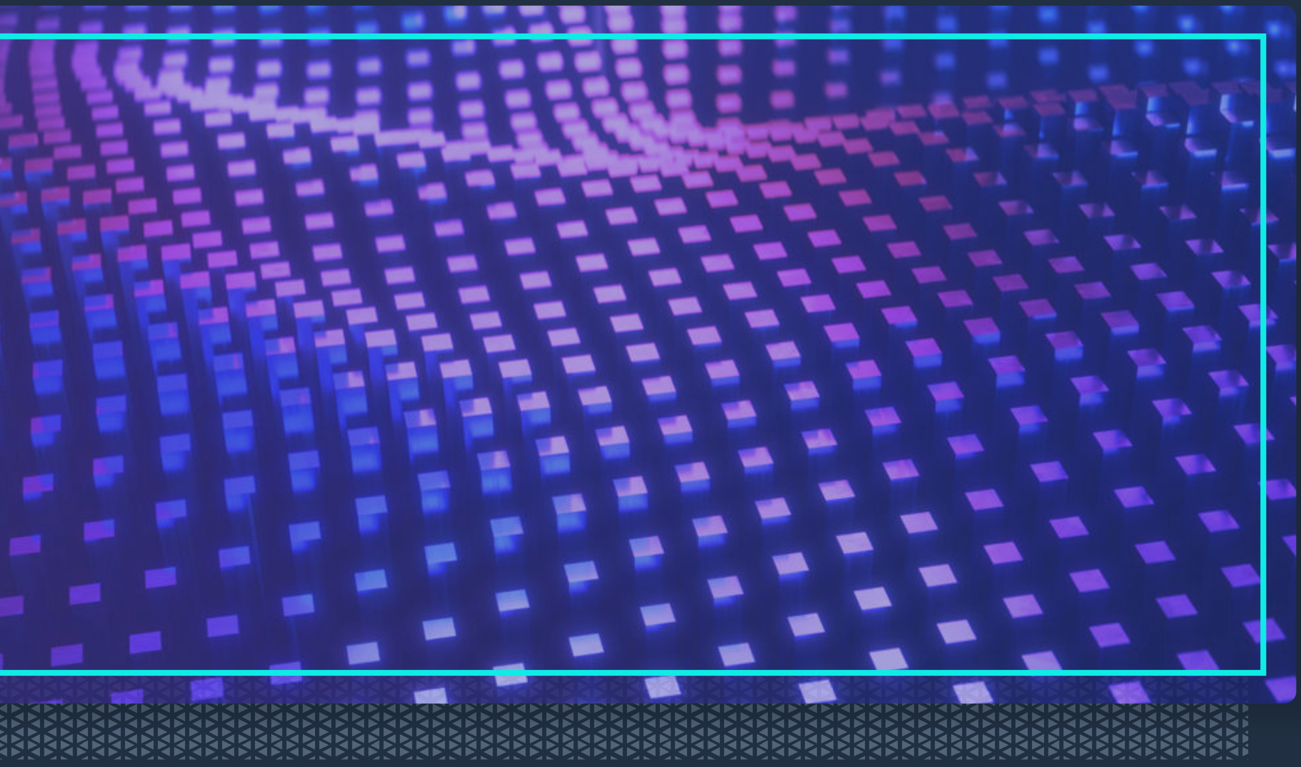
HORIZON3.ai

~~TRUST BUT~~ VERIFY

WHITE PAPER

CTEM and ASM

Shifting the Focus to **Exploitability in CTEM and ASM**



@Horizon3ai info@horizon3.ai www.horizon3.ai

The Exploitable Attack Surface Keeps Expanding

With the rise of hybrid cloud infrastructures, increased public exposure due to Open-Source Intelligence (OSINT), and shortcomings in security approaches, the exploitable attack surface is expanding significantly. Hybrid cloud environments extend the boundaries of the traditional perimeter, creating more entry points for potential threats. OSINT, the public information readily available, can be leveraged by attackers to identify ways to compromise organizations. Lastly, ineffective security approaches can leave organizations unprepared to effectively manage and respond to new security threats.

