FORENOVA SECURITY

www.ForeNova.com

sales@forenova.com

NovaCommand Was ist NDR?

NovaCommand: Intelligent Threat Detection and Response Platftorm

NovaCommand

Nova Command ist eine intelligente Plattform zur Erkennung von Gefahren und zur Reaktion auf Bedrohungen, die die Erkennungs- und Reaktionsmöglichkeiten der Kunden im Bereich Sicherheit deutlich verbessert.

Was ist NDR (Network Detection and Response)?

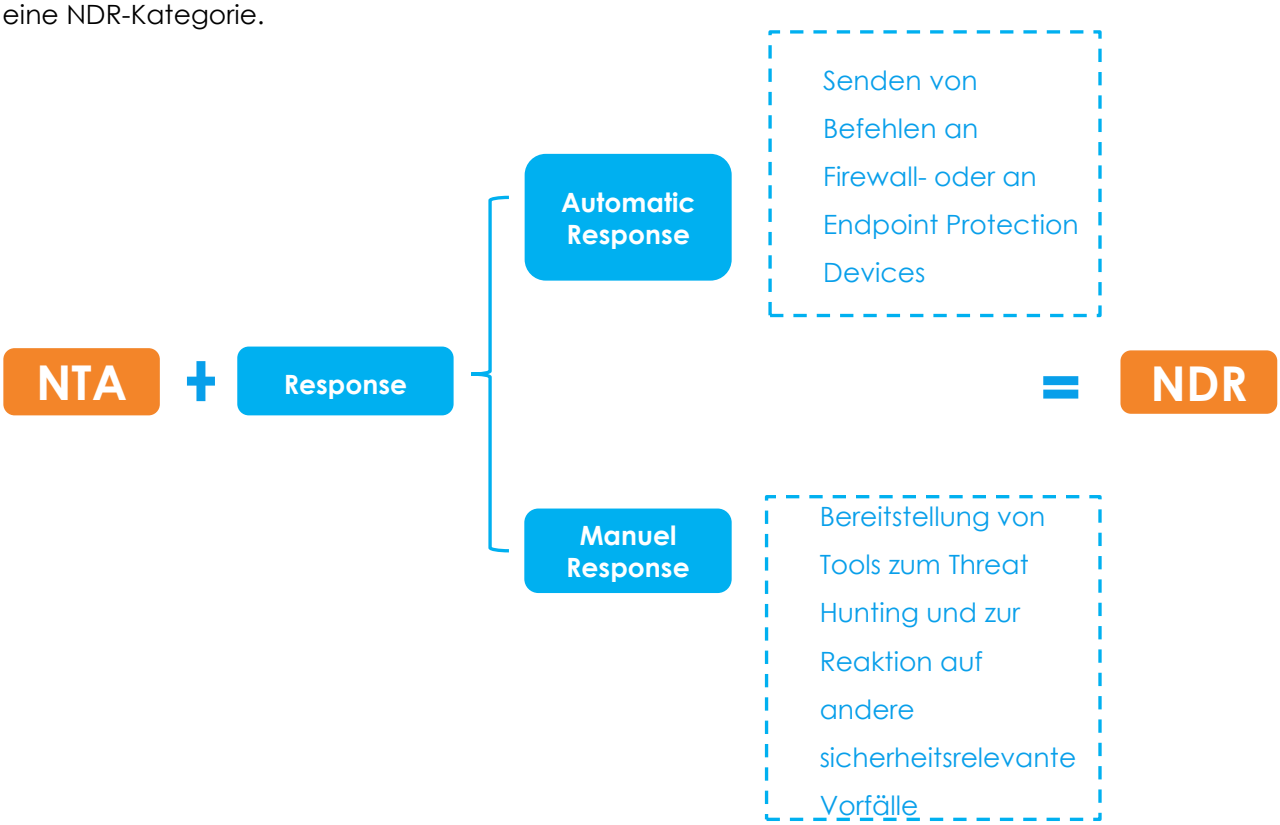
NTA

- Analyse der rohen Verkehrs-daten
- Beobachtung und Analyse des S-N & O-W Verkehrs
- Darstellung von anormalen Verkehr
- Nutzung von Verhaltenst echniken
- Betonung der Threat Detection Phase

Im Jahr 2019 veröffentlichte Gartner den ersten NTA-Marktleitfaden, in dem festgelegt wurde, dass NTA die folgenden Kriterien umfassen muss:

- Analyse von rohem Netzwerk-Paketverkehr oder Verkehrsflüssen (z. B. NetFlow-Aufzeichnungen) in Echtzeit oder nahezu in Echtzeit
- Überwachung und Analyse des Nord/Süd-Verkehrs (beim Überqueren der Grenzen) sowie des Ost/West-Verkehrs (bei der seitlichen Bewegung im Netzwerk)
- Modellierung des normalen Netzverkehrs und Erkennung des anomalen Verkehrs
- Anwendung von Verhaltenstechniken (nicht signaturbasierte Erkennung), wie maschinelles Lernen oder fortgeschrittene Analysen, die Netzwerkanomalien erkennen
- Schwerpunkt: Phase der Bedrohungserkennung und nicht die forensische Phase eines Angriffs, z. B. die Analyse von Paketaufnahmen (PCAP)

Im Jahr 2020 hat Gartner den "NTA Market Guide" in den "NDR Market Guide" umbenannt.
Im vergangenen Jahr haben alle NTA-Anbieter damit begonnen, ihre Lösungen um weitere automatische und manuelle Antwortfunktionen zu erweitern. So wurde aus NTA plus Reaktion eine NDR-Kategorie.



www.ForeNova.com
sales@forenova.com

Warum NDR?

