premier®
experts

Autonomes PEN-Testing

NodeZero

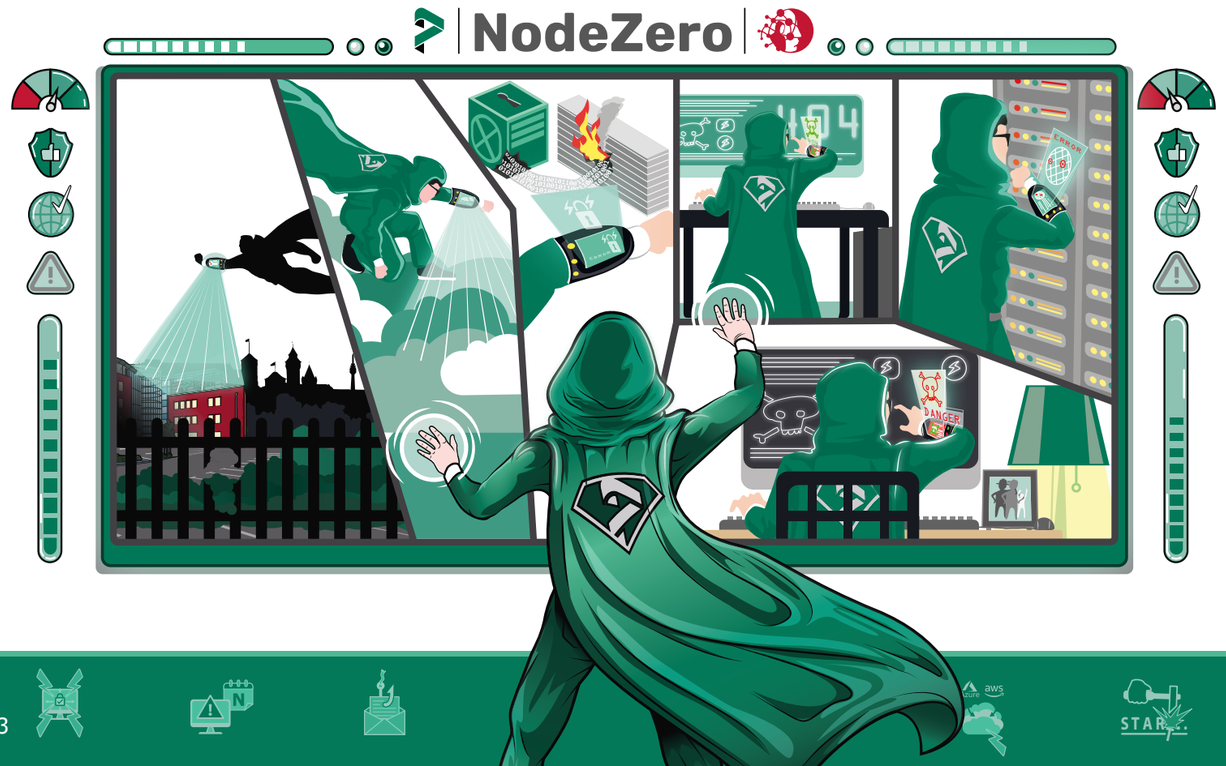
HORIZON3.ai
~~TRUST BUT~~ VERIFY

NIS 2 Directive

DORA
Digital Operational Resilience Act

Betrachten Sie Ihre IT ?
aus Sicht der Angreifer .

Was wäre, wenn Sie diese Frage
IMMER mit einem JA
beantworten könnten?



NodeZero ist ein Cybersicherheits-Tool, das folgende Schlüsseloperationen zur Bewertung und Validierung der Sicherheitslage selbstständig ausführt:

Internes PEN-Testing

NodeZero ermöglicht es unkompliziert – ganz im Sinne des „Assume-Breach-Mindsets" – die Perspektive eines Angreifers oder böswilligen Insiders einzunehmen, der sich bereits Zugang zum internen Netzwerk verschafft hat. **NodeZero** priorisiert mögliche Auswirkungen und bietet detaillierte Anleitungen zur Behebung.

Externes PEN-Testing

In der **Horizon3-EU-Cloud** gehostet und ohne zusätzlichen Einrichtungsaufwand durchführbar, bewertet das externe PEN-Testing schnell und präzise die Sicherheitslage aus der Perspektive eines Angreifers, der z.B. versucht den Perimeter zu durchbrechen.

Rapid Response & N-Day-Testing

Der einzigartige Horizon3 Rapid Response Service bietet **NodeZero**-Benutzern umfassende Bedrohungsinformationen über gezielte, hochkarätige Angriffe in Echtzeit. So kann präventiv reagiert werden, bevor diese Bedrohungen großflächig ausgenutzt werden. Bedrohungen können mittels Rapid Response entschärft werden, bevor diese in der Praxis Schaden anrichten.

