HORIZON3.ai

~~TRUST BUT~~ VERIFY

WHITE PAPER

Enhancing Splunk Deployments with NodeZero

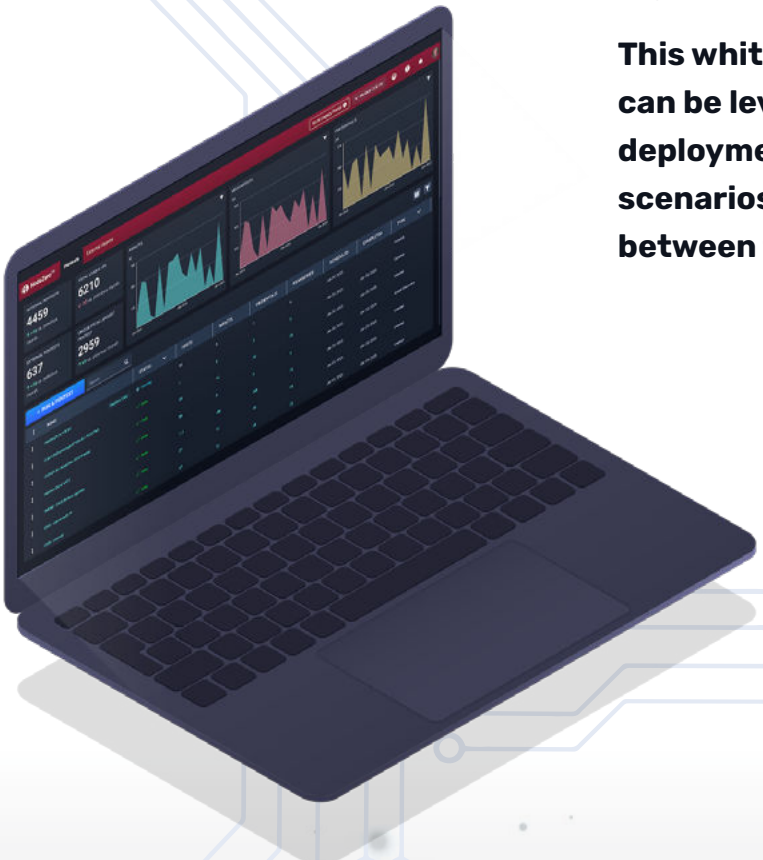
Enhance Splunk

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

Introduction

As security threats continue to evolve and become more sophisticated, the need for advanced security mechanisms and strategies has become paramount. Two technologies that stand out in this domain are the NodeZero™ platform and Splunk. NodeZero delivers powerful autonomous penetration testing, and Splunk is a leading security information and event management (SIEM) solution. When used together, these tools can significantly bolster an organization's security posture.

This whitepaper delves into how NodeZero can be leveraged to enhance a Splunk deployment and outlines five detailed scenarios that illustrate the synergy between these two technologies.



