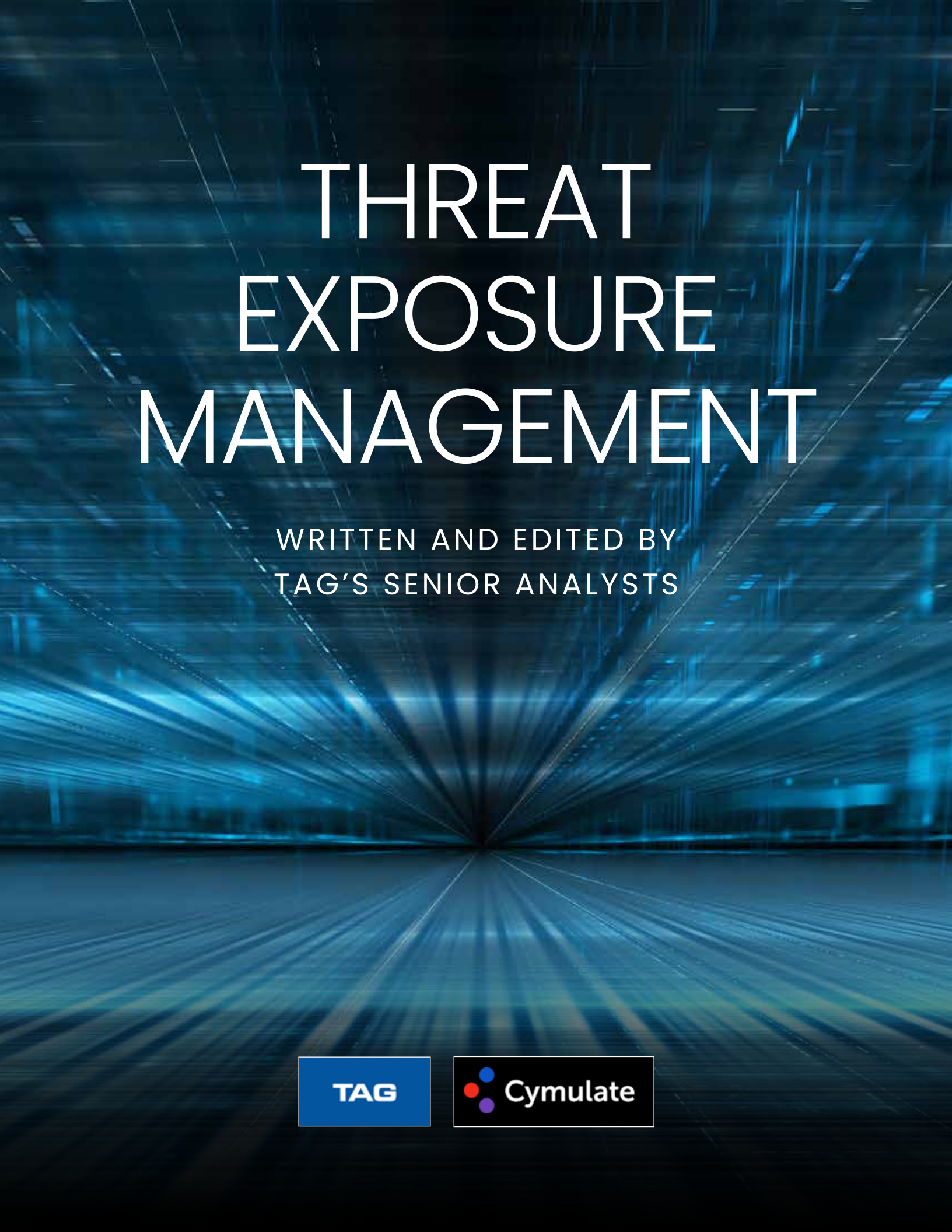
THREAT
EXPOSURE
MANAGEMENT
WRITTEN AND EDITED BY
TAG'S SENIOR ANALYSTS
TAG
Cymulate

THREAT EXPOSURE MANAGEMENT

THE SENIOR ANALYSTS OF TAG

–1–

INTRODUCTION TO THREAT EXPOSURE MANAGEMENT AND ITS OUTCOMES

DAVID NEUMAN, LEAD ANALYST, TAG

Organizations face increasingly sophisticated threats, outpacing traditional defensive measures. The key to staying ahead in this relentless cyber arms race lies in understanding and adopting a proactive and attacker-centric approach: Threat Exposure Management. Unlike traditional vulnerability management, which often reacts after threats have been realized, exposure management shifts the paradigm to focus on how exposed an organization is, how it appears from an attacker's perspective, and how effectively its controls and security operations processes perform against threats.