AD Password Audit

Angreifer brechen nicht ein – sie loggen sich ein. Kompromittierte Zugangsdaten sind die Ursache für einen Großteil der Cyberangriffe. Mit regelmäßigen Überprüfungen der Wirksamkeit von Passwort- und Zugangsrichtlinien durch **NodeZero** wird sichergestellt, dass Cyberkriminellen hier keine Schwachstellen geboten werden.

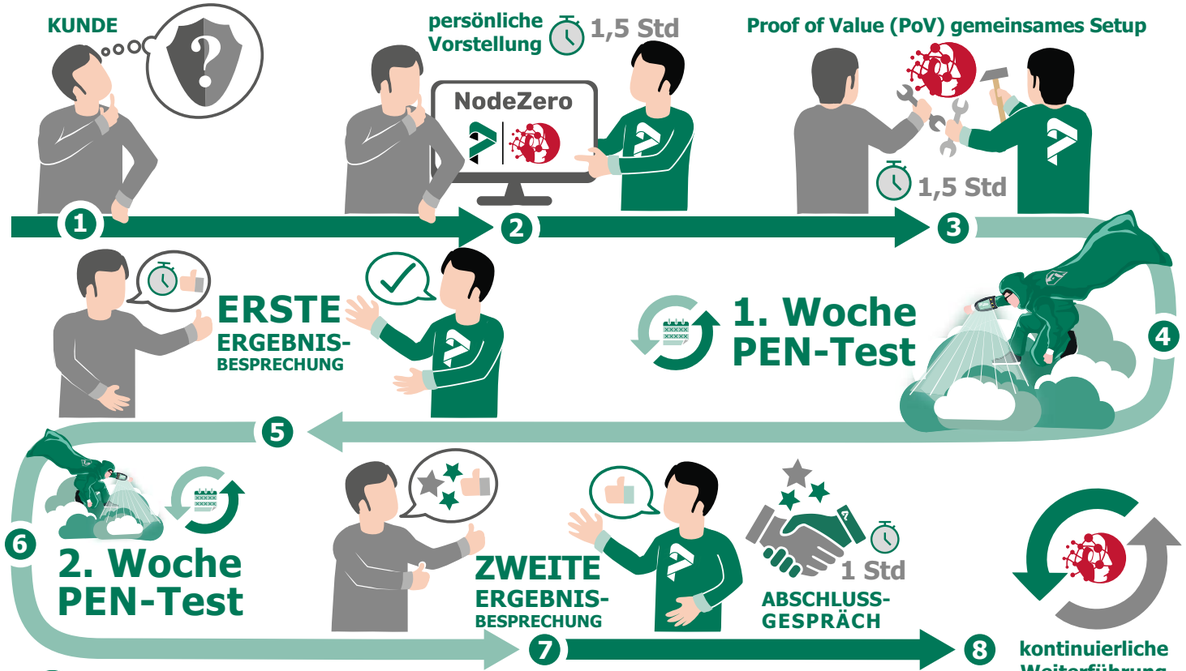
Cloud PEN-Testing

NodeZero integriert sich während interner PEN-Tests nahtlos in gängige Cloud-Umgebungen und entdeckt Angriffspfade zu Cloud-Assets und Cloud gehosteten Daten. Fehlkonfigurationen in der Cloud sowie kompromittierte oder hinterlegte Anmeldeinformationen eröffnen Angreifern den Zugang. Zusätzlich lassen sich gezielte Cloud-PEN-Tests durchführen, indem der **NodeZero**-Host direkt in der entsprechenden Umgebung platziert wird.

Phishing Impact Test

Es wird geprüft, was Angreifer mit über Phishing gewonnenen Anmeldeinformationen in der IT-Umgebung erreichen können. **NodeZero** hilft, die Auswirkungen eines Phishing-Incidents zu verstehen und empfiehlt Maßnahmen zur Minderung des Risikos.

DER WEG ZUM AUTONOMEN PEN-TESTING



Während des PoV entstehen keine Lizenzkosten und es wird im Gegensatz zu herkömmlichen PEN-Tests jede Menge Zeit eingespart.

DIE SCHRITTE IM DETAIL

1 Ausgangslage

Ist die IT Infrastruktur On-Premise und in der Cloud ausreichend vor Hackern geschützt?

2 Live Demo

Vorstellung von Horizon3 und **NodeZero** im Rahmen eines persönlichen Termins.

3 Gemeinsames Setup

Durch einen persönlichen PoV können erste PEN-Tests selbstständig durchgeführt und gemanaged werden.

4 Erste PEN-Tests

Für den Zeitraum von einer Woche werden interne und externe PEN-Tests autonom durchgeführt.