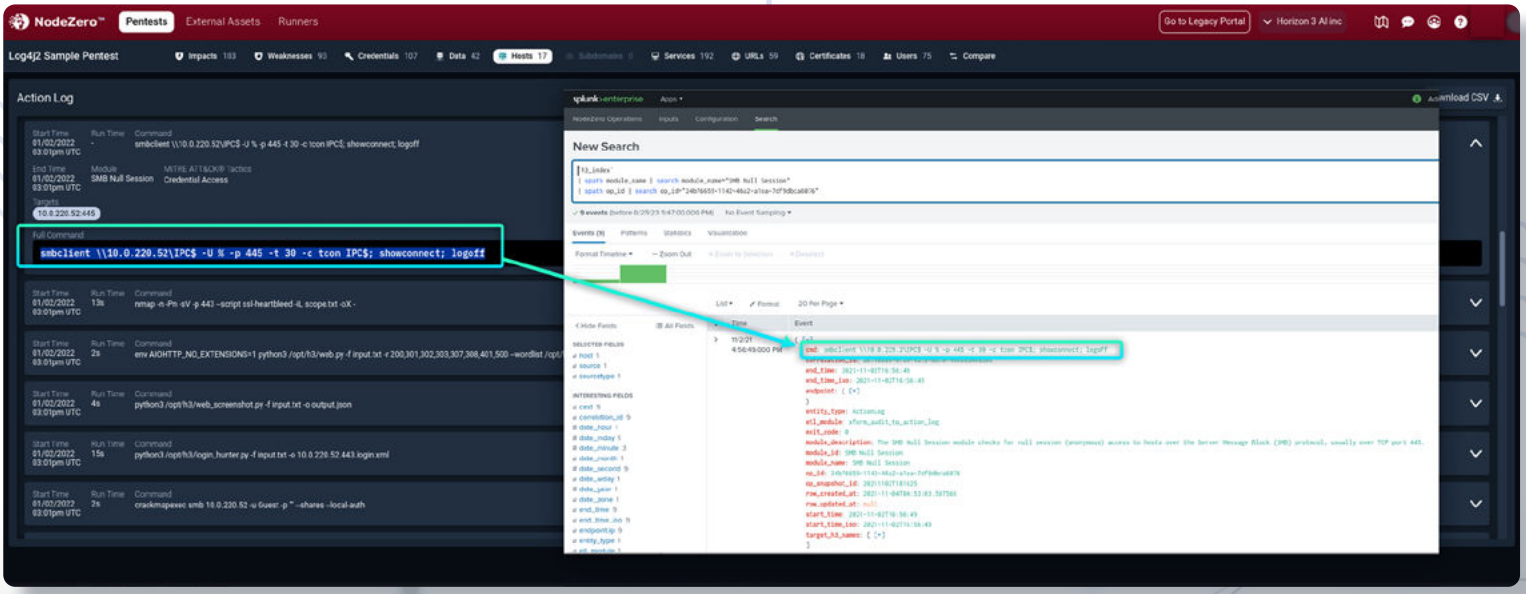
1 Identifying Logging Blindspots

Splunk excels at analyzing and visualizing data, but its effectiveness can be undermined by logging blindspots. NodeZero's continuous penetration testing can expose these blindspots, providing an opportunity to improve Splunk's data collection.

- The NodeZero Action Log lists every command executed on each IP. That data can be compared with Splunk logs to identify logging blindspots.

Workflow:

- NodeZero conducts penetration tests, executing specific commands on various hosts within your network.
- These actions produce digital exhaust, (messy machine information streams emanating from software applications, servers, IoT devices with their sensors and other core pieces of IT machinery), which should be picked up and logged by Splunk.
- Splunk users can then cross-reference the commands executed by NodeZero with the corresponding logs generated within Splunk.
- If a command executed by NodeZero doesn't have a corresponding log in Splunk, a logging blindspot is identified.
- The user can then troubleshoot and rectify this issue, adjusting the logging configuration as necessary to ensure comprehensive coverage and enhance Splunk's overall visibility.