This approach aligns with the core business drivers of managing exposure risk. It's not just about identifying vulnerabilities; it's about understanding the real-world implications of those vulnerabilities on your organization's security posture and business continuity. Exposure management , therefore, becomes a strategic tool that enables businesses to anticipate, identify, and neutralize threats before they are exploited. It addresses critical questions such as: How exposed is our organization? What does our organization look like to a potential attacker? How robust and effective are our controls and security operations against these evolving threats?

Exposure management offers a more comprehensive and proactive approach to cybersecurity by answering these questions. This blog delves into the intricacies of exposure management, exploring its components like breach attack simulation and attack surface management and illustrating its operational and business impacts. We will also discuss why platforms like **Cymulate** are instrumental in implementing this advanced security strategy, helping organizations safeguard against potential threats and thrive in a landscape where cyber threats are an ever-present challenge.

ENABLERS OF EXPOSURE MANAGEMENT

Exposure management leverages technologies like Cyber Asset Attack Surface Management (CAASM), Attack Surface Management (ASM) and Breach and Attack Simulation (BAS) to identify and validate exposure risks. Consolidating these various cybersecurity tools and technologies, along with third-party data (vulnerability scans, cloud security posture management, continuous control monitoring, etc.), plays a crucial role in enhancing the effectiveness of CTEM. Here's how this consolidation contributes to risk prioritization and baseline measurement:

Integrating CAASM, ASM, BAS, and third-party data provides a comprehensive view of the organization's cybersecurity posture.

Integration and Holistic View: Integrating CAASM, ASM, BAS, and third-party data provides a comprehensive view of the organization's cybersecurity posture. CAASM offers visibility into all assets, ASM focuses on identifying vulnerabilities in these assets, and BAS simulates attacks to validate these vulnerabilities. When combined with third-party data, such as vulnerability scans and CSPM, this integration offers a detailed and nuanced understanding of the organization's security vulnerabilities.

Prioritization Based on Validated Risk: This consolidated approach allows organizations to validate and quantify the risks associated with different vulnerabilities and threats. By using BAS to simulate real-world attack scenarios, organizations can understand which vulnerabilities are more likely to be exploited by attackers. This information and insights from CAASM, ASM, and third-party data enable more informed decision-making about which vulnerabilities to prioritize for remediation.

Risk Assessment and Remediation: The data gathered through these tools can be analyzed to assess the level of risk each vulnerability poses to the organization. This assessment considers the severity of the vulnerability and the importance of the affected asset to business operations. The organization can then prioritize remediation efforts, focusing first on vulnerabilities that pose the greatest risk.

Continuous Monitoring and Improvement: Continuous monitoring of these tools allows for detecting new vulnerabilities and changes in the organization's attack surface. This ongoing process ensures that the organization can quickly respond to new threats and continuously improve its security posture.

ALIGNING CYBERSECURITY WITH BUSINESS GOALS

Exposure management not only elevates an organization's security posture but also empowers CISO to be more effective in their roles. This approach enables CISOs to:

Understand and Measure Exposure Risks: By adopting the perspective of an attacker, CISOs can gain a deeper understanding of their organization's exposure risks. This insight is crucial in measuring the security posture accurately and making informed decisions.

Prioritize Projects Based on Exposure Risk: Exposure management aids in identifying and prioritizing security projects and initiatives based on their potential to reduce exposure risk. This ensures that resources are allocated efficiently and effectively, addressing the most critical vulnerabilities first.

Unify SecOps Towards a Common Goal: Exposure management provides a framework for unifying security operations around the common goal of reducing cyber risk. By fostering collaboration and a shared understanding of security priorities, teams can work more cohesively towards mitigating threats.

Aligning the cybersecurity program with the overall business strategy is another critical aspect of CTEM. This alignment involves:

Using Common, Non-Technical Language: To define and communicate acceptable risk levels in terms that are understandable to non-technical stakeholders, fostering better decision-making and support across the organization.

Agreement on Handling Unacceptable Risks: Establishing a clear understanding and agreement on handling risks exceeding acceptable thresholds, including the potential for business operation disruptions during mitigation efforts.

Justifying Budgets and Projects: Exposure management enables CISOs to justify cybersecurity budgets and projects by demonstrating how they contribute to achieving business goals and reducing risks, thereby securing necessary resources and support.

