SANS

Analyst Program

Product Review

Your Network, Under Control

Written by **Matt Bromiley**

August 2021

FORCENOVA

Deutsche Übersetzung: Jacqueline Krause

Inhalt

Einleitung

Sie können nicht etwas beschützen, das sie nicht sehen.

Diese Worte mit einem wahren Kern spiegeln die Informationssicherheit in vielen Unternehmen wieder. Viele Unternehmen sind nach einem Angriff unvorbereitet und stellen fest, dass sie keinen umfassenden Überblick über die Sicherheit ihres Unternehmens hatten. Die Situation wird nur noch schlimmer, wenn eine Untersuchung ergibt, dass der Angreifer entweder breiter aufgestellt ist oder älter als bisher angenommen (beide Szenarien sind möglich).

Um diese Situation von Anfang an zu vermeiden, sollten Sicherheitsteams nach einem Tool Ausschau halten, mit dem sie einen Überblick über ihre gesamte Sicherheitslandschaft erhalten. Glücklicherweise hat jede Organisation einen "gemeinsamen Nenner", den alle angeschlossenen Anlagen nutzen: das Netzwerk. Network detection and response (NDR) ist der richtige Ansatz, um potentielle Sicherheitsrisiken und Gefahren in jedem Unternehmen sichtbar zu machen und um Angreifer aufzuspüren, da sie das Netzwerk nicht einfach umgehen können. NDR erweist sich jedoch als leichter gesagt als getan, denn Netze enthalten von Natur aus eine Vielzahl an Daten, die sich mit halsbrecherischer Geschwindigkeit im Netzwerk bewegen.

In diesem Produktbericht untersuchen wir eine Plattform, die Unternehmen dabei hilft, einen Überblick über ihr Netzwerk zu erlangen und NDR sinnvoll zu nutzen: ForeNova.

ForeNovas einfach zu bedienende Plattform, NovaCommand, macht die Untersuchung und den Zusammenhang Ihrer Netzwerkdaten einfach. NovaCommand verbindet Echtzeit-Identifizierung und -Klassifizierung mit robusten Erkennungs- und Reaktionsfähigkeiten. Analysten erhalten dadurch einen einzigartigen Überblick über ihre Sicherheitslandschaft.

NovaCommand bietet folgende Funktionen/Vorteile:

- Überblick über das gesamte Netzwerk eines Unternehmens in Echtzeit und mit einem sofortigem Überblick und Identifizierung aller Geräte
- Automatische Klassifizierung von Server- und Non-Server-Assets, die granulare Asset Kontrollen ermöglichen und den erwarteten Datenverkehr jeder Gruppe mit dem tatsächlichen Datenverkehr vergleichen
- Erkennung von Bedrohungen und Reaktion auf Vorfälle, alles gebündelt in einem leistungsstarken Tool
- Netzwerkzentrierte Erkennung und Reaktion für eine Organisation, einschließlich Nord-Süd und Ost-West-Verkehr
- Third-Party-Integration zur einfachen Einbindung von NDR in andere Sicherheitskontrollen, die bereits in Ihrer Umgebung eingesetzt werden

NovaCommand macht ein komplexes und vielschichtiges Thema wie NDR sofort für Sicherheitsteams umsetzbar. Wenn es heute darum geht, Angreifer aufzuspüren und zu stoppen, sollten Sie Ihr Netzwerk nicht aus der Telemetrie ausschließen.

Stellen Sie sich beim Lesen dieses Berichts folgende Fragen:

- Habe ich die gleiche Sichtbarkeit/Transparenz in meinem IT-Security Umfeld?
- Nutzt mein Sicherheitsteam das Netzwerk als gemeinsame Quelle, um Bedrohungen zu erkennen und darauf zu reagieren?
- Wenn mein Unternehmen Netzwerkdaten verwendet, wie werden diese dann aufgenommen? Erfassen wir einfach Logs und korrelieren sie mit den Daten, oder können wir im Netzwerk genauso vorgehen wie an den Endpunkten?

Wenn eine der obigen Fragen Sie stutzig gemacht hat oder Sie Ihre Unternehmenssichtbarkeit in Frage stellen, sollten wir untersuchen, wie eine NDR-Plattform so aufgebaut werden kann, dass sie zu den Bedürfnissen ihres Teams und zu den Anforderungen ihres Unternehmens passt.

