powered platform that can revolutionize the SOC and deliver step-function improvements in MTTD and MTTR. The platform combines our knowledge of every known attack pattern (Palo Alto Networks detects over 275,000 new attack patterns each day) with AI-based prediction and analytics to protect against new, as yet unseen attack patterns. With prebuilt integrations to over 900 cybersecurity products, XSIAM allows companies to remediate incidents in near real-time, using the richest, context-aware playbooks in the industry.

XSIAM produces staggering improvements in outcomes. Historically, the Palo Alto Networks SOC analysts spent most of their day triaging alerts, with each analyst manually investigating about 13 incidents per day. After deploying XSIAM, those same analysts now spend 70% of their day threat hunting and running attack simulations because they enjoy 100% alert coverage from AI and automation. Manual incident investigations are down to eight per day and, most crucially, the SOC has reduced its MTTD to less than one minute, and its MTTR to a few minutes. And, in the last three years, the average number of events presented per day has increased from one billion to 36 billion.

That is the power of XSIAM – true, machine-scale AI applied to analyze large amounts of data in real-time to protect against known and unknown threats. This automated solution will facilitate an organization's determination of whether an incident is "material" and dramatically reduce its remediation window from days and hours to minutes.

Finally, a full reimagining of your security operations requires additional strategies:

- **Proactive Cyber Offenses – a Better Offense Makes for Better Defense**: Organizations need the foundational components for an industry-leading cybersecurity program, including an automated attack surface management solution that accurately inventories their global internet-facing assets, to allow for discovery and mitigation of risk. On average, our Cortex Xpanse customers find 35% more assets than they previously tracked. Attack Surface Management is also an integrated module of the XSIAM platform.
- **Reconsider Your Governance Model** – Managing cybersecurity risk is not exclusively the responsibility of CISOs and IT teams. Corporate boards are key players in the effort. Consider establishing a separate security committee for the board. After all, ensuring that effective plans are in place to mitigate cyber risks, which can »

shut down a business, is as important as the work of audit committees to address financial risks.

- **Get That Incident Response Plan Battle Ready and Test** – Companies should prioritize the development of a comprehensive incident response plan that includes how to engage key experts from across the enterprise and then simulate events to test the organization's readiness to respond and remediate effectively.
- **Call in the Experts** – CISOs should prioritize assembling a team of dedicated incident responders and cybersecurity experts. These professionals are primed to spring into action when a cybersecurity incident arises, armed with a deep understanding of the organization's unique landscape and regulatory requirements.

The SEC's new incident reporting rules reflect one of the core challenges of our age – protecting our digital way of life from persistent, tenacious and ingenious cyber attackers. A marriage of smart, next-generation security platforms and sound corporate governance practices will be a powerful means to meet this challenge.

1. "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies." *SEC.gov*, 26 July 2023.
2. Unit 42. "2023 Unit 42 Network Threat Trends Report." *Palo Alto Networks*, 6 June 2023.
3. "What's Next in Cyber." *Palo Alto Networks*, 13 December 2022.

Nikesh Arora is the CEO and Chairman at Palo Alto Networks

Limiting Remote Access Exposure in Hybrid Work Environments

6 Recommendations Organizations Can Follow to Develop a More Practical Approach to Maintaining Secure Control over Infrastructure

By Matt Kraning

Remote work began as a temporary measure during the pandemic but has long been a permanent fixture in our new way of working. Organizations have shifted to remote desktop work environments at an increasing speed since then – simultaneously expanding their attack surface and exposing themselves to greater cybersecurity threats. The remote work revolution has pushed companies to rethink their security and data protection practices amidst hybrid work and cloud environments. In turn, threat actors have continued to exploit the vulnerabilities companies exposed themselves to, including those publicly identified, in keeping pace with rapid digital transformation efforts. Cybersecurity Ventures estimates that the annual increase costs related to cybercrime will reach 10.5 trillion by 2025, as cyber risk management has not kept up with digital transformation posing serious risks to organizations' security and revenue.[1]

As a result, companies find it increasingly difficult to manage their attack surface at the speed and scale necessary to prevent attacks. Here are the top attack surface exposures and trends from the past year, and ways institutions can remediate these threats before they transform into critical issues. »

Top Attack Surface Exposures

Palo Alto Networks' 2023 Unit 42 Attack Surface Threat Management report[2] found that the top attack surface exposures exist via two methods: actions directly taken on a compromised device (such as exfiltrating sensitive files stored locally on the device) or leveraging unauthorized access on a compromised attack surface asset (such as compromising VPNs) to gain further access within an organization. Both methods affect hybrid work environments and exist in various forms. However, the cloud is one increasingly popular attack surface cybercriminals have homed in on. Cloud is the dominant attack surface through which these critical exposures are accessed, due to its operational efficiency and pervasiveness across industries. The key types of exposures, in order of prevalence, include web framework takeover, remote access services, IT and networking infrastructure, file sharing, and database exposures and vulnerabilities.