Measuring Outcomes with Tangible Results: Exposure management provides a way to measure the outcomes of cybersecurity efforts with tangible results, such as reduced incidence of successful attacks and improved compliance with regulatory standards. These metrics are vital in demonstrating cybersecurity investments' value to stakeholders and continuously improving security practices.

CONCLUSION

Wrapping up, exposure management is vital to modern cybersecurity. For organizations looking to implement a comprehensive and proactive approach to securing their network, Cymulate's platform is worth considering. With its advanced capabilities in continuous monitoring, breach attack simulation, and attack surface management, Cymulate provides organizations with the tools to effectively identify and mitigate vulnerabilities, reduce the likelihood of a successful attack, and ultimately improve their security posture and bottom line.

–2–

THREAT EXPOSURE MANAGEMENT:

CONTINUOUS MONITORING AND ON-GOING ASSESSMENT

DR. EDWARD AMOROSO, CEO & FOUNDER, TAG

Threat exposure management is explained and illustrated in the context of its component processes, and how it supports continuous monitoring and assessment of cyber threats in the context of existing security platforms and tools.

INTRODUCTION

The enterprise security community is always seeking new ways to improve how it addresses cyber risk, especially in the context of real-time posture management. A major component of the best modern strategies involves so-called continuity. That is, whereas many prior methods involved reviewing security at a given time, usually resulting in a status report, practitioners are more interested in having a continuous view, one that maintains an on-going current view.

This is certainly not a new idea, as breach and attack simulation (BAS), automated penetration testing, attack surface management (ASM), and crowdsourced bug bounty testing are all modern versions of early scanning solutions. These methods are consistent with this idea of on-going checks, but they are point solutions, and enterprise teams tend to prefer integrated platforms that combine siloed methods into a unified approach.

To that end, a new model has emerged in the community known as threat exposure management. This paper outlines the salient aspects of implementing an exposure management program and shows how it supports the goal of continuous monitoring and on-going assessment of cyber threats. We hope the discussion is useful, since many modern commercial security platforms are now beginning to emerge that describe their functionality in terms of this model.

OVERVIEW OF THREAT EXPOSURE MANAGEMENT

Exposure management is a security practice focused on the reduction of threat exposure via a structured and iterative approach to prioritizing safeguards and improving security posture. Traditional approaches to

scanning, testing, and vulnerability management are often somewhat less effective due to the rapidly expanding attack surface. Exposure management goes beyond common vulnerability management by integrating known and unknown vulnerabilities, as well as control gaps.

Exposure management programs focus on the continuous cycles of security posture improvement by:

- Discovering your attack surface, its vulnerabilities, control weaknesses, and changes over time
- Validating controls, threats, and attack paths
- Prioritizing remediation for the validated exposure risks
- Remediating and mitigating risks with the best option that balances risk reduction and business disruption.

Many organizations can build exposure management programs by simply expanding existing functions, adding new capabilities, and integrating the results for a common purpose of seeking out threats and mitigating them before they endanger your environment.

Security teams are learning now how important it is to connect controls with actual business risk.

Discovery naturally includes vulnerabilities and configuration risks and should expand to build asset inventories with details of exposure risk and business context – i.e. the role that asset plays in business operations. The challenge is that the attack surface for most organizations continues to expand, so this is not a trivial step.

The inclusion of validation is one of the biggest advantages of exposure management over traditional vulnerability management. Validation provides the confirmation of exposure risk by assessing the likelihood of attack success and identifying the potential impact of successful attacks. Security programs that already include controls testing and red teaming should connect those practices to the results from discovery to accomplish the goal of exposure validation.

Prioritization is nothing new, but the need has never been greater as the number of vulnerabilities and potential threat grows exponentially. Prioritization in an exposure management program aims to focus your remediation on the threats that your organization is most likely to face. Security teams are learning now how important it is to connect controls with actual business risk.

The final step in exposure management is to mitigate the risk – and then retest to confirm and validate that the patch, configuration update, new control, or other remediation effectively addresses the risk.

Practitioners are advised to certainly make use of this exposure management model but will find that platforms will include (and often not include) aspects of the model. In addition, cost and implementation constraints will dictate that integration of exposure management platforms be done for legacy and existing tools and platforms. This is usually done via application programming interfaces (APIs) or data sharing connectors.

CONTINUOUS MONITORING AND ASSESSMENT

Exposure management is not just about implementing a set of new security tools, but rather represents a more continuous monitoring and assessment program that requires cross-team collaboration and organizational-level remediation of vulnerabilities and gaps. Exposure management helps organizations plan optimization of their security posture, while also providing a framework for continuous improvement.