The Emergence of Continuous Threat Exposure Management (CTEM)

As the attack surface expands, a new approach to security has become essential: Continuous Threat Exposure Management (CTEM). However, CTEM is not an actual tool. It is a term coined by Gartner® that defines an integrated, iterative program containing five process stages:

- Scoping
- Discovery
- Prioritization
- Validation
- Mobilization

Rather than operating in episodic bursts of reactive efforts, often because of a suspected breach, a newly publicized n-day vulnerability, or some sort of audit-based exercise, CTEM promotes a proactive, continuous approach to identifying, assessing, and minimizing vulnerabilities within an organization's attack surface.

CTEM programs play a critical role in shaping the future of cybersecurity because they enable the transition from isolated security operations to an integrated, continuous defense system. Organizations building a CTEM program use various tools to achieve the following:

- Inventory and categorize assets and vulnerabilities
- Simulate and test various attack scenarios
- Continuously assess security postures
- Deliver effective and actionable findings

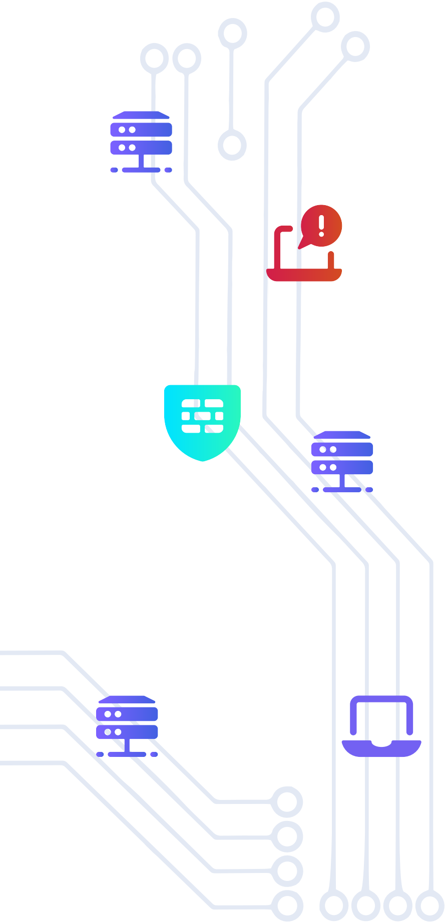
CTEM redefines security from a static, point-in-time assessment to a continuous assessment approach so organizations can keep pace with the rapidly evolving threat landscape.

A cornerstone of CTEM focuses on the exploitable attack surface—those parts of an organization's systems that are both vulnerable and susceptible to a successful attack.

> **By concentrating on reducing this exploitable attack surface, organizations can effectively prioritize their security efforts, ensuring resources are allocated to the areas of greatest risk.**

In the future state of cybersecurity, we believe CTEM will become the guiding strategy that unifies various security practices. It brings together continuous asset monitoring, autonomous pentesting, security orchestration, automation, response (SOAR), and detection engineering into a unified platform-based approach. This integrated approach allows organizations to continuously assess their exploitable weaknesses, rapidly respond to identified vulnerabilities, and use the data gathered to improve threat detection and response capabilities.

This vision of CTEM represents the next evolution in cybersecurity. Understanding the principles of CTEM, Horizon3.ai's NodeZero meets the objective of accurately discovering the exploitable attack surface.



The Importance of an "Assume Breach" Perspective

An assume breach perspective presumes that a breach will happen, or may have already happened, rather than operating under the illusion of impenetrable security. It fundamentally shifts the focus from solely trying to prevent intrusions, to also preparing for rapid detection, containment, and remediation when the inevitable breach occurs.

By incorporating an assume breach mentality into the fabric of their cybersecurity strategy, organizations can cultivate an ethos of vigilance and resilience. It steers the focus towards understanding the exploitable attack surface and continuously striving to minimize it, which aligns perfectly with the principles of CTEM.

In the emerging integrated future of cybersecurity, the assume breach approach becomes even more crucial. It not only helps drive the proactive continuous testing and mitigation activities central to CTEM, but also fosters a mindset of constant evolution and adaptation – essential in staying ahead of advancing cyber threats.

Understanding the Difference: Being Vulnerable vs. Being Exploitable

While vulnerabilities are weaknesses that can potentially be exploited, not all vulnerabilities necessarily pose a serious threat to an organization. This distinction brings us to the difference between being vulnerable vs. being exploitable.