Sichtbarkeit mit NovaCommand

Wir beginnen unser Review dort, wo Analysten ihren Tag verbringen: auf der Seite des ersten Dashboards. Das Dashboard von NovaCommand (siehe Abbildung 1) ist vollgepackt mit Einblicken über die Organisation und Maßnahmen zur Analyse und Reaktion auf Bedrohungen.

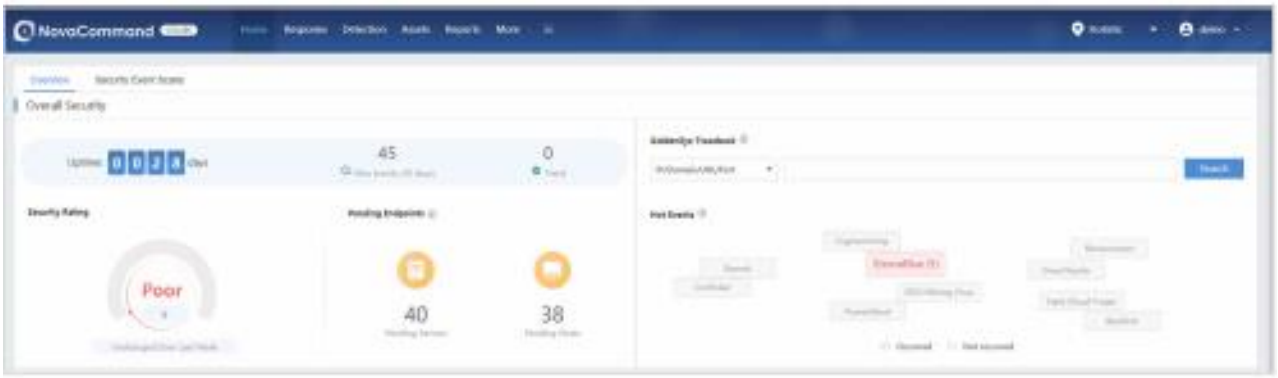

Abbildung 1: Erste Zeile von NovaCommands Dashboard

Wie die Abbildung veranschaulicht, bietet die erste Zeile des Dashboards zusammengefasste Analysen und Schlüsseldaten, wie zum Beispiel:

- Eine gesamte Bewertung der Sicherheit des Unternehmensnetzes in Echtzeit
- Im Netz beobachtete "heiße" Ereignisse
- Eine Übersicht über ausstehende Endpunkte, aufgeteilt in Server und Hosts
- Die Betriebszeit des Netzes
- Eine GoldenEye Traceback-Suchleiste (mehr dazu später)

In diesem Bericht gehen wir mehrfach auf jeden dieser Punkte ein. Ein Thema zieht sich jedoch wie ein roter Faden durch alle Themen und das ist die Frage: **Was passiert gerade in meinem Netzwerk?** Wir sind große Fans von Dashboards, die "auf den Punkt" kommen und NovaCommand tut dies sofort. Die oberste Zeile bietet einen zusammenfassenden Blickwinkel. Der letzte Teil, dargestellt in Abbildung 2, zeigt einen detaillierten Einblick in die Organisation und die tatsächlichen Fähigkeiten von NovaCommand im Umgang mit empfangenen Daten. NovaCommand trennt die Umgebung automatisch nach Server und Host (wir interpretieren Host als einen Nicht-Server-Endpunkt). Wir schätzen die Klassifizierung der Assets in Server und Nicht-Server. Einige Analysten argumentieren möglicherweise, dass die Kategorisierung von Daten zwischen Server und Nicht-Server keine Rolle spielt, wenn ein Angriff stattfindet. Bedenken Sie jedoch, dass wir das Unternehmen aus einer Netzwerkperspektive heraus betrachten. Beide Asset-Gruppen stellen unterschiedliche Arten von Verkehr dar. Daher sollten sie analysiert werden und auf unterschiedliche Weise in Berichte einfließen. In diesem Produktbericht untersuchen wir NovaCommand, die Plattform zur Analyse des Datenverkehrs und zur Erkennung und Reaktion auf sicherheitsrelevante Vorfälle. NovaCommand