Web framework takeover and remote access service exposures accounted for over 40% of exposure types.[3] Such services are heavily utilized in hybrid work environments and are fundamental to smooth business operations. Over 85% of organizations analyzed have RDPs accessible via the internet for at least 25% of a given month, leaving them open to ransomware attacks.[4] Given that threat actors exploit critical vulnerabilities within mere hours of publication, this poses a serious security risk for companies.

The attack landscape has evolved to target critical infrastructure. These targets are more appealing to threat actors because they haven't been regularly maintained in the past. Some of the most at-risk industries include several critical infrastructure sectors such as:

- Healthcare
- Utilities and energy
- Manufacturing
- Education
- State/national governments

The growing trend of targeting critical infrastructure is concerning, as we've seen attacks like SolarWinds have devastating impacts.

Interestingly enough, high-tech companies were also among the top organizations targeted by threat actors. These companies heavily rely on remote access services, which can be a significant attack vector due to insecure servers, inadequate security protocols, cloud misconfigurations, exposure of security infrastructure (such as routers and firewalls), and more. Organizations across all industries can benefit from secure practices to limit their remote access exposures.

Key Recommendations

Today's threat actors are adept at exploiting organizational vulnerabilities to gain access to remote environments. In addition to implementing the below suggestions, I suggest monitoring for emerging threats through comprehensive efforts that will set up a strong baseline for your company, such as a service retainer for threat landscape briefings or an audit of your organization's attack surface for risk.

Here are key recommendations and best practices organizations should consider strengthening their security posture and actively manage their attack surfaces.

1. **Change your vulnerability mindset** to identify legacy vulnerability management systems. This will assist your organization in resolving issues before they become mission-critical.
2. **Implement strong authentication methods** for key internet-facing systems, such as multi-factor authentication. This way, organizations can secure remote access services and monitor for signs of unauthorized access attempts.
3. **Ensuring continuous visibility** into on-premises and cloud assets is a must for security. By maintaining a real-time understanding of all company assets that are accessible online, you set your teams up for success in premeditating attacks.
4. **Attack premeditation** is another vital way to secure your systems. Focus on addressing the most critical vulnerabilities across severity and likelihood through the Common Vulnerability Scoring System[5] and Exploit Prediction Scoring System[6] scores, respectively.
5. **Address cloud misconfigurations head-on**. Regularly review and update your organization's cloud configurations to align »

with industry best practices; have your security and DevOps teams work together to drive secure deployments. While remote access services are crucial for hybrid work environments, their faulty configurations pose significant risks to company security.

6. **Respond to threats quickly**. It is of chief importance that your security team respond instantly. Install protocols and mechanisms to help your team quickly leverage attack surface management tools to prioritize patches and remediate common exposures.

Understanding the threats you face, and what you need to protect your organization against them, is critical for a successful cybersecurity program. As research shows, companies and government agencies struggle to understand which assets expose them to the most risk. By implementing these key recommendations, organizations can take a more proactive and holistic approach to maintaining control over their infrastructure and evolving with the changing nature of their attack surface.

To learn more, visit us here.

[1] Morgan, Steve. "Cybercrime To Cost The World $10.5 Trillion Annually By 2025." *Cybercrime Magazine*, Cybersecurity Ventures, 13 November 2020.

[2] Unit 42. "2023 Unit 42 Attack Surface Threat Report." *Palo Alto Networks*, 14 September 2023.

[3] Ibid.

[4] Ibid.

[5] "Common Vulnerability Scoring System Version 3.1 Calculator." FIRST.org.

[6] "Exploit Prediction Scoring System (EPSS)." FIRST.org.