Of course, exposure management does complement vulnerability management investment and can be integrated with other security initiatives. It requires a phased approach to deployment, starting with familiarization and gradually expanding to cover areas like attack surface management and security posture validation. By implementing exposure management programs, organizations can better manage their exposures and make informed decisions to enhance their overall security resilience.

NEXT STEPS

Enterprise teams are well-served to absorb the exposure management model into their source selection process for new continuous security platforms. As suggested above, the integration of such new tools into existing programs (e.g., an on-going bug bounty program, a deployed vulnerability management process) must be a requirement, since no enterprise team has the budget to rip and replace their protection infrastructure – even if it represents an improvement.

–3–

THREAT EXPOSURE MANAGEMENT:

A SHIFT IN STRATEGY

DAVID NEUMAN, LEAD ANALYST, TAG

In the ever-changing realm of cybersecurity, the initial thrill of successfully mitigating a breach attack was often short-lived. We would repair the breaches and celebrate, but these were temporary victories in an ongoing battle against evolving threats. Our approach resembled a patchwork, with each fix being a stopgap against the relentless emergence of new exploitable weaknesses. Attack Surface Management (ASM) broadened our perspective, allowing us to identify exposed vulnerabilities akin to hazards in a landscape. However, ASM was like a static map, unable to track the ever-shifting tactics of modern cyber-attacks. We were merely observers, bracing for the next unpredictable challenge.

The introduction of threat exposure management signifies a significant shift in strategy. Exposure management isn't just a temporary solution but a comprehensive program to prepare defense systems for the next attack and improve cyber resilience. Its focus was not on merely reacting to threats but on proactively understanding and predicting the evolving cyber landscape. Leading the way is Cymulate and their exposure management platform. This blog explores the transition from running BAS and ASM in silos to a threat exposure management program that integrates exposure discovery with exposure validation.

ESTABLISHING A STRONG FOUNDATION

The first step is a thorough examination of the digital infrastructure. It scrutinizes every element, from regular network devices to unauthorized cloud services. This process resembles creating a detailed blueprint of our entire digital environment, identifying potential weak spots for cyber threats.

ASM provides vigilant monitoring system in an exposure management program to identify new asset, changes to the existing attack surface, and understand their gaps. Exposure management combines traditional vulnerability scanning with the new ASM functionality to create a single inventory of assets, vulnerabilities, poor configurations and other exposures.

Various threat intelligence sources are also integrated, gathering insights from the cyber world, and monitoring unusual activities within our systems. This intelligence network becomes a guide, leading to detection and proactive response to potential cyberattacks.

Before jumping to remediation and mitigation, threat exposure management includes a validation step where offensive testing tools like BAS play a crucial role to:

- Validate controls and existing defenses that mitigate the threat
- Validate the threat against the IT stack to understand potential impact
- Validate attack paths to fully understand how the exposure could be exploited

With full visibility to the attack surface and validation of the exposures, threat exposure management programs can then focus remediation and mitigation on the biggest risks and with action that has the biggest reduction on risk.

CONSTRUCTING THE FORTRESS: THE THREAT EXPOSURE MANAGEMENT TRANSITION

Once there is a clear understanding of the current state, the focus shifts to developing a robust exposure management strategy.

Transitioning from BAS and ASM to exposure management is a complex, multi-faceted process that requires a blend of technical acumen and strategic foresight. Each demands meticulous attention and expertise. The journey begins with a comprehensive assessment of the BAS and ASM capabilities. This involves delving deep into the outcomes of previous simulations and surface management strategies, and dissecting them to identify their strengths and weaknesses. The goal is not just to pinpoint what's lacking but also to understand the dynamics of how these tools interact with our cybersecurity landscape. A critical part of this phase is conducting a gap analysis. This isn't just a superficial review; it requires a detailed examination of our security posture to uncover areas where BAS and ASM are not keeping pace with the evolving cyber threats.

Once there is a clear understanding of the current state, the focus shifts to developing a robust exposure management strategy. This strategy formation is a meticulous process of defining precise objectives aligned with broader cybersecurity goals. It's not just about selecting the right tools; it's about crafting policies and procedures that seamlessly integrate exposure management into our existing cybersecurity framework. This step is crucial as it sets the foundation for approaching continuous monitoring, threat intelligence, and vulnerability management in an exposure-centric environment.

The next phase revolves around infrastructure and resource planning. This is the nitty-gritty of determining the resources needed for implementing threat exposure management. It involves decisions about staffing, technology investments, and budget allocations. This phase demands a keen eye for detail as we select and acquire technology solutions that support exposure management functionalities and synergize with existing systems.