HORIZON3.ai
TRUST BUT VERIFY

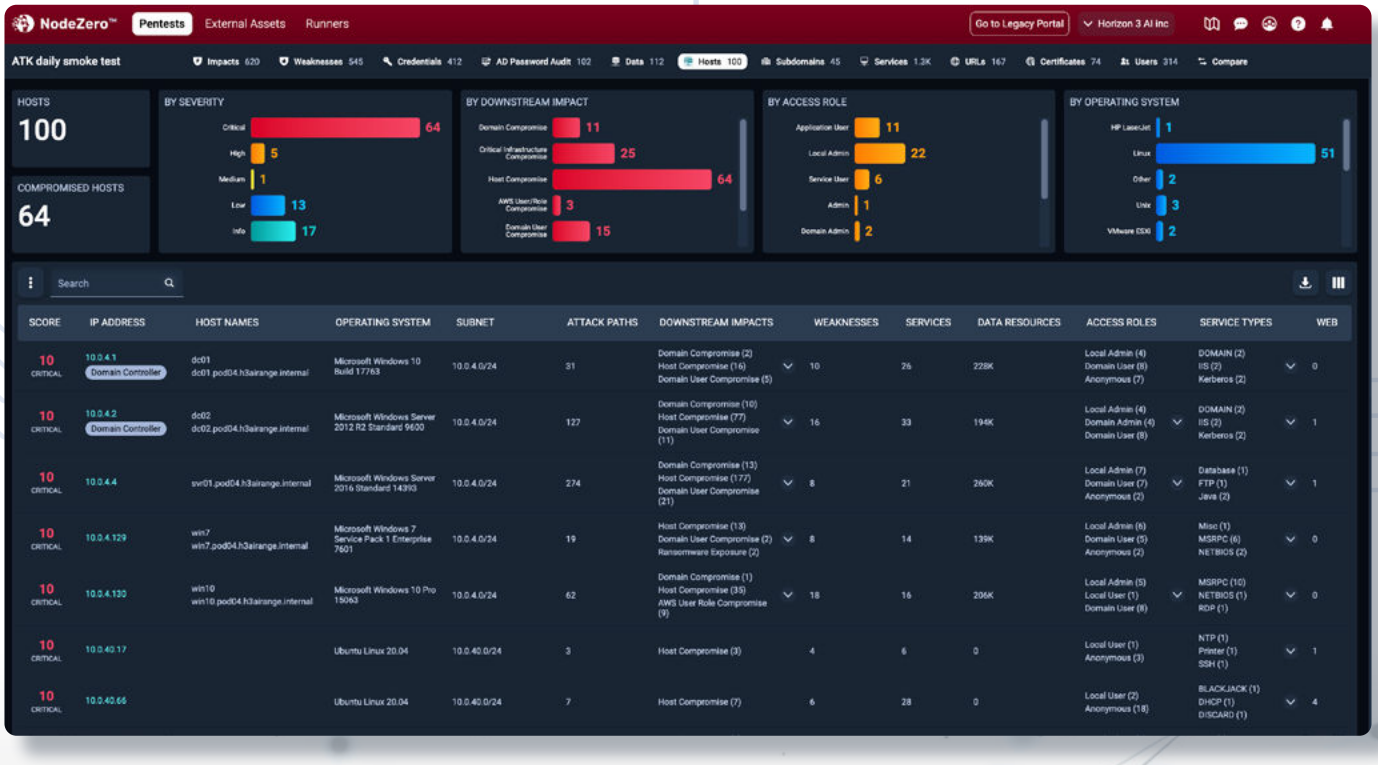
2 Prioritizing Host Logging

Given factors such as licensing and storage limitations, Splunk users often grapple with determining which hosts to prioritize for logging. NodeZero's contextual scoring system can guide these decisions.

- 64 of the 100 hosts identified have a critical severity score.

Workflow:

- NodeZero carries out penetration tests and assesses the criticality of each host based on how it could be exploited to compromise the environment.
- Splunk users can utilize these criticality scores to prioritize which hosts to focus their logging efforts.
- Scores can also be used to fine-tune the logging volume from each host, thereby ensuring the efficient use of Splunk licenses and storage resources.
- By doing so, Splunk users can ensure that the most critical and vulnerable hosts are being monitored appropriately, and no significant data is missed due to resource constraints.