Matt Kraning is the CTO of Cortex at Palo Alto Networks

Platforms in Action — Three Companies That Supercharged Risk Posture

By Lakshmi Kandadai

Today's organizations face cybersecurity challenges on multiple fronts. Many applications and workloads have moved to the cloud while employees now work in hybrid and remote environments – connecting to the network from anywhere and on any device. What's more, new threats continue to emerge as attacks grow more sophisticated every week, often with AI as a driving force.

Building a strong risk posture in today's threat landscape requires a shift away from traditional cybersecurity defenses. Security architecture, built on point products, is complex and lacks the integration needed to stop sophisticated zero-day attacks. Cybersecurity consolidation, combines best-of-breed tools into unified security platforms, leverages shared threat intelligence across the enterprise to identify attack patterns and enables rapid incident response.

We've connected with several customers in different industries across the world to see how Palo Alto Networks platforms enhanced their risk posture, elevated business value, and delivered a strong return on their investments. Here is a look at organizations in mortgage, life insurance and semiconductors.

1. Better

Better is a homeownership company founded in 2014 that supports multiple aspects of the homeownership journey – from mortgages to insurance and repairs. The company handles massive volumes of highly sensitive customer data, in addition to intellectual property critical to its business operations.

Challenges

Like many organizations, Better's security team faced a tidal wave of threat alerts that took days and weeks to triage manually. Ali Khan, CISO at Better, says:

"As we scaled up, we couldn't keep up with all the threats that were coming in. A lot of them were rinse-and-repeat alerts. It's not something we really needed a human for; you can automate this." »

They also needed to transition to a cloud-based VPN to allow thousands of employees to connect remotely and work from anywhere. Perhaps most importantly, they needed to secure highly valuable customer and company data.

Business Impact

Khan's team chose to consolidate their security footprint with a suite of Palo Alto Networks solutions. The team automated 90 percent of alert responses, cutting investigation time from hours to just minutes with Cortex XSOAR. This freed up the team to work on more complex, future-facing tasks. Prisma Access also enabled Better to secure access and quickly pivot to remote work for all employees without compromising the security of its people, data and applications.

Read more about the platforms and services Better chose to improve its security outcomes.[1]

2. Resolution Life

Resolution Life is a life insurance service provider in Australia that manages a large number of businesses and portfolios. When it acquired another life insurance company, AMP Life, the security had an opportunity to build a security infrastructure from the ground up.

Challenges

The financial services industry grapples with some of the strictest cybersecurity regulations compared to other industries. At the same time, a change in market trends meant that Resolution Life needed a partner to secure its journey while modernizing the business. Rob Jillson, Head of Cyber Security at Resolution Life Australasia, says:

"We needed to ensure that we safeguarded our clients' confidential personal and health information while adhering to a strict regulatory environment. Being compliant does not guarantee that information is secure and being secure does not guarantee compliance with regulatory obligations."

Jillson's team also wanted to streamline investigation and incident response so IT personnel could focus on larger value-added tasks. Results had to be quantifiable and backed by data for regulatory purposes.

Business Impact

Resolution Life chose to deploy a suite of Palo Alto Networks products for the completeness of our platform and the ability to integrate, customize and automate. Next-Generation Firewall, Prisma Cloud, Prisma Access and CDSS provided advanced threat protection and security stack reduction, while Cortex XSOAR gave security analysts full visibility across the network with automated threat detection and resolution.

The solutions also allowed Jillson's team to implement "audit built-in" where defendable metrics could be generated in the event of regulatory scrutiny. This helped Resolution Life continue to safeguard customers' personal and health information and keep up with the latest cyberthreats.

Read more about the platforms and services Resolution Life chose to improve its security outcomes.[2]

3. Imagination Technologies Group

Imagination Technologies Group designs and licenses intellectual property processor solutions in the semiconductor industry. The company had always prioritized agility and innovation over data security, but security challenges were rapidly mounting.

Challenges

The entire organization needed a fresh take on cybersecurity, from tools down to culture. It never had a dedicated SOC, and multiple, disjointed point products made it difficult to get full visibility into the security posture. As an engineering-led organization, cybersecurity was viewed as a roadblock to processor development. Paul Alexander, Director of IT Operations at Imagination Technologies Group, says:

"We used to comment that cybersecurity was important until it was inconvenient. Nothing was allowed to impact engineering, and the perception was that restrictive cybersecurity controls did exactly that."