Integrating BAS and ASM systems into an exposure management process is the most technically challenging part of the transition. It requires a strategic approach to ensure that exposure management tools can effectively leverage data and insights from existing systems. This step involves meticulous planning and precise execution to create a cohesive and interoperative security environment.

Training and empowering our staff is critical to the success of threat exposure management. This phase goes beyond basic training; it involves in-depth sessions designed to equip teams with the skills to utilize exposure management tools effectively and interpret the insights they provide. This is where operations are transformed from passive technology users to proactive participants in our cybersecurity strategy.

Pilot testing the exposure management implementation is where theory meets practice. Start small, applying exposure management in a controlled environment, carefully observing its effectiveness, and making necessary adjustments. The transition to threat exposure management is not a one-time event but an iterative process. Performance is continuously monitored, learning and adapting as the implementation is gradually expanded.

The most ongoing aspect of this transition is the continuous monitoring and analysis. Utilizing exposure management tools, keep a vigilant eye on our organization's digital landscape. This isn't just about watching for threats; it's about actively analyzing the data collected and turning information into actionable insights. Finally, establishing a feedback loop and fostering a culture of continuous improvement is essential for keeping our threat exposure management strategy relevant and effective. As the digital landscape evolves, so must our approach to managing and mitigating cyber threats.

In essence, transitioning to threat exposure management is a journey that intertwines technical expertise with strategic planning. It requires a deep understanding of both the tools at our disposal and the ever-changing nature of cyber threats. By meticulously executing each step, we can effectively move from traditional BAS and ASM methodologies to a dynamic and proactive framework for threat exposure management, fortifying our cybersecurity defenses for the challenges ahead.

CONCLUSION: A CALL TO ACTION

We now face a choice: continue with temporary fixes or adopt threat exposure management for a more robust cybersecurity strategy. The time for makeshift solutions is over; the threat exposure management system is our path forward. We invite our fellow cybersecurity professionals to join us in this journey. With threat exposure management, we can navigate the unpredictable terrain of cyber threats and secure our digital future. This is just the beginning of the journey. We encourage the sharing of experiences and the cultivation of a community of security experts. Together, we can explore new frontiers in cybersecurity and ensure a safer digital environment for all. Until our next update, we wish you success and progress in your cybersecurity endeavors.

–4–

THREAT EXPOSURE MANAGEMENT:

IMPLEMENTATION OF BEST PRACTICES

DAVID NEUMAN, LEAD ANALYST, TAG

Threat exposure management is a cybersecurity framework that enables organizations to continuously monitor and assess their threat exposure and proactively mitigate risks. Exposure management is critical to any organization's cybersecurity posture, as it helps identify and address vulnerabilities before attackers can exploit them.

Organizations can follow many best practices to implement a successful exposure management program. These best practices provide the principals to build an exposure management program that delivers on the core requirements of:

- **Discovery**
- **Validation**
- **Prioritization**
- **Remediation & Mitigation**

In this blog I will examine the application of these best practices by Cymulate's exposure management and security validation platform.

DISCOVERY BEST PRACTICES

Discovering potential threats and vulnerabilities is paramount for cybersecurity teams utilizing threat exposure management platforms. These platforms offer an integrated approach, combining automated scanning tools, advanced analytics, and comprehensive databases to scan the digital ecosystem thoroughly.

Advanced Scanning
Its Advanced Scanning Capabilities are at the heart of a threat exposure management platform. Picture this as a relentless and meticulous digital sentinel tirelessly combing through the intricate layers of an organization's network, applications, and systems. Unlike the human eye, prone to oversight and fatigue, this automated guardian delves deep into the digital framework, unearthing vulnerabilities that might lurk unseen. These hidden weak spots, often missed in manual inspections, are brought to light, offering a comprehensive understanding of the organization's cyber health.

Harnessing the Pulse of Real-Time Threat Intelligence
As the narrative progresses, the platform seamlessly integrates real-time threat intelligence, a crucial component in the arsenal of modern cybersecurity. Imagine this as a continuous stream of vital information, a live feed pulsating with data on emerging threats and exploitations from around the globe. By tapping into this wealth of knowledge, the platform remains ever-vigilant, always a step ahead. This intelligence becomes the eyes and ears of the organization in the cyber world, enabling proactive defenses against potential attacks that evolve by the minute.