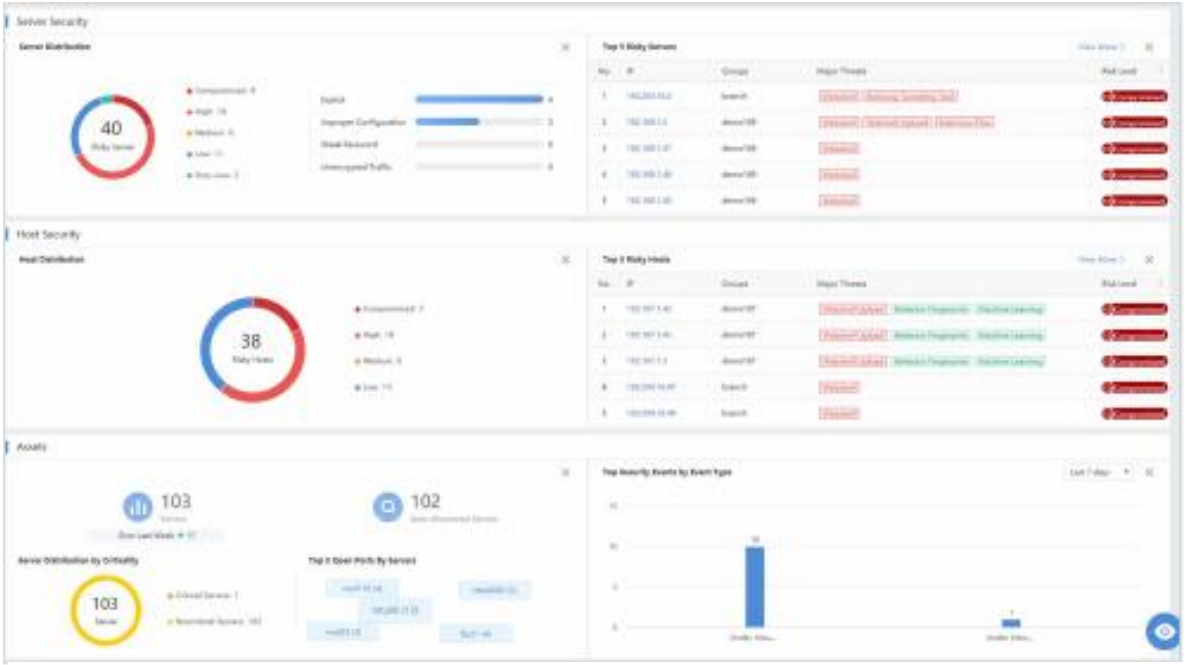

Abbildung 2: Letzter Teil von NovaCommands ursprünglichem Dashboard

wird mit Daten von ForeNovas NovaSensor gespeist, einem leistungsstarken Sensor, der Daten auf der Grundlage von künstlicher Intelligenz und benutzerdefinierten Regeln klassifiziert. NovaSensor stellen wir in diesem Bericht nicht ausführlicher vor, jedoch ist er notwendig für die Weiterleitung des Datenverkehrs und für Metadaten an die NovaCommand-Plattform.

Verschiedene Systeme innerhalb der Servergruppe sind mit dem Internet verbunden, während dies bei Nicht-Servern nicht zu erwarten ist. Ein weiterer Vorteil dieser Art der High-Level-Klassifizierung ist, dass Analysten NovaCommand verwenden können, um Erkennungen von Bedrohungen auf der Grundlage des Host-Typs zu schreiben und so mehr Bedrohungen aufzudecken.