Business Impact

Alexander's team chose several platforms in the Palo Alto Networks portfolio to modernize their security architecture. ML-powered NGFWs were deployed across 14 sites, securing more than 1,000 staff and over 12,000 devices (many unmanaged). Cortex XSIAM provided security visibility across the organization to prevent the most advanced attacks. It also delivered automated threat detection and response, dropping the number of incidents per day from 175 to less than 30 and freeing » the three-person security team from tedious manual resolutions.

In addition, Imagination took advantage of Unit 42's Managed Threat Hunting, gaining 24/7 protection across the entire security environment. These deployments allow the organization to continue developing semiconductor technologies without compromising security features.

Read more about the platforms and services Imagination Technologies Group chose to improve its security outcomes.[3]

Consolidation — Future-Proof Your Security

At best, multiple disparate security tools across your enterprise can cause lost productivity and an unmanageable web of features and vendors. At worst, those same tools can create gaps in your risk posture, allowing cybercriminals to exploit and breach your organization. But, with security consolidation, you get best-of-breed security tools that share threat intelligence, recognize attack patterns, and stop even the most sophisticated threats.

See more of what customers say about Palo Alto Networks platforms.

[1] Case study. "Better: Digital-first homeownership company adopts a consolidation strategy to modernize security." *Palo Alto Networks*, 18 January 2024.

[2] Case study. "Security exemplified for Resolution Life Australasia." *Palo Alto Networks*, 1 January 2023.

[3] Case study. "Imagination Technologies: "No-compromise cybersecurity posture for global semiconductor manufacturer." *Palo Alto Networks*, 12 December 2022.

Lakshmi Kandadai is the director of product marketing, Cross-Portfolio and 5G Security at Palo Alto Networks

Healthcare Cybersecurity — Three Trends to Watch in 2024

By Paul Kaspian

Our new guide, The Healthcare CISO's Guide to Cybersecurity Transformation, highlights the latest trends in healthcare today and where security leaders should focus their defensive efforts going forward.

Malicious attacks on healthcare have grown exponentially in recent years. According to the HHS Office for Civil Rights (OCR), large breaches increased by 93% between 2018 and 2022.[1] Additionally, large breaches involving ransomware increased by 278%. Healthcare in particular is a prime target. Customer information is valuable for identity theft and blackmail, while many health systems still operate with legacy technologies.

Healthcare is undergoing rapid modernization. New technologies in the field can dramatically improve outcomes while new care delivery models make the experience of receiving care much more pleasant for patients. This also introduces a new level of risk that must be addressed: an ever-expanding attack surface in healthcare.

Understanding the largest drivers of healthcare transformation today is key to securing digital transformation and providing the quality of care patients deserve. Here is a look at several trends highlighted in the guide.

1. The Rise of Remote Care

Telehealth and remote patient monitoring are revolutionizing the care delivery experience. Patients enjoy better access to care, especially those with disabilities or those who live in underserved communities. According to the CDC, 37% of Americans used telemedicine for at least some services in 2021.[2]

»

> “According to the HHS Office for Civil Rights (OCR), large breaches increased by 93% between 2018 and 2022."

While innovations, like remote care, optimize patient-centric care delivery, they also introduce new cybersecurity challenges. Remote care requires access to EMRs, PHI, virtual visits and RPM devices delivered from multiple channels: Data centers, cloud providers and SaaS providers. Security teams must also manage the IT infrastructure and connectivity between hospitals and patients. Ultimately, this shift toward decentralized care delivery models expands the attack surface and makes securing the entire network much more painstaking.

2. The Proliferation of Connected Devices

Connected medical and non-medical devices now make up a sizable portion of a hospital’s network. MRI machines, IV pumps, blood pressure monitors, laptops and security cameras, and even HVAC systems, just to name a few. Preventing data compromise and risks to patient safety requires securing these connected devices from end to end.

Complete visibility among the diversity of devices can be extremely challenging, especially among providers practicing distributed-care delivery models. Devices are often connected to complex medical IT environments while located in medical centers, remote clinics and patient homes. This widens the endpoint sprawl, making every device a potential target for cybercriminals. To further complicate this problem, many IoT and IoMT devices are both critical to provider operations and highly insecure.

3. The Increasing Complexity of Medical IT Environments

Applications and services are now hosted in data centers and the cloud, or they’re delivered by SaaS providers, while clinicians deliver care from anywhere using an array of connected medical devices. Many of these run on antiquated operating systems, and often cannot be patched or secured effectively. Security teams are tasked with managing these increasingly complex IT environments, which require significant technical resources.