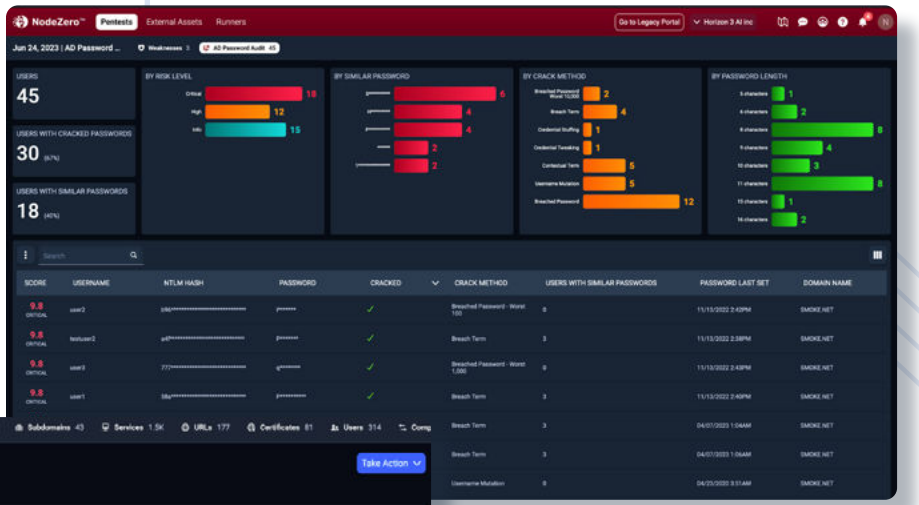


3 Triggering Remediations via SOAR Integration

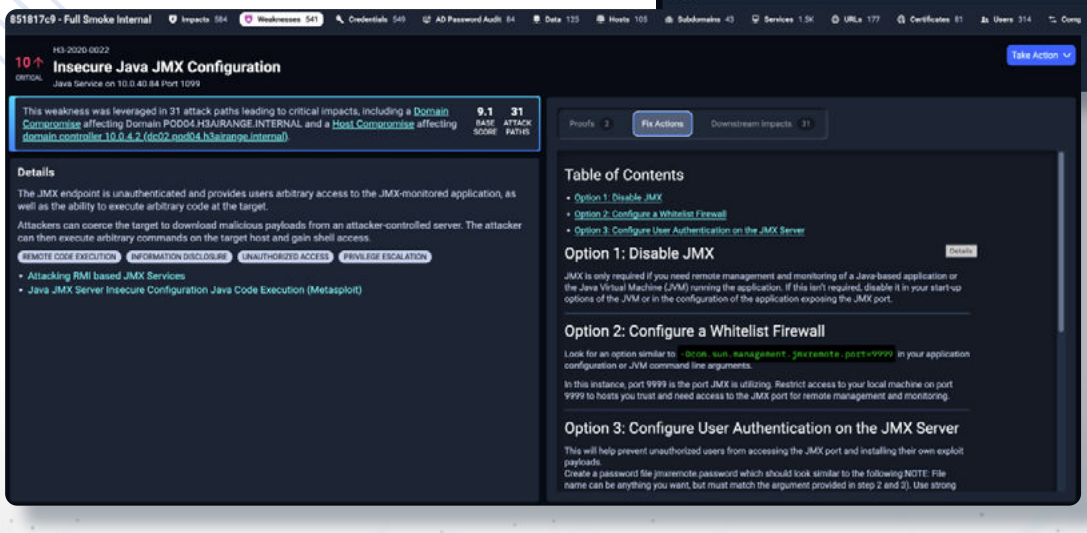
Security Orchestration, Automation, and Response (SOAR) platforms can provide automated workflows to accelerate the remediation process. NodeZero's API accessible data can aid in the creation of these workflows within a SOAR solution, thereby enhancing the automation of security operations.

Workflow:

- NodeZero identifies vulnerabilities, such as credentials with easily crackable or reused passwords.
- These identified vulnerabilities can be accessed via NodeZero's API.
- Splunk users can leverage this data to create new automated workflows within their SOAR solution, such as a password reset automation.
- These workflows can then be triggered based on NodeZero's findings, enabling quicker and more efficient remediation.