A system is vulnerable if it has a weakness that "could" be exploited. However, that same weakness becomes truly exploitable if an attacker can leverage that vulnerability to compromise the system, given the system's context and the attacker's capabilities. For instance, a server may have a vulnerability, but if it is not accessible from the internet and is well-secured internally, the vulnerability is less likely to be exploitable.

Focusing on exploitable vulnerabilities – those that are realistically likely to be used in an attack – provides a more accurate reflection of an organization's risk exposure. It's not just about having a vulnerability; it's about whether that vulnerability can be compromised.

The Shift from Vulnerability Management to Reducing the Exploitable Attack Surface

Traditional vulnerability management, which involves identifying and patching all vulnerabilities, regardless of knowing if they are exploitable or not, has become a never-ending, resource-draining task due to the sheer volume of known vulnerabilities (aka CVEs). In 2022 alone, there were 25,080 vulnerabilities disclosed, which is an 18.78% increase over 2021. Also, vulnerability management does not necessarily translate into effective risk reduction if it fails to prioritize exploitable vulnerabilities.

That's why organizations should shift their focus towards identifying and reducing their exploitable attack surface. This approach, part of the broader CTEM strategy, involves identifying the vulnerabilities that are most likely to be exploited based on the organization's specific context, then taking steps to mitigate those first.

Rethinking Attack Surface Management with an Emphasis on Exploitability

Attack Surface Management (ASM) has become a critical component of today's cybersecurity strategy. ASM involves the continuous discovery, inventory, classification, prioritization, and security monitoring of digital assets that contain, process, or access an organization's data. These assets could be in the cloud, on-premises, or in third-party networks, and include everything from domains, IP addresses, and websites, to computers, applications, APIs, and IoT devices. However, is managing your attack surface enough to stop today's attack?

Simply "managing" the entire attack surface is no longer sufficient to stop today's attackers. There is a growing recognition of the need to focus more specifically on the exploitable attack surface – the subset of the attack surface that can be feasibly exploited by an attacker. This shift in focus is vital for efficient and effective risk management.

The current state of ASM often involves multiple, siloed tools, loosely stitched together into a "platform" whereby each tool focuses on distinct aspects of the attack surface. These disparate tools can create inefficiencies and blind spots, leading to a fragmented view of the attack surface and making it difficult to identify and manage what is truly exploitable.

A More Comprehensive Approach to ASM

The market should expect – and indeed, demand – a convergence of these siloed ASM tools into an integrated, purpose-built platform that focuses on identifying and reducing the exploitable attack surface. This is due to several key reasons:

1

Comprehensive Visibility:
An integrated platform can provide complete visibility of the entire attack surface, breaking down the silos and ensuring no exploitable asset is overlooked.

2

Efficiency:
By bringing together the capabilities of multiple tools into a single platform, organizations can streamline their processes, reduce the complexity of managing multiple tools, and improve their ability to manage the exploitable attack surface.

3

Consistency:
An integrated platform can offer consistent and unified risk scoring and reporting across the entire attack surface, helping organizations better understand and manage their exploitable risks.

4

Scalability:
As organizations grow and their attack surface expands, managing multiple tools can become increasingly challenging. An integrated platform can scale more effectively, maintaining performance and functionality as the number of assets increases.

5

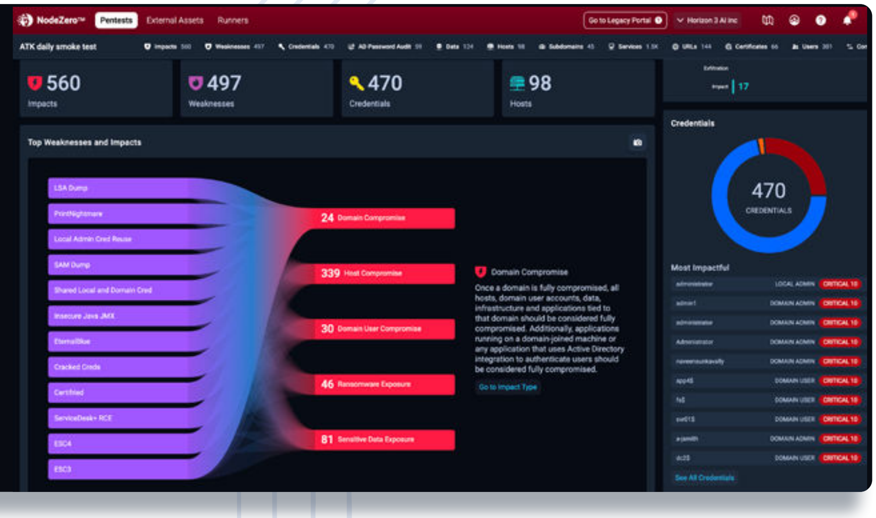
Cost-effectiveness:
By consolidating multiple tools into one, organizations can potentially reduce their total cost of ownership and improve their return on investment.