Healthcare organizations often attempt to secure this digital landscape by tacking on point product solutions that provide a single security function each. These products typically lack integration and cohesiveness, only adding to the complex challenge.

Securing Digital Transformation in Healthcare

Today’s healthcare cybersecurity can’t run on multiple disjointed products. Continuous care delivery requires a unified approach designed to identify and prevent known and unknown threats in real time. How do you achieve this while protecting your environment in an ever-evolving threat landscape? Start by prioritizing three focus areas:

1. Securely deliver care from anywhere.
2. Secure connected devices.
3. Simplify security through consolidation.

Our newest guide delves into the many challenges of securing healthcare digital transformation, and how cybersecurity consolidation empowers security teams to protect data, support better patient outcomes, accelerate innovation, and ensure positive experiences for both patients and providers. Check out *The Healthcare CISO’s Guide to Cybersecurity Transformation*[3] to improve the security of your healthcare environment.

[1] “HHS Announces Next Steps in Ongoing Work to Enhance Cybersecurity for Health Care and Public Health Sectors.” *HHS.gov*, 6 December 2023.

[2] Lucas, Jacqueline W., and Maria A. Villarroel. “Products - Data Briefs - Number 445 - October 2022.” *Centers for Disease Control and Prevention*, 12 October 2022.

Paul Kaspian is a principal product marketing manager focusing on Zero Trust and AI at Palo Alto Networks

Addressing Vulnerabilities in OT Environments Requires a Zero Trust Approach

By Navneet Singh

Cyberattacks on operational technology (OT) systems are rapidly rising. In fact, manufacturing was one of the sectors most impacted by extortion attacks last year, according to Palo Alto Networks Unit 42, as reported in the 2023 Unit 42 Extortion and Ransomware Report.[1]

Attacks against OT systems can have a significant impact, including physical consequences such as shutdowns, outages, leakages, or worse. The Colonial Pipeline attack in 2021[2] is one of the most well-known examples of a major OT attack; the attack prompted a temporary shutdown of nearly half the gasoline and jet fuel supply delivered to the East Coast. That led to fuel shortages and price hikes.

Why is this sector at such risk? There are several factors which we'll explore in this piece. The good news is that a Zero Trust approach can go a long way toward helping organizations take back control and develop a more robust security posture.

How we got here

With the rise of digital transformation, we've seen the increased convergence of IT and OT systems. As a result, OT systems that were previously isolated are now connected and therefore accessible from the outside world, making them more at risk of being attacked.

Another factor that has increased the security risks in this sector is that critical infrastructure often relies heavily on legacy systems. This means many systems are running older, unsupported operating systems. They weren't designed with cybersecurity considerations in mind, and they can't be easily patched or upgraded because of operational, compliance, or warranty concerns.

Manufacturers also face a lack of skilled employees who can manage these converged environments. An August 2022 survey by the National Association of Manufacturers[3] found that three-quarters of respondents named attracting and retaining a quality workforce as one of their top business challenges. Finding people with cybersecurity expertise is an ongoing challenge – with ISC2 putting the global cybersecurity skills gap at 3.4 million people[4] – and finding people with both security and OT knowledge is even more difficult.

The rise of ransomware and increased regulations

Not only are manufacturers grappling with the above trends, but they're also under constant pressure to keep operations up and running. A ransomware attack on a factory can cripple a business's ability to produce products, leading to days if not weeks of downtime, resulting in financial loss.

Bad actors are increasingly seizing this opportunity. In fact, manufacturing has become the second most targeted sector in Unit 42's client base for ransomware attacks. »

On top of being a target for ransomware and other cyberattacks, governments have noticed the exposure manufacturers face and have imposed more regulations. Most notably, as of December 18, the Securities and Exchange Commission will now require larger publicly traded companies to report a cyber incident within four days, a regulation that puts even more pressure on companies to be ready to understand and act fast. This doesn't just apply to manufacturing companies, but rather, all publicly traded companies.

Starting with a foundation built on Zero Trust

Manufacturers have multiple environments to protect that run on different operating systems and applications. There are OT devices and networks (for example, the factory floor.) There are remote operations. And there are 5G connected devices and networks at the cutting edge of deployments. Neither IT nor OT managers have tools that offer visibility into all of the different environments, applications, systems, and devices.