NodeZero identifies credentials with weak or reused passwords that should be reset



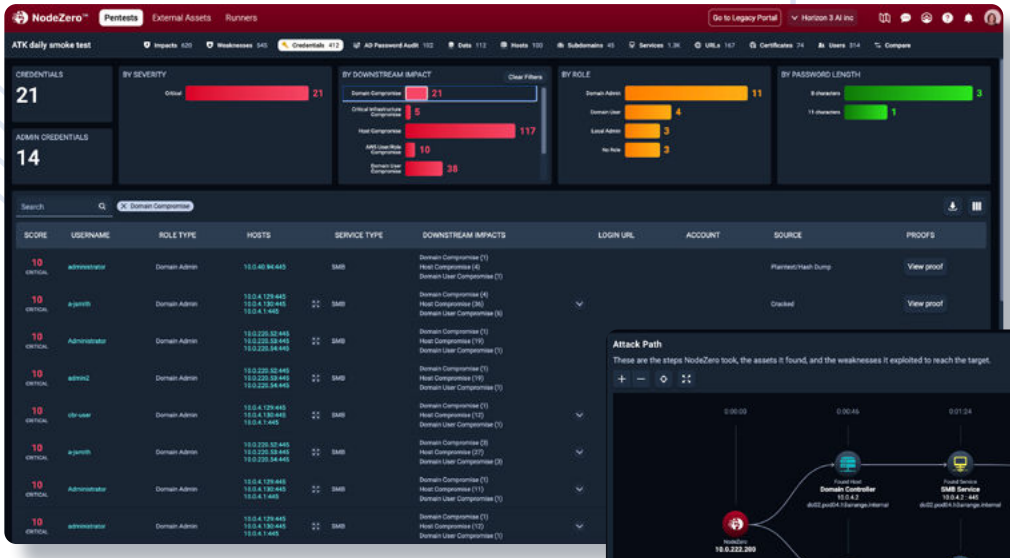
NodeZero provides detailed fix actions that can be automated in SOAR platforms

4 Monitoring and Alerting for Exploitable Attack Paths

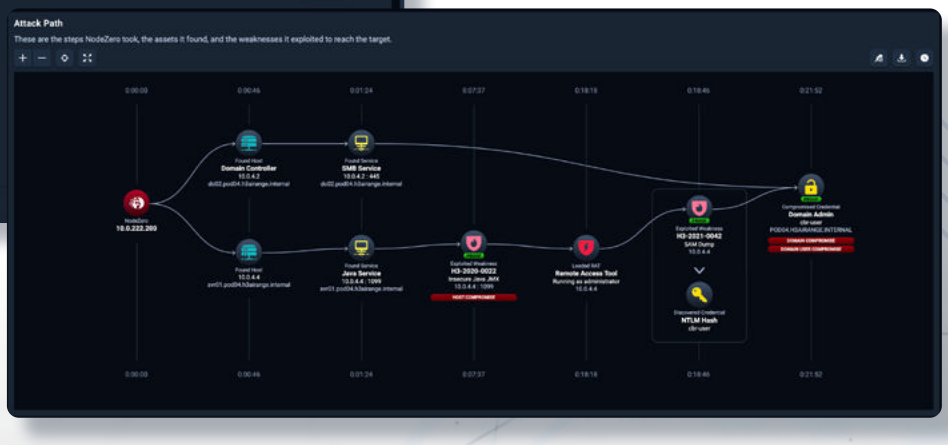
One of the most impactful ways in which NodeZero can bolster a Splunk deployment is by facilitating enhanced monitoring and alerting for exploitable attack paths. NodeZero's autonomous pentesting identifies and maps out these attack vectors, laying bare the steps an adversary could take to penetrate the network's defenses.

Workflow:

- NodeZero executes its autonomous pentesting and identifies an exploitable attack path in the environment. This could involve various tactics, from exploiting unpatched vulnerabilities to using compromised credentials for lateral movement across the network.
- The identified attack path can be added as a glass table or tailored dashboard within Splunk.
- A user can set up monitoring dashboards and alerting systems that focus specifically on the activities associated with the exploitable attack path. For instance, if an attack path involves exploiting a particular service on a host, Splunk can be set up to trigger an alert whenever an anomalous activity related to this service is detected.
- In addition to real-time alerting, Splunk users can use the historical data to analyze trends and patterns associated with the attack path to provide deeper insights and support strategic decision-making about network security.