5 Nachbesprechung

Erste Ergebnisse und resultierende Lösungsmaßnahmen werden gemeinsam besprochen.

6 Weiterführende PEN-Tests

Verfizierung der bisher umgesetzten Lösungsmaßnahmen sowie weitere interne und externe PEN-Test-Durchläufe.

7 Abschlussgespräch

Planung für weiteres Vorgehen auf Grundlage der Ergebnisse der PEN-Tests wird gemeinsam erarbeitet.

8 Ziel

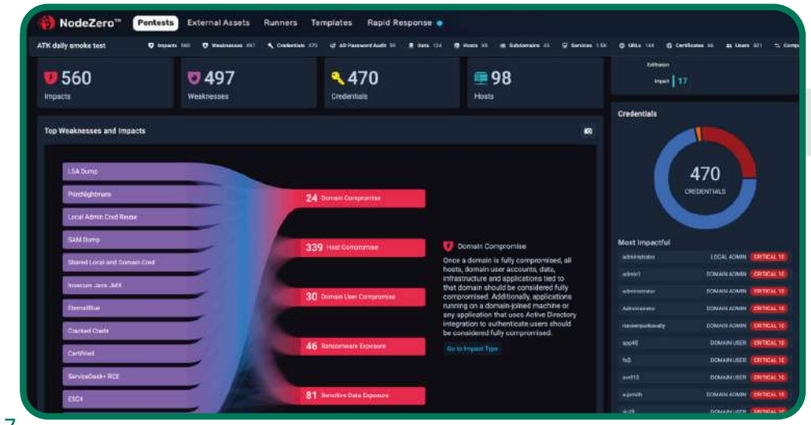
Übergang in regelmäßigen, autonomen PEN-Test-Betrieb. PoV-Tenant und alle bisherigen Ergebnisse können weiter verwendet werden.

ERKLÄRUNG VON NODEZERO

Die Planung und Durchführung beliebig vieler autonomer und parallel laufender PEN-Tests ist selbst in großen und komplexen Netzwerken möglich.

NodeZero entlastet das IT- und Sicherheitsteam – unabhängig von deren Erfahrungsniveau – sodass der Fokus stets auf dem Wesentlichen bleibt.

Erste **NodeZero**-PEN-Tests können in wenigen Minuten unkompliziert eingerichtet und autonom durchgeführt werden.



UNBEGRENZTE PEN-TESTS sind durchführbar auf:

- **On-premises Infrastruktur**
- **Identitäts- und Zugriffsmanagement**
- **Cloud-Infrastruktur**
- **Virtuelle Infrastruktur**
- **Öffentlich zugänglichen Assets**

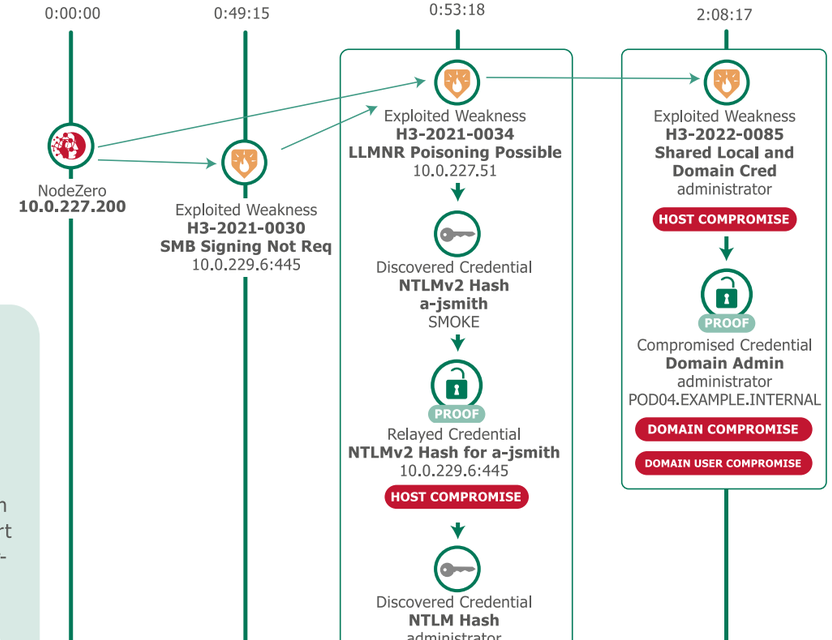
TRANSPARENZ & BERICHTERSTATTUNG ÜBER PEN-TESTS

Die von **NodeZero** durchgeführten Aktionen sind vollständig transparent und lassen sich im Anschluss nachvollziehen. Die Echtzeitansicht liefert Einblicke in die **NodeZero**-Exploits & Checks, während diese ausgeführt werden. Angriffspfad, Nachweis und Auswirkungen jeder identifizierten Schwachstelle können eingesehen werden.