Automated Audits: The Unseen Watchers
The final yet equally pivotal element in this narrative is the implementation of automated audits. Envision these as systematic, unwavering scrutineers operating round the clock. These audits act as a consistent and thorough check on the organization's cyber practices and defenses. By regularly scrutinizing the system, they uncover potential security gaps that might otherwise go unnoticed. These automated overseer activities ensure that no stone is left unturned and no vulnerability is left hidden, providing an ongoing assurance of security and compliance.

Simulation and Modeling, Benchmarking and Analysis, and Community-Based Validation are pillars.

Integrating these key techniques within a threat exposure management platform narrates a story of relentless vigilance, proactive intelligence, and meticulous oversight, weaving together a formidable defense in the ever-shifting landscape of cyber threats.

VALIDATION BEST PRACTICES

The critical approaches of Simulation and Modeling, Benchmarking and Analysis, and Community-Based Validation are pillars, each contributing uniquely to fortifying an organization's cyber defenses.

The Art of Simulation and Modeling
Imagine a world where cyber-attacks can be foreseen and dissected before they ever occur. This is the realm of simulation and modeling. Here, the threat exposure management platform resembles a sophisticated virtual battleground. Organizations can simulate and enact various cyber-attack scenarios within this safe, controlled environment. This approach is not just about understanding the attacks; it's about delving into the adversary's mind. By witnessing the simulated attacks unfold, teams gain invaluable insights into real-world threats' behavior and potential damage. It's a proactive rehearsal, preparing the defenders by offering them a glimpse into the possible chaos, enabling them to strategize and fortify defenses against actual threats.

Benchmarking and Analysis: The Measure of Threats
Continuing the narrative, we encounter benchmarking and analysis, a methodological approach embedded in the platform. This is where discovered vulnerabilities are observed and measured against a vast library of known issues and industry benchmarks. Think of it as an enormous encyclopedia of cyber threats, with each discovery being cross-referenced and analyzed. This process is critical in deciphering the severity of each

vulnerability. It's not enough to know the enemy; one must understand where they stand in the grand scheme of things. This analysis helps prioritize responses, ensuring that the most dangerous threats are addressed with the urgency they demand.

PRIORITIZATION BEST PRACTICES

The role of a threat exposure management platform is akin to that of a master strategist in high-stakes chess. These platforms bring an intelligence-driven approach to prioritizing threats, ensuring that the most critical vulnerabilities are addressed with the urgency and resources they demand. This strategic play is executed through a trilogy of effective strategies: Risk Assessment Algorithms, Regulatory Compliance Tracking, and Stakeholder Reporting Tools.

Risk Assessment Algorithms: Digital Threat Prioritization
Envision risk assessment algorithms as the digital oracles of the platform, gifted with the foresight to discern the potential impact and likelihood of exploitation of each identified vulnerability. These sophisticated algorithms delve into the intricate details of each threat, analyzing and evaluating them against a myriad of factors. The result is a prioritized list of threats, ranked not just on their current status but on their potential to wreak havoc. This systematic approach ensures that resources are smartly allocated, focusing first on the vulnerabilities that pose the most significant risk to the organization's digital kingdom.

Regulatory Compliance Tracking: Navigating the Maze of Legal Obligations
Compliance with regulatory and legal frameworks is not just a matter of good practice; it's a necessity. This is where regulatory compliance tracking comes into play. Keeping a watchful eye on the ever-evolving landscape of legal obligations and standards is critical. By aligning the threat prioritization with these regulatory requirements, organizations ensure that their defense strategies are effective and compliant. This alignment is crucial in navigating the legal maze, avoiding potential fines and legal complications, and maintaining a reputation of reliability and trust.

Stakeholder Reporting Tools: The Harbingers of Clarity and Alignment
Finally, the narrative brings us to stakeholder reporting Tools, the communicators in the platform. These tools are pivotal in ensuring the prioritized threats are known to the cybersecurity team and communicated to all key stakeholders. Imagine these tools as the heralds that bring clarity and alignment across the organization. With comprehensive and understandable reports, stakeholders from various departments –IT, finance, or executive leadership – are kept in the loop. This clarity ensures that everyone understands the gravity of the threats and the rationale behind the prioritized responses, fostering a unified approach to cybersecurity.

Risk assessment algorithms, regulatory compliance tracking, and stakeholder reporting tools – form the core of intelligent threat prioritization in the exposure management platform. They represent a harmonious blend of foresight, compliance, and communication, ensuring the organization's

response to cyber threats is reactive and strategically proactive. In the grand chessboard of cybersecurity, these strategies provide that the right pieces are moved with precision and purpose, safeguarding the digital realm against its myriad threats.