The 21 credentials that led to Domain Compromise can be monitored in Splunk for abuse.



Exploitable attack path identified by NodeZero

Seamless Integration via SplunkBase

To ensure smooth interoperability between NodeZero and Splunk, an application is available on SplunkBase: NodeZero App for Splunk. SplunkBase is a marketplace for Splunk apps that enhance and extend the power of the Splunk platform.

Workflow:

- Users can download the NodeZero application from SplunkBase and install it within their Splunk environment.
- Once installed, the app communicates with the NodeZero platform via API to pull in relevant data.
- The NodeZero data is then ingested into Splunk, providing users with immediate access to actionable intelligence within the familiar Splunk interface.
- Splunk users can then leverage this information to identify logging blindspots, prioritize host logging, and trigger automated remediations via their SOAR integration, as detailed in the previous sections. Another option is to fold this new data into their existing workflows to enrich existing processes.

LINK: https://splunkbase.splunk.com/app/6461

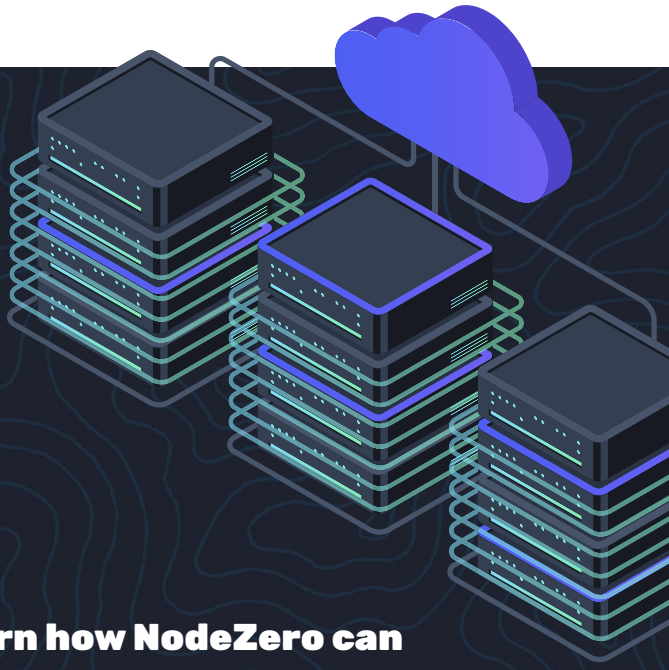
The NodeZero App for Splunk on SplunkBase has been designed to facilitate effortless integration between NodeZero and Splunk, making it easier for users to capitalize on the synergies of the two technologies. The app automatically ingests data from NodeZero, such as weaknesses found, criticality scores, host data, and detailed activity logs, and brings it into the Splunk environment, ensuring that key information is readily accessible within your Splunk deployment.

By bridging the gap between NodeZero and Splunk, the NodeZero App for Splunk on SplunkBase enhances the efficiency and efficacy of your security operations. This seamless integration allows you to derive more value from both NodeZero's autonomous penetration testing capabilities and Splunk's powerful data analysis and visualization features, fortifying your security posture.

Conclusion

By enabling precise and tailored monitoring and alerting based on identified attack paths, NodeZero and Splunk together create a proactive and intelligence-driven approach to network security. With this approach, organizations can not only react faster to threats but also strategically improve their overall security posture based on the intelligence provided by NodeZero's pentesting and Splunk's analytics.

The integration of NodeZero with Splunk offers a potent and proactive approach to tackling security challenges. By identifying logging blindspots, enabling prioritization of host logging, and triggering automated remediations via SOAR integration, these two technologies together provide a robust response to the complex security threats of the modern digital landscape. As cyber threats continue to become more sophisticated, the combined capabilities of NodeZero and Splunk ensure that organizations can maintain a strong security posture and protect their digital assets effectively.



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

https://www.horizon3.ai/trial

- **To learn how NodeZero can help you enhance Splunk, schedule a demo today.**

https://www.horizon3.ai/demo