Gartner stellt fest: "Die Anwendung von maschinellem Lernen und anderen Analysetechniken auf den Netzwerkverkehr hilft Unternehmen, verdächtigen Datenverkehr zu erkennen, der von anderen Sicherheitstools übersehen wird."

Erkennung der 1%

Täglich werden mehr als 500.000 neue Malware-Varianten entwickelt. Ihre vorhandenen Sicherheitslösungen können bis zu 99 % davon blockieren. Jedoch gibt es immer noch Tausende neuer Malware-Varianten, die Ihre Sicherheitseinrichtungen umgehen und Schaden anrichten können.

KI vs. KI

Hacker entwickeln immer raffiniertere Methoden um die KI-Technologie als Waffe einzusetzen. Herkömmliche Sicherheitssysteme können KI-Bedrohungen nur begrenzt erkennen. Deshalb brauchen wir KI, um KI zu besiegen.

100%ige Sichtbarkeit in Ihrem Netzwerk

NDR überwacht und analysiert sowohl den Nord/Süd- als auch den Ost/West-Verkehr. Das ist der schnellste und effizienteste Weg, um Bedrohungen in Ihrer Cloud, Ihrem Rechenzentrum, Ihrem Unternehmensnetzwerk und Ihren IoT-Geräten zu entdecken.

Warum NovaCommand?

Umfassende Detektionsfähigkeiten

Während andere NDR-Produkte lediglich Verhaltenserkennung einsetzen, nutzt NovaCommand mehrere Funktionen zur Erkennung von Gefahren. NovaCommand kombiniert signaturbasierte Erkennungen, Threat Intelligence und KI. Dadurch hat NovaCommand eine niedrige False-Positive Rate und eine hohe Erkennungsrate von Bedrohungen im Netzwerk.

Einfaches Modell zum Threat Hunting

Viele NDR-Produkte sind schwer zu bedienen. Mit NovaCommand können Bedrohungen schnell und einfach gefunden werden. NovaCommand verbessert die Usability durch die integrierte Bedrohungssuche, die Auswirkungsanalyse, eine Zeitleistenansicht für Eintrittspunkte sowie die Wiederherstellung von Angriffspatches.

Eingehende korrelierte Antwort

NovaCommand verbessert die Reaktionsmöglichkeiten durch die Integration von 3rd Party Produkten, wie Firewalls, Endpoint Protection und/oder Access Management Lösungen über eine offene API. Dadurch kann die Reaktion sowohl manuell als auch automatisch erfolgen.

Die Unterschiede zwischen NDR and SIEM

	NDR	SIEM
3rd-party Integration	• Fokus auf Response (Verwendung von Open AI für automatische Reaktionen) • Integration mit Endpoint Security, Firewalls und/oder Access Management Lösungen	• Schwerpunkt: Korrelation von Sicherheitsereignissen (Verwendung der Normalisierung von Logs) • Integration von vielen IT-Geräten (Server, Router, Switches, Sicherheitsgeräte)
Schlüssel-Szenario	• Fokus auf die Sicherheit (Erkennen Sie die Bedrohungen, die andere Lösungen übersehen) • Security Operation Center für mittelgroße Unternehmen - Einsatz von Sensoren zur Erkennung des gesamten Netzwerkverkehrs und Korrelation des Response mit Endpoint Security- und Netzwerksicherheitslösungen	• Logs Management • Bericht über die Einhaltung gesetzlicher Vorschriften (HIPPA, HIPAA, SOX, PII, NERC, COBIT 5, FISMA, PCI, etc.) • MSS/Großunternehmens-Security Operation Center - Aufbau für umfangreiche Sammlung von Logs (Sicherheitsanalysen basieren auf riesigen Datensätzen. Benötigt viele Ressourcen für den Betrieb)
Schlüssel-Technologien	• KI-Erkennungssysteme (Maschinelles Lernen/Big Data) • Analyse des Rohverkehrs • Integrierte Tools zur Untersuchung und zum Threat-Hunting	• Sammlung von Logs (API standardisieren) • Normalisierung von Logs • Korrelations-Engines (zugehörige Statistiken von Sicherheitsereignissen, Schwachstelleninformationen, Überwachungslisten, Asset-Informationen, Netzwerkinformationen und historische Informationen)
Technische Trends	• Erkennung von Anomalien im Netzwerk • Vereinfachtes Threat Hunting und Untersuchung von Bedrohungen • Automatischer Response (Verwendung offener API)	• Integrierte UEBA engines • Integrierte SOAR (Verwendung offener API)