Die Abschlussberichte sind auf die internen und externen Audit-Anforderungen zugeschnitten.

Sie beinhalten eine Zusammenfassung für Führungskräfte, PEN-Test-Berichte, Handlungsempfehlungen sowie Segmentierungsberichte und vieles mehr.

Der Angriffspfad rechts zeigt, wie **NodeZero** eine Schwachstelle auf dem Server ausnutzen konnte, um an Benutzer-Zugangsdaten zu kommen und mit diesen privilegierte Zugangsdaten des Servers zu extrahieren. Da ein Passwort-Audit fehlte, konnte der Admin des Unternehmens das gleiche Kennwort für einen domänenweiten Administrator-Account verwenden. **NodeZero** hat diesen Zustand ausgenutzt und damit die Domäne erfolgreich kompromittiert.



NODEZERO SERVICE BEI PREMIER EXPERTS

MANAGED SERVICE

Schluss mit vielen verschiedenen Tools, die sagen, was man zu tun hat?

- Das Team der premier experts kümmert sich um den Betrieb von **NodeZero**, wertet die Ergebnisse aus, plant, priorisiert und löst Findings zusammen mit dem IT-Team des Kunden und externen Partnern. Die Abarbeitung erfolgt nach Aufwand.
- In einem regelmäßigen Jour fixe werden Fortschritte sowie neu gefundene Sicherheitslücken besprochen und Arbeitspakete zur Behebung dieser Findings geschnürt.

Ein persönlicher premier expert sowie das Know-How des gesamten Teams stehen dabei zur Verfügung.

You scare – we care

HELP ON DEMAND SERVICE

Ist ein internes IT-Team mit ausreichend Ressourcen zur Koordination verfügbar?

- premier experts unterstützt dieses auf Anfrage bei der Abarbeitung der Findings interner und externer PEN-Tests nach Aufwand.
- Während des Proof of Value wird das IT-Team bereits mit dem Einsatz von **NodeZero** vertraut und kann bereits nach kurzer Zeit eigene PEN-Tests durchführen sowie den Scope dieser selbstständig erweitern.

You report – we support

Der Fokus liegt nicht auf Einzellösungen, sondern auf einer ganzheitlichen Betrachtung von Problemstellungen im Kontext der gesamten IT-Security-Strategie und -Planung. Mit umfassendem Know How unterstützen die premier experts das Unternehmen nachhaltig in den Bereichen IT und Security.

NodeZero bietet einfache Informationen inkl. Kennzahlen sowie kompakte & umfangreiche Reports inkl. maßgeschneiderte Informationen für ...

- **Informationssicherheitsbeauftragte**
- **IT-Teams**
- **CIOs**
- **Experten**

Das umfangreiche Security Portfolio der premier experts deckt von der Begleitung durch **ISO/TISAX**-Zertifizierungen, über eine **ISMS**-Einführung, bis hin zum **SoC**-Betrieb das gesamte Security Spektrum ab. Die große Stärke liegt dabei in der hohen technischen Expertise, abgerundet durch ein umfangreiches Software- & Lösungsportfolio.

NIS 2

Mit autonomen Penetrationstests haben Unternehmen ein leistungsstarkes Mittel zur Verbesserung ihrer Cybersicherheitspraktiken und zur Einhaltung der NIS-2-Richtlinie. Durch den Einsatz von Automatisierungen lassen sich umfassende Schwachstellenbewertungen effizienter durchführen, sodass Unternehmen Sicherheitslücken rechtzeitig erkennen und beheben können. Die Skalierbarkeit, Reproduzierbarkeit und Berichtsfunktion autonomer Penetrationstests machen sie zu einem wertvollen Instrument zur Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus in der gesamten Europäischen Union und zum Schutz kritischer Infrastrukturen sowie digitaler Dienste.

DORA

Autonome Penetrationstests sind ein leistungsstarkes Werkzeug, mit dessen Hilfe z.B. Finanzinstitute den Digital Operational Resilience Act (DORA) einhalten können. Dank des technologiegesteuerten Ansatzes können Unternehmen ihre digitale Infrastruktur laufend überwachen, Schwachstellen identifizieren und die betriebliche Widerstandsfähigkeit proaktiv stärken. Autonome Penetrationstests sind ein wesentlicher Bestandteil bei der Einhaltung der strengen Standards von DORA und tragen letztendlich zu einem sichereren und widerstandsfähigeren Finanzökosystem in der Europäischen Union bei.

SCAN ME

SCAN ME

premier experts

INTERESSE GEWECKT?

sales@premier-experts.de

Jetzt Kontakt aufnehmen