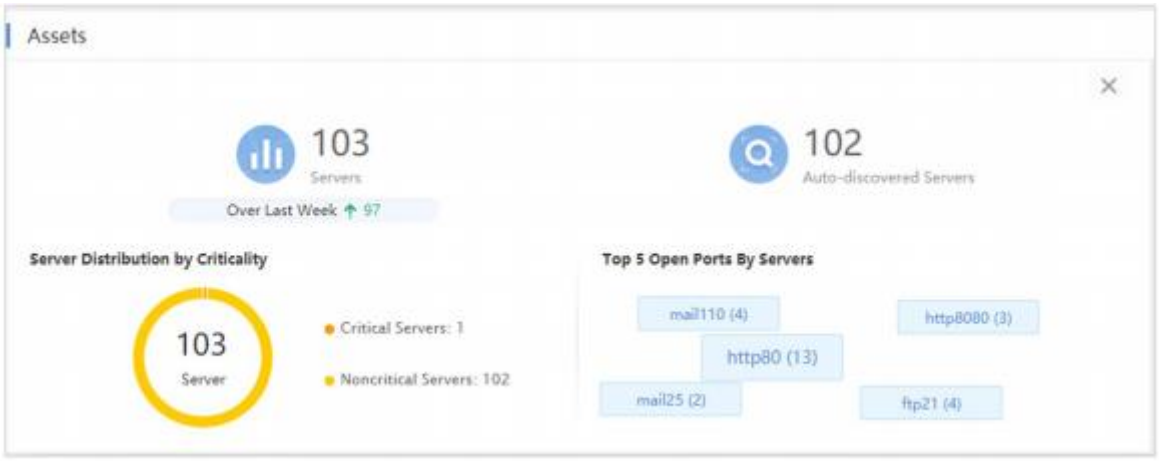

Abbildung 3: Ausschnitt des Asset Widget (NovaCommands Dashboard)

In Abbildung 2 werden NovaCommand Server-spezifische Details über Angriffe dargestellt, beispielsweise, ob ein Exploit verwendet wurde oder ein Server unsachgemäß konfiguriert war. Außerdem zählt NovaCommand auch die risikoreichsten Anlagen in jeder Gruppe auf und liefert detaillierte Informationen über die beobachteten Bedrohungen und den Risikograd des Systems. In einem späteren Abschnitt werden wir dies weiter ausführen. NovaCommand ist mehr als eine Plattform zur Erkennung und Reaktion von potenziellen Bedrohungen und Gefahren, da das gesamte Netzwerk übersichtlich dargestellt ist. Zudem ist NovaCommand ein unglaublich leistungsfähiges Instrument zur Verwaltung von Assets. Weder Angreifer noch vernetzte Geräte können das Netzwerk umgehen. NovaCommand bietet eine Asset-Klassifizierung, die weder den Einsatz von endpunkt- noch domänbasierten Inventarisierungstools erfordert (siehe Abbildung 3). Zudem werden auf der Grundlage des beobachteten Datenverkehrs automatisch alle Server im Netzwerk entdeckt. Eine weitere, nützliche Funktion ist die Einbeziehung offener Ports, die im Datenverkehr beobachtet wurden. Wir haben festgestellt, dass Analysten und Serveradministratoren dadurch eine schnelle Überprüfung durchführen können. Ein seltsamer oder unerwarteter Port in dieser Kategorie kann ein einfacher und effizienter Weg sein, um eine mögliche Fehlkonfiguration zu entdecken oder um verdächtige Aktivitäten aufzudecken.

Umsetzbare Sichtbarkeit

Bevor wir uns mit der Erkennung und Reaktion von Bedrohungen und Gefahren mit NovaCommand beschäftigen, wollen die Verwendung der Plattform als Instrument zur Klassifizierung von Assets näher betrachten. Leider kommt es in Unternehmen in vielen Fällen zu Sicherheitslücken, weil ein System unübersichtlich gestaltet ist und somit schlecht von dem Sicherheitsteam kontrolliert, werden kann. Wir lösen dieses Problem, indem wir Netzwerke übersichtlich darstellen und klassifizieren.

Abbildung 4: Ausschnitt aus der Nova Command Navigationsleiste, zeigt Assets als Schlüsselfunktion der Plattform

Sowohl die Klassifizierung als auch die Übersichtlichkeit des Netzwerkes sind entscheidende Kriterien für eine erfolgreiche Erkennung und Reaktion auf Bedrohungen. ForeNova hat dies erkannt und baute die Klassifizierung von Assets als Hauptmerkmal der Plattform ein (siehe Abbildung 4). NovaCommand stellt nicht nur Assets übersichtlich dar, sondern kann sie auf der Grundlage von Schwachstellen kategorisieren, die zuvor mithilfe von Analysen und integrierten Bedrohungsdaten der Plattform ermittelt wurden. Die Übersichtsseite der Assets ist der erste Schritt, um einen Überblick in die Organisation zu erlangen. Wie in der Abbildung 5 dargestellt, bietet die Seite "Assets" von NovaCommand noch mehr Einblick in die im Netzwerkverkehr beobachteten Assets. Zusätzlich zu der Kategorisierung von Servern und Nicht-Servern ermöglicht NovaCommand eine Gruppierung von Assets, eine Einstufung kritischer Systeme, eine Betriebssystemidentifizierung und eine Änderung (Erhöhung oder Verringerung) der Asset-Nummern. Wie das anfängliche Dashboard stellt dieser nützliche Bildschirm alle Assets übersichtlich dar. NovaCommand bietet im Rahmen seiner Asset-Klassifizierungsfunktionen auch eine Übersicht über gefundene Schwachstellen. In dem Tab „Schwachstellen“ können Sie alle eingesetzten Assets sehen und können diese verwalten.