REMEDIATION & MITIGATION BEST PRACTICES

Remediation and mitigation are where strategic planning and prioritization culminate in decisive action, akin to a well-oiled machine springing into motion at the moment of need. In this context, the threat exposure management platform emerges as a dynamic protagonist adept in remediation and mitigation.

Strategic planning and prioritization culminate in decisive action, akin to a well-oiled machine springing into motion at the moment of need.

Integrated Patch Management: The Swift Healer
Picture integrated patch management as the platform's swift healing mechanism, poised to mend the vulnerabilities that have been exposed swiftly. This system is like a vigilant medic, constantly looking for injuries (vulnerabilities) in the digital infrastructure. Upon detection, it deftly deploys patches – the healing salves – to these wounds, often before they can fester into more significant problems. This immediate deployment of fixes to known vulnerabilities is crucial, as it significantly reduces the window of opportunity for attackers to exploit these weak spots.

Automated Response Protocols: The Digital First Responders
Then there are the automated response protocols, akin to a team of digital-first responders. Time is of the essence in moments of threat, and these automated protocols act with precision and speed. Set up to handle known threats, they jump into action when a familiar adversary is detected, efficiently neutralizing routine issues and freeing up human resources to tackle more complex challenges. This automation is akin to having a well-trained reflex that reacts instantaneously to specific stimuli, providing a consistent and reliable defense against recurring threats.

Feedback and Learning Loop: The Evolving Shield
The narrative is complete with the feedback and learning loop, a mechanism embodying continuous improvement. Imagine this as an ever-evolving shield, learning from every blow it withstands. The platform's analytics are a repository of wisdom from each past incident. This knowledge is then used to adapt strategies and fortify defenses, ensuring that each response is more robust than the last. It's a perpetual learning and adaptation process, keeping the organization's cybersecurity posture current and ahead of the curve.

Organizations craft a resilience and dynamic defense narrative by incorporating these tactical measures within the platform. This approach enables them to react to cyber threats and anticipate and understand them, enhancing their capability to counteract them effectively.

CONCLUSION

Threat exposure management is a holistic approach to cybersecurity that considers all aspects of the organization's environment, including its people, processes, and technology. It is a continuous process of monitoring and assessing the organization's threat exposure and taking proactive steps to mitigate risks.

Exposure management is critical for organizations of all sizes and industries. Cyber threats are constantly evolving, and no organization is immune to attack. By implementing a successful exposure management program, organizations can reduce their risk of becoming cyber-attack victims and protect their critical assets from harm.

Here are some of the key benefits of implementing exposure management:

- **Reduced cyber-attack risk:** Exposure management helps organizations identify and address vulnerabilities before attackers can exploit them. This reduces the risk of successful cyber attacks and the associated damage to the organization.
- **Improved security posture:** Exposure management helps organizations improve security by continuously monitoring their environment for threats and proactively mitigating risks. This makes it more difficult for attackers to succeed.
- **Increased compliance:** Many industry regulations require organizations to implement specific cybersecurity measures. Exposure management can help organizations meet these requirements and improve their compliance posture.
- **Reduced costs:** A cyber-attack can be significant in terms of financial losses and damage to reputation. Exposure management can help organizations reduce the risk of cyber-attacks and the associated costs.

Overall, threat exposure management is a valuable investment for any organization serious about protecting its organization. By following the best practices outlined above, organizations can implement a successful exposure management program that will help protect their critical assets from cyber threats.

–5–

THREAT EXPOSURE MANAGEMENT:

THE FUTURE OF CYBERSECURITY

ANDY MCCOOL SENIOR ANALYST, TAG

The cybersecurity landscape is continuously evolving, marked by an ever-expanding array of threats and challenges. Organizations, both large and small, find themselves grappling with the dynamic nature of cyber threats. From ransomware to supply chain compromises, threat actors are rapidly innovating new ways to exploit vulnerabilities for financial and strategic gain.

In this fluid threat environment, organizations cannot rely on static defenses. Organization's need to adopt a proactive and adaptive approach to cybersecurity. This is where threat exposure management comes in. Exposure management provides the capability to continuously monitor assets, identify vulnerabilities, quantify risks, and prioritize remediation.

