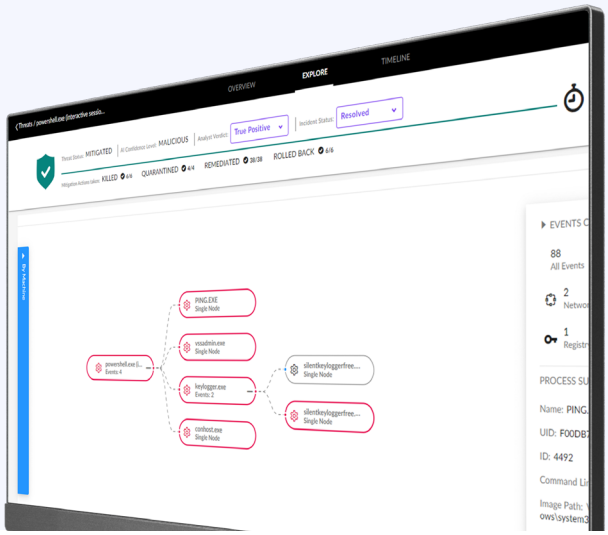
N-ABLE™

DATENBLATT

Endpoint Detection and Response

Eine eigenständige Lösung von N-able – powered by SentinelOne®

Endpoint Detection and Response (EDR) von N-able™ unterstützt MSPs und IT-Abteilungen dabei, die sich stetig weiterentwickelnden Cyberbedrohungen mithilfe von verhaltens- und KI-basierter Gefahrenerkennung sowie automatisierten Behebungsfunktionen und Rollbacks schnell zu erkennen und abzuwehren. Sicherheitsfachleute profitieren von der einfachen Automation-Manager-Richtlinie, der (AMP)-basierten Bereitstellung und der EDR-Statusüberprüfung innerhalb der N-able Remote-Überwachungs- und Management-Plattformen.



Einsatz mehrerer KI-basierter Erkennungs-Engines

- Nutzung von KI-Funktionen zur Analyse neuer Bedrohungsmuster und Maschinelles Lernen zur Entwicklung passender Reaktionen
- Erkennung bösartiger Aktivitäten wie dem Ausspähen des Speichers mithilfe von verhaltensbasierter KI
- Signaturlose Erkennung hochentwickelter dateibasierter Malware mithilfe von statischer KI

Effektive Abwehr von Cyberangriffen

- Schutz vor neuesten Bedrohungen ohne langwierige regelmäßige Scans oder Updates von Malware-Definitionen
- Durchsetzung benutzerspezifischer Schutzrichtlinien durch gezieltes, bedarfsorientiertes Blockieren/Zulassen von USB- und Geräteverbindungen

Wirksame Reaktionen durch Automatisierung

- Automatisierte, schnellere Abwehr von Bedrohungen sowie zügigeres Handeln bei Löschungs-, Quarantäne- und Abwehraktionen
- Zurücksetzen von Endpunkten und beschädigten Dateien auf ihren Zustand vor dem Angriff im Falle einer Attacke durch Ransomware (nur bei Windows-Betriebssystemen)

Schnelleres Aufspüren von Bedrohungen

- Aufspüren von Bedrohungen durch unmittelbar verfügbare Threat Intelligence führender Drittanbietersysteme und SentinelOne-Quellen
- Visualisierung von Bedrohungsaktivitäten – und zwar der gesamten Ereigniskette – um den Kontext, die Ursachen sowie die Seitwärtsbewegungen schnell analysieren zu können

Powered by SentinelOne®,

führend bei der 2022 MITRE Engenuity™ ATT&CK® Evaluation:

- 100 % Schutz und Erkennung
- Optimale Sichtbarkeit und Analysemöglichkeiten
- 100 % Echtzeit. Keine Verzögerungen bei der Erkennung

Einfache Einbindung von Drittanbietersystemen

- Optimale Anpassung von Syslog-Ereignissen an Ihr SIEM
- Nutzung lückenloser Benachrichtigungen zur Priorisierung und Steuerung von Tickets über Ihr PSA-Ticketsystem
- Nutzung von API-Diensten

Basierend auf der Singularity™-Plattform

- Singularity™-Steuerung und vollumfängliche Plattformpakete verfügbar
- Beinhaltet Steuerungsfunktionen für Geräte- und Endpunkt-Firewalls, Remote-Ausführung von Shell-Befehlen, Durchführung von Netzwerkquarantänen sowie Antimanipulationsfunktionen

Über N-able

N-able bietet MSPs und IT-Serviceanbietern leistungsstarke Software zur Überwachung, Verwaltung und Absicherung von IT-Infrastrukturen und Netzwerken. Unser Angebot umfasst eine skalierbare Plattform, eine sichere Infrastruktur, Tools für die einfachere Verwaltung komplexer IT-Umgebungen und Ressourcen für die digitale Transformation. Wir unterstützen unsere Partner in jeder Wachstumsphase beim Schutz ihrer Kunden sowie beim Ausbau ihres Angebots – durch das ständig wachsende flexible Portfolio an Integrationen führender Anbieter.

n-able.com/de

© 2022 N-able Solutions ULC und N-able Technologies Ltd. Alle Rechte vorbehalten.

Die Marken, Servicemarken und Logos von N-able sind ausschließlich Eigentum von N-able Solutions ULC und N-able Technologies Ltd. Alle anderen Marken sind Eigentum der jeweiligen Inhaber.

Dieses Dokument dient nur zu Informationszwecken und stellt keine Rechtsberatung dar. Für die hierin enthaltenen Informationen und deren Korrektheit, Vollständigkeit oder Nutzen übernimmt N-able weder ausdrücklich noch stillschweigend Gewähr noch Haftung oder Verantwortung.