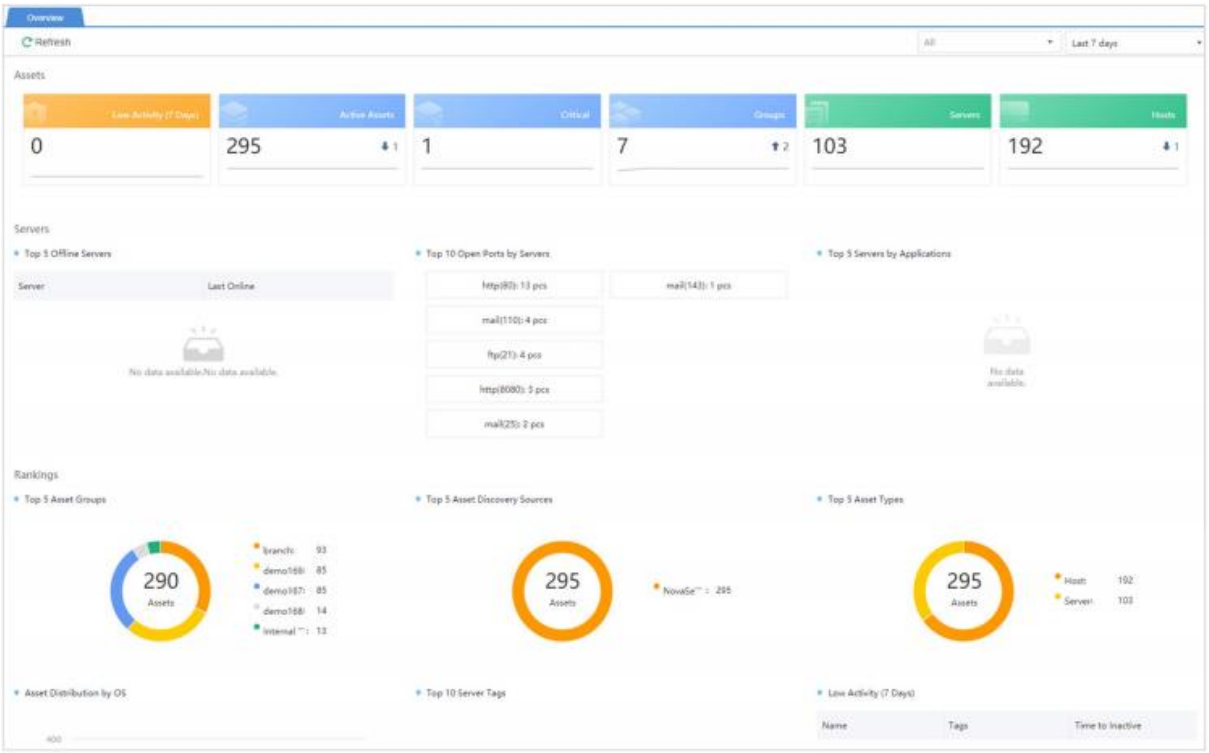

Abbildung 5: Screenshot des Dashboards Asset Overview

Jahrelang galt der Überblick über alle eingesetzten Assets als das essenzielle Erfolgskriterium zur Aufdeckung und Reaktion auf Angriffe und Bedrohungen. Das bloße "Wissen", dass sich ein Asset

in einem Netzwerk befindet, reicht jedoch nicht aus. Mit NovaCommand können Sicherheitsteams bessere Erkennungen von Gefahren und Bedrohungen schreiben, effektive Reaktionspläne entwickeln und die Sicherheit ihres Netzwerkes erhöhen.