Without visibility, it's pretty much impossible to know if there are vulnerabilities within any of these devices. This, coupled with the difficulties in operating excessively complex systems creates exponential risk from threat actors, often with the threats outpacing the ability of the technology teams to prevent attacks. The reason that ransomware works in manufacturing is because those Windows-based operation controls are largely identical to those found on the business side of the house.

A Zero Trust approach – especially at the higher architectural layers of a factory where OT and IT first converge – can help solve many of these issues. Zero Trust is predicated on a simple concept – trust no one. It's a strategic approach that eliminates implicit trust and continuously validates every stage of a digital interaction to secure an enterprise. By implementing a Zero Trust strategy, you apply security to users, devices, applications, and infrastructure in the same consistent manner, across the entire organization. A Zero Trust framework makes it easier to secure all of the different environments within a manufacturer.

Think of Zero Trust as a framework that includes the following principles/steps:

1. **Gaining visibility of all assets – and their inherent risks**: Broad visibility that includes behavioral and transaction flow understanding is an important step to evaluate risk and also to inform the creation of Zero Trust policies.
2. **Applying Zero Trust policies**. These include least-privilege access and continuous trust verification, an important security control that greatly limits the impact of a security incident. This must include continuous security inspection, which ensures transactions are safe by stopping threats without affecting user productivity.
3. **Making it simple to operate**. Don't throw multiple point solutions at every environment. This creates more complexity, costs more, and can ultimately leave security gaps. You need to ensure a seamless experience and integration with your IT team.

A Zero Trust approach plays a central role in helping OT organizations remain operationally resilient, reduce the potential attack surface, and minimize new or expanding risks brought on by digital transformation. The reality is that OT is likely to continue to be a major target for bad actors in the foreseeable future. And for most organizations, there will be a constant struggle to find and retain talent with the right skills. These are almost inevitable factors, as is the continued convergence of IT and OT. IT leaders working in OT have a unique set of challenges, and it can certainly feel like an uphill battle at times, but starting with Zero Trust provides the foundation for creating a stronger, better security posture now.

To learn more, visit us here.

[1] "2023 Unit 42 Ransomware and Extortion Report." *Palo Alto Networks*, 21 March 2023.

[2] Brumfield, Cynthia. "Colonial Pipeline shutdown highlights need for better OT cybersecurity practices." *CSO Online*, 10 May 2021.

[3] "2022 3rd Quarter Manufacturers' Outlook Survey - NAM." *National Association of Manufacturers*, 19 September 2022.

[4] (ISC)^2 Research Reveals the Cybersecurity Profession Needs to Grow by 3.4 Million People to Close Global Workforce Gap." *PR Newswire*, 20 October 2022.

***Navneet Singh** is the VP of network security marketing at Palo Alto Networks*

2023 Unit 42 Attack Surface Threat Report Highlights the Need for ASM

By Matt Kraning

Palo Alto Networks Unit 42 illuminates some of the riskiest security observations around attack surface management (ASM) with the 2023 Unit 42 Attack Surface Threat Report.[1] The report contrasts the dynamic nature of cloud environments with the speed at which threat actors are exploiting new vulnerabilities. It found that cybercriminals are exploiting new vulnerabilities within hours of public disclosure. Quite simply, organizations are finding it difficult to manage their attack surfaces at a speed and scale necessary to combat threat actor automation.

Most organizations have an attack surface management problem, and they don't even know it, because they lack full visibility of the various IT assets and owners. One of the biggest culprits of these unknown risks are remote access service exposures, which made up nearly one out of every five issues we found on the internet. Defenders need to be vigilant, because every configuration change, new cloud instance or newly disclosed vulnerability begins a new race against attackers.