In the future, we foresee ASM evolving into a tightly integrated platform that combines continuous monitoring, autonomous pentesting, and SOAR capabilities, among others, thus making the platform a completely unified solution. NodeZero is well-positioned to be at the forefront of this evolution. By integrating ASM with CTEM fundamentals, and with a specific focus on the exploitable attack surface, NodeZero offers an innovative solution that can revolutionize an organization's approach to cybersecurity.

Autonomous Pentesting Focuses on Exploitability

Autonomous pentesting enables the shift to continuous security assessments and supports the assume breach narrative by identifying vulnerabilities in a real-world context. NodeZero actively breaches the environment – just as an actual attacker would – allowing your organization to understand its vulnerabilities under realistic conditions.

Consulting pentesters, while providing valuable expertise, are typically time-bound and may not be able to deliver the level of continuous, comprehensive coverage required in today's evolving threat landscape. In addition, vulnerability scanners, while useful for detecting known vulnerabilities, lack the context and capability to fully assess complex, exploitable vulnerabilities.



Domain Compromise

Once a domain is fully compromised, all hosts, domain user accounts, data, infrastructure and applications tied to that domain should be considered fully compromised. Additionally, applications running on a domain-joined machine or any application that uses Active Directory integration to authenticate users should be considered fully compromised.

NodeZero, a leading autonomous pentesting solution, overcomes both of these limitations. It is designed to test an organization's IT infrastructure continuously and comprehensively, providing detailed, actionable reports on detected vulnerabilities. During an autonomous pentest, NodeZero discovers exploitable attack paths that organizations must quickly remediate. NodeZero allows organizations to find, fix, and verify that exploitable vulnerabilities have been reduced and in doing so, lessens the exploitable attack surface.

Example Attack Path

Attack paths provide a graphical representation of the possible paths an attacker can take to exploit weaknesses in your computers, servers, applications, infrastructure, and security controls. Figure 1 shows an example attack path safely discovered by NodeZero during an autonomous pentest in a real organization that eventually led to domain compromise.