EMERGING THREATS AND CTEM

The cyber threat landscape is experiencing an exponential increase in complexity and sophistication of attacks. While foundational threats like phishing remain prevalent, new threat types continue to emerge. Some key threats on the horizon include:

- **AI/Deepfakes:** Realistic AI-doctored audio/video content is weaponized to enable highly targeted social engineering attacks against organizations.
- **Ransomware 3.0:** More advanced ransomware with capabilities for data encryption, data exfiltration and data alteration.
- **IoT and OT Attacks:** Lack of security in many IoT and OT devices provides an easy initial foothold into corporate networks for threat actors.
- **Third-Party Risks:** Vendors, suppliers and partners connected into an organization's IT environment multiply the attack surface. Compromise of third parties enables island hopping to the ultimate targets.
- **Nation-State Threats:** Geopolitical tensions continue to drive growth in nation-state sponsored cyber warfare capabilities and attacks.

Exposure management offers a lifeline for organizations to get ahead of these trends. By providing continuous visibility into the asset inventory and vulnerabilities, exposure management enables proactive identification of risk exposures and attack vectors. Organizations can find and fix security gaps before they are leveraged by threat actors. Prioritizing vulnerabilities for remediation based on exploitability, potential business impact and other contextual factors also becomes more efficient. With comprehensive, up-to-date insights into the risk surface, organizations can make strategic decisions on security investments. Cybersecurity becomes a data-driven discipline integrated with business objectives. Exposure management also facilitates reporting cyber risk in business terms to senior management and demonstrating risk reduction over time.

Exposure management also facilitates reporting cyber risk in business terms to senior management and demonstrating risk reduction over time

NEW EXPOSURE MANAGEMENT CAPABILITIES

Exposure management platforms are rapidly advancing with new features and capabilities focused on driving greater automation, using AI/ML and deeper integration with the other cybersecurity capabilities including:

- **Cyber Validation:** Offensive testing tools like breach and attack simulation and automated red teaming provide the automation needed for continuous security validation.
- **AI and Machine Learning:** AI and machine learning to analyze large volumes of data and identify patterns indicative of potential threats. These technologies can help automate threat detection and response.
- **Cloud/SaaS Security Posture Management:** Tools to provide visibility into misconfigurations, policy violations and risk exposures in complex SaaS and cloud environments.
- **IoT and OT Asset Management:** Discovery, inventory and monitoring specifically customized for Internet of Things and Operational Technology environments and use cases.
- **Third-Party Risk Ratings:** Leveraging external data sources to analyze supply chain entities and provide cyber risk ratings to enable better vendor selection and monitoring.
- **Cyber Risk Quantification:** Flexible models to quantify cyber risks by potential financial impact based on asset value, threat landscape and vulnerability to provide mitigation priorities.
- **Attack Surface Reduction:** Using exposure management intelligence to shrink attack surfaces by closing unneeded ports/protocols, decommissioning redundant systems and tightening permissions.
- **Security Orchestration and Automation:** Tight integration with SIEM/SOAR platforms to enable CTEM triggered workflows and automated mitigation/response.

PREPARING FOR THE FUTURE WITH EXPOSURE MANAGEMENT

Organizations should take a strategic approach to integrating exposure management programs into their security operations. Obtaining executive buy-in and educating leadership about emerging threats and how exposure management provides financial risk visibility that boards care about can guide strategy and investment priorities.

It is also essential to cultivate in-house expertise in leveraging exposure management tools and capabilities. Organizations should hire or train personnel with practical knowledge of implementing exposure management frameworks. This ensures your team can fully leverage exposure management technologies and integrate them into existing workflows for maximum impact.

Furthermore, adaptability and flexibility are paramount in the face of a constantly changing threat landscape. Organizations need to regularly reassess and update their exposure management strategies to address emerging threats and technologies. This involves staying informed about the latest cybersecurity trends, regularly updating security policies, and incorporating new tools and technologies that enhance the efficacy of continuous exposure threat management.

CONCLUSION:

Exposure management is a cornerstone in the defense against ever-evolving cybersecurity threats. By adopting a proactive and continuous approach to identify and mitigate threats before they endanger your business, organizations can significantly enhance their security posture. The integration of emerging technologies, the expansion into cloud security, and the emphasis on collaboration and education position exposure management as a critical component in preparing organizations for the dynamic future of cybersecurity. As threats continue to evolve, embracing and adapting exposure management strategies will be key to safeguarding the enterprise and maintaining the trust of stakeholders.

For organizations looking to implement a comprehensive and proactive approach to securing their IT environment, Cymulate's platform with its advanced capabilities in continuous monitoring, breach attack simulation, and attack surface management is well worth considering.

ABOUT TAG

TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity, artificial intelligence, and climate science/sustainability.


THREAT
EXPOSURE
MANAGEMENT
TAG
Cymulate