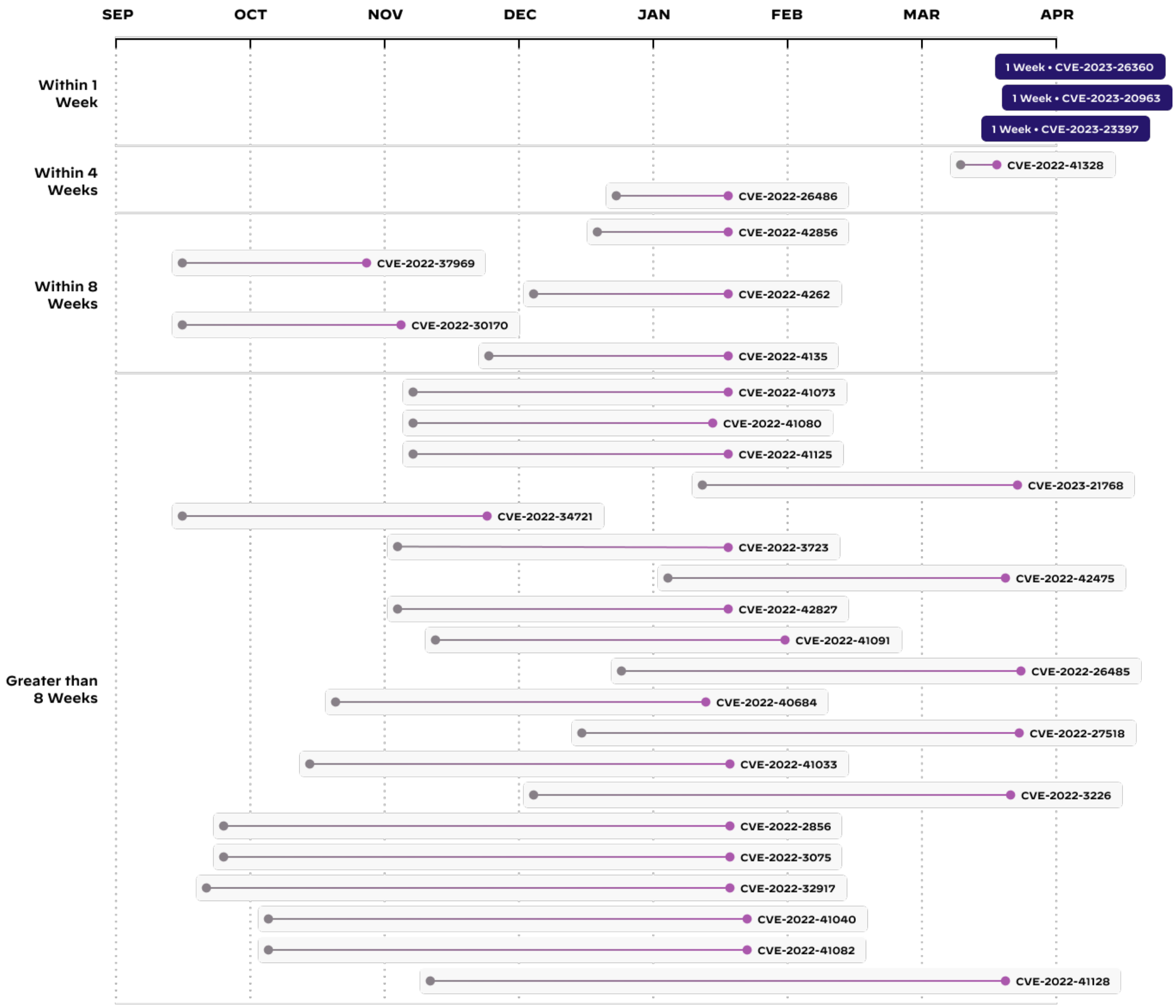
Notable Findings from the Report

Attackers Move at Machine Speed

- Today's attackers can scan the entire IPv4 address space for vulnerable targets in minutes.
- Of the 30 common vulnerabilities and exposures (CVEs) analyzed, three were exploited within hours of public disclosure and 63% were exploited within 12 weeks of the public disclosure.
- Of the 15 remote code execution (RCE) vulnerabilities analyzed by Unit 42, 20% were targeted by ransomware gangs within hours of disclosure, and 40% of the vulnerabilities were exploited within 8 weeks of publication.

Cloud Is the Dominant Attack Surface

- 80% of security exposures are present in cloud environments compared to on-premises at 19%.
- Cloud-based IT infrastructure is always in a state of flux, changing by more than 20% across every industry every month.
- Nearly 50% of high-risk, cloud-hosted exposures each month were a result of the constant change in cloud-hosted new services going online and/or old ones being replaced.
- Over 75% of publicly accessible software development infrastructure exposures were found in the cloud, making them attractive targets for attackers. »



Time elapsed before first reported ransomware attack against some of the top vulnerabilities by a known threat actor in the last 12 months

Remote Access Exposures Are Widespread

- Over 85% of organizations analyzed had Remote Desktop Protocol (RDP) internet-accessible for at least 25% of the month, leaving them open to ransomware attacks or unauthorized login attempts.
- Eight of the nine industries that Unit 42 studied had internet-accessible RDP vulnerable to brute-force attacks for at least 25% of the month.
- The median financial services and state or local government organizations had RDP exposures for the entire month.