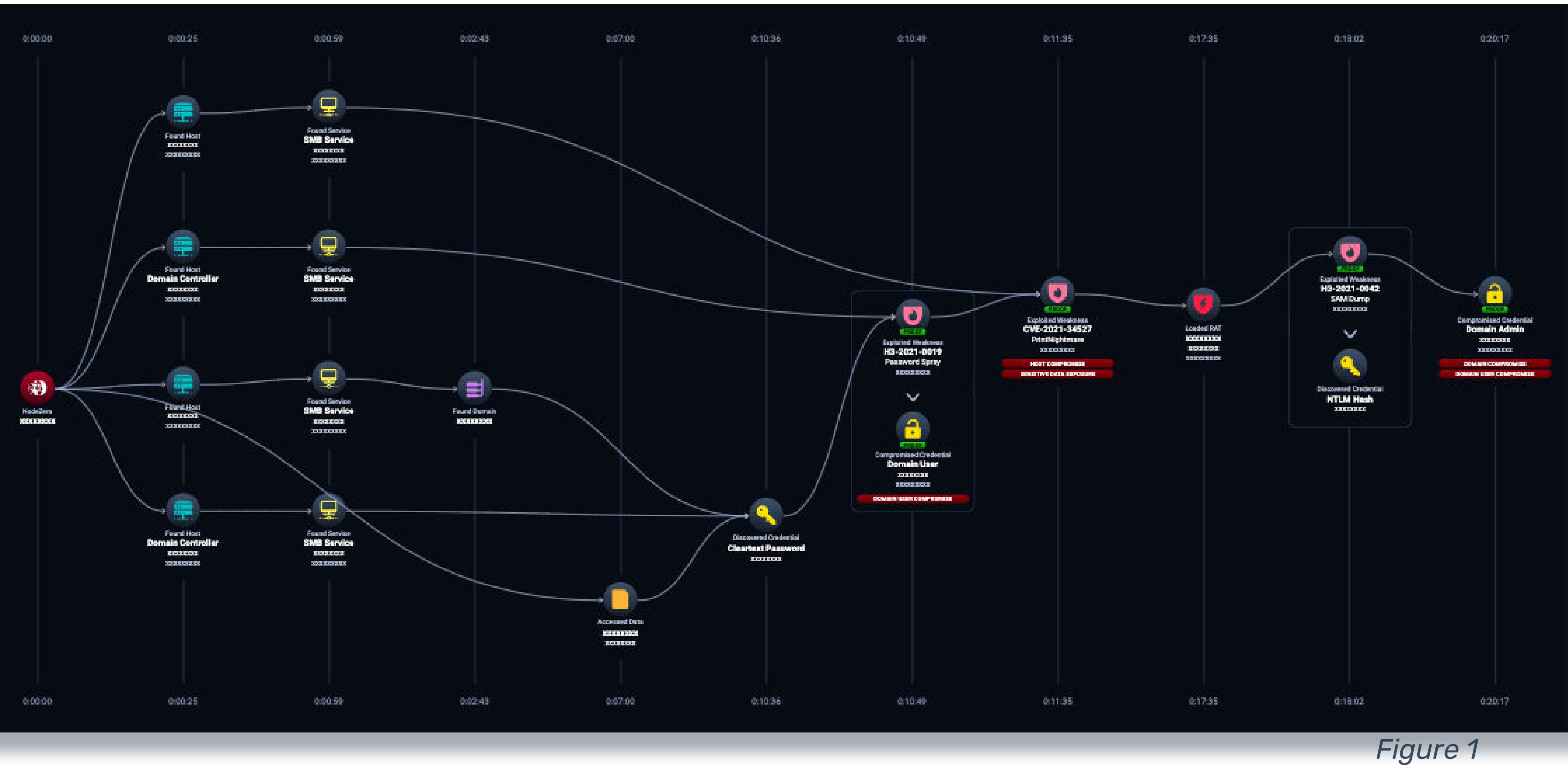


Figure 1

During this attack path, NodeZero began by discovering 45 verified usernames. It then went on to discover a cleartext password and used a password spraying technique to compromise the credential of a certain domain user. Once it verified the domain user, NodeZero then went on to exploit a known CVE-2021-34527: Windows Print Spooler Remote Code Execution vulnerability (aka PrintNightmare).

From there, NodeZero loaded a Remote Access Tool (RAT) using the same compromised credential, performed a SAM dump to discover an NTLM Hash for admin administrator, and finally became a domain admin in just over 20 hours. No humans were involved in the discovery of this exploitable attack path. From something as simple as a cleartext password, to gaining domain admin, this attack path certainly expands the exploitable attack surface..

NodeZero: A Critical Tool for CTEM Programs

NodeZero is becoming a key tool for organizations adopting CTEM. By breaching the environment in a safe and controlled manner, NodeZero helps organizations identify their exploitable vulnerabilities, understand their real-world risk, and take targeted action to reduce their exploitable attack surface.

1. **Continuous Vulnerability Detection:** Deploy NodeZero across your infrastructure to continuously monitor and identify vulnerabilities. Upon detection, NodeZero provides immediate notification and detailed reports, prompting your security team to begin remediation immediately. This workflow helps reduce your attack surface and the time-to-remediate.

2. **Efficient Remediation Verification:** After your team applies a fix to address a detected vulnerability, use NodeZero to retest the area and verify the effectiveness of the remediation. This quick verification process can reduce the likelihood of leaving unresolved or insufficiently addressed vulnerabilities.

3. **Prioritization of Vulnerabilities:** Use NodeZero to rank identified vulnerabilities based on severity, exploitability, and potential impact on your business. This can guide your team in prioritizing remediation efforts, ensuring that the most critical vulnerabilities are addressed first.