The Demand for Attack Surface Management

Enabling SecOps teams to reduce mean time to respond (MTTR) in a meaningful way requires accurate visibility into all organizational assets and the ability to automatically detect the exposure of those assets. Attack surface management solutions, like Palo Alto Networks industry-leading Cortex Xpanse, give SecOps teams a complete and accurate understanding of their global internet-facing assets and potential misconfigurations to continuously discover, evaluate and mitigate the risks on an attack surface.

Cortex Xpanse is agentless, automatic and routinely discovers assets that IT staff are unaware of and are not monitoring. Each day, it conducts over 500 billion scans of internet facing assets. This helps organizations actively discover, learn about, and most importantly, respond to unknown risks in all connected systems and exposed services. Cortex Xpanse is one of the only products that not only gives businesses the ability to see their exposures, but to also automatically remediate them. Cortex Xpanse also recently introduced new capabilities to help organizations better prioritize and remediate attack surface risks by utilizing real-world intelligence and AI-assisted workflows.

It has become clear that the legacy technologies powering today's security operations center (SOC) are no longer working and that customers require a massive reduction in their mean time to respond and remediate. The Cortex portfolio of products, such as XSIAM, incorporates AI and automation to revolutionize security operations and help customers be more agile and secure.

[1] Unit 42. "2023 Unit 42 Attack Surface Threat Report." *Palo Alto Networks*, 14 September 2023.

Matt Kraning is the CTO of Cortex at Palo Alto Networks

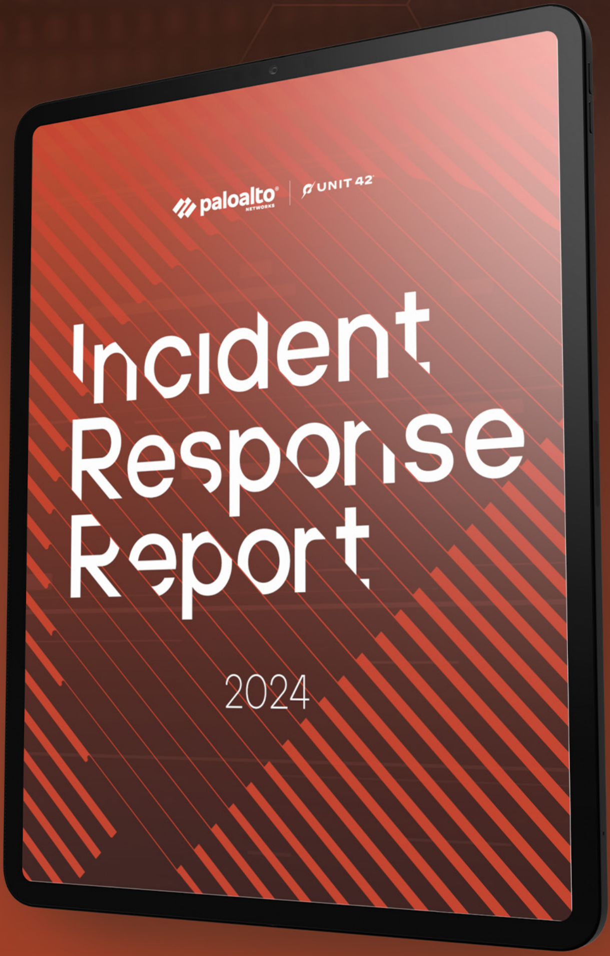
CORTEX
paloalto
UNIT 42
EXPOSURE
UNIT 42 ATTACK SURFACE THREAT REPORT
UNIT 42 ATTACK SURFACE THREAT REPORT

Click the QR code to download the full report.

paloalto NETWORKS
CORTEX

Are you ready to **defend against** the increasing speed, scale, and sophistication of **threat actors**?

Read the 2024 Unit 42 Incident Response Report to discover the latest attacker tactics and get expert recommendations to safeguard your organization better.



paloalto NETWORKS | UNIT 42

Incident Response Report

2024

Read the report

paloalto NETWORKS | UNIT 42