4. **Compliance Assurance:** Use NodeZero's continuous testing and detailed reporting to demonstrate compliance with various cybersecurity regulations including SOC2, HIPAA, DORA, CMMC, and GDPR. The reports can serve as evidence of your organization's proactive approach to identifying and addressing vulnerabilities.

5. **Proactive Threat Hunting:** Use the data from NodeZero's continuous pentesting to feed into your threat hunting efforts. Analyze patterns in the identified vulnerabilities, look for anomalies, and preemptively hunt for potential threats. This proactive approach can enhance your ability to detect and respond to threats early.

6. **Identifying Data at Risk:** Utilize NodeZero to perform a penetration test, simulating the behavior of an attacker attempting to gain unauthorized access to sensitive data. NodeZero identifies the vulnerabilities that could potentially lead to data exposure. Once vulnerabilities are identified, map them to the data assets they could compromise. This gives you an understanding of which data is at risk.

7. **Determining the Blast Radius of a Compromised Credential:** Use NodeZero to attack with a compromised credential. The scenario should attempt to escalate privileges, gain lateral movement within the network, and access sensitive data. The extent of access achieved in the scenario defines the blast radius of the compromised credential.

8. **Verifying the Effectiveness of Credential Policies:** Use NodeZero to execute a credential-based attack, attempting to compromise and reuse credentials based on your organization's credential policies. The success or failure of these attacks can provide insights into the effectiveness of your credential policies.

9. **Verifying the Effectiveness of Security Tools like EDR and SIEM:** After deploying NodeZero for autonomous pentesting, monitor the alerts and responses from your EDR (Endpoint Detection and Response) and SIEM (Security Information and Event Management) systems. If these tools detect and respond to the threats effectively, they are functioning as expected. If not, it might indicate a need for tuning or upgrading these security tools.

NodeZero's Capabilities in Support of CTEM and ASM

The following list of NodeZero's capabilities fit seamlessly into the CTEM and ASM frameworks. CTEM focuses on continuous, proactive vulnerability assessment, and NodeZero supports this by continuously discovering exploitable attack paths. In ASM, NodeZero reduces the exploitable attack surface, ensuring organizations prioritize real-world risks while streamlining detection, remediation, and compliance in their on-prem, cloud, and hybrid environments.

NodeZero Internal Pentests identifies vulnerabilities such as software misconfigurations, weak credentials, and insufficient security controls that could lead to domain compromise, data theft, and ransomware exposure. This helps organizations protect internal assets and ensures resilience by continuously assessing and reducing risks across various internal network infrastructures.

NodeZero External Pentests assess the security of publicly accessible assets like websites, servers, and applications. By scanning for exploitable vulnerabilities in external-facing systems, NodeZero ensures that organizations stay ahead of evolving attack vectors. It helps prevent external threats from infiltrating the network through these critical access points, offering proactive security.

NodeZero Phishing Impact Tests captures compromised credentials during internal phishing exercises. It then shows how attackers could leverage phished credentials to escalate privileges, move laterally through the network, or access sensitive data. By understanding the real-world impact of being phished, organizations reinforce their defenses against credential-based attacks.

NodeZero Rapid Response Service provides new attack content for the most critical vulnerabilities recently added to the CISA KEV. Organizations run targeted test so they can rapidly respond to zero-day or N-day vulnerabilities. This real-time capability determines if a vulnerability is exploitable, minimizes potential damage, and ensures rapid mitigation of critical vulnerabilities.

NodeZero Cloud Pentests are designed to identify IAM misconfigurations and vulnerabilities in cloud environments like AWS and Azure. By continuously testing cloud infrastructure, it helps organizations secure their assets in hybrid and multi-cloud setups. The automated nature of these pentests ensures scalability, offering comprehensive coverage and detailed remediation reports.

NodeZero Tripwires deploys decoys, such as fake credentials or files during its pentests to protect high-risk assets. These decoys provide real-time alerts when attackers engage with them, enabling organizations to detect breaches early. With low false-positive rates and seamless integration into existing security setups, Tripwires enhances proactive threat detection and response.

NodeZero GRC Insights offers a comprehensive view of the exploitable attack surface from multiple perspectives, tracking its evolution over time. It provides valuable metrics for risk reduction and compliance, with insights displayed through intuitive dashboards. Users can also generate detailed security reports for auditors and boards, ensuring transparent and effective communication.

Benefits of NodeZero to Red Teams, Blue Teams, and Security Analysts

NodeZero benefits red teams by automating the repetitive tasks associated with large-scale infrastructure pentesting. This allows red teams to focus their efforts on more complex, targeted testing, effectively serving as a force multiplier.

For blue teams, NodeZero offers the capability to proactively identify vulnerabilities and quickly verify that they have been remediated. Its detailed reporting also provides actionable insights that can help blue teams maintain a robust security posture.

Security analysts can leverage NodeZero's continuous testing data to enhance their threat detection and response capabilities. By understanding the vulnerabilities present in their organization's infrastructure, they can build better detection rules and respond more effectively to potential threats.

The Benefits and ROI of NodeZero within CTEM Programs

Implementing a CTEM program with NodeZero can bring a myriad of benefits to organizations, including improved security posture, increased operational efficiency, and significant return on investment (ROI).

From an operational perspective, NodeZero's autonomous pentesting capabilities can free up valuable time for security teams. It handles the time-consuming task of performing large-scale infrastructure penetration tests, allowing teams to focus on strategic tasks such as threat hunting, incident response, and remediation of critical vulnerabilities. This can lead to significant improvements in operational efficiency and productivity.

Additionally, NodeZero can support organizations in demonstrating compliance with various cybersecurity regulations, which can help avoid potential penalties and litigation.

From a financial perspective, investing in NodeZero can lead to substantial cost savings over time. Manual pentesting consulting services can be expensive, and the costs can add up significantly over time, especially given the need for regular testing in the modern threat landscape. NodeZero, on the other hand, provides continuous testing capabilities at a fraction of the cost, delivering significant ROI.

Furthermore, by helping organizations avoid the costs associated with data breaches – including remediation costs, regulatory fines, and lost business due to reputational damage – the ROI of NodeZero becomes even more substantial.

Finally, implementing the principles and practices outlined in this paper, and leveraging the power of NodeZero, you can transform your organization's approach to cybersecurity, delivering meaningful benefits and a strong return on investment.

The Future State: A Unified Platform for Attack Surface Management and Continuous Threat Exposure Management

As we move forward, the future of cybersecurity demands a unified, integrated ASM platform that brings together the key capabilities of continuous monitoring, autonomous pentesting, and security orchestration, automation, and response (SOAR). Such a platform can provide a holistic approach to managing and reducing the exploitable attack surface, facilitating a comprehensive and efficient CTEM program.

> **This envisioned platform will continuously identify vulnerabilities within an organization's attack surface, actively exploit these vulnerabilities to better understand real-world risk, and streamline the process of mitigating identified risks through orchestrated and automated responses. The unified platform will also incorporate detection engineering, using the data gathered to improve threat detection capabilities.**

Using this integrated platform, organizations will be able to seamlessly move from identifying vulnerabilities to assessing their exploitability and immediately acting upon this information. This real-time, cyclical process will significantly enhance an organization's ability to manage its risk and protect their network against threats.

NodeZero, with its autonomous pentesting capabilities, forms a critical part of this future state. Its ability to actively breach environments just as an actual attacker would, enables organizations to effectively identify their exploitable vulnerabilities and understand their real-world risk.

As more elements of the attack surface management process become integrated, organizations will gain a more comprehensive and actionable understanding of their real threat landscape. This integrated future will allow them to better manage their security posture, reduce their exploitable attack surface, and swiftly and effectively respond to the continuously evolving threat environment.

Gartner, Implement a Continuous Threat Exposure Management (CTEM) Program, Jeremy D'Hoinne, Pete Shoard, and 1 more, 21 July 2022.

Continuously find, fix, and verify your exploitable attack surface with NodeZero

- **To test drive NodeZero in your own environment, sign up for a free trial.**

https://www.horizon3.ai/trial

- **To learn how NodeZero can help secure your business, schedule a demo today.**

https://www.horizon3.ai/demo

@Horizon3ai info@horizon3.ai www.horizon3.ai

HORIZON3.ai
~~TRUST BUT~~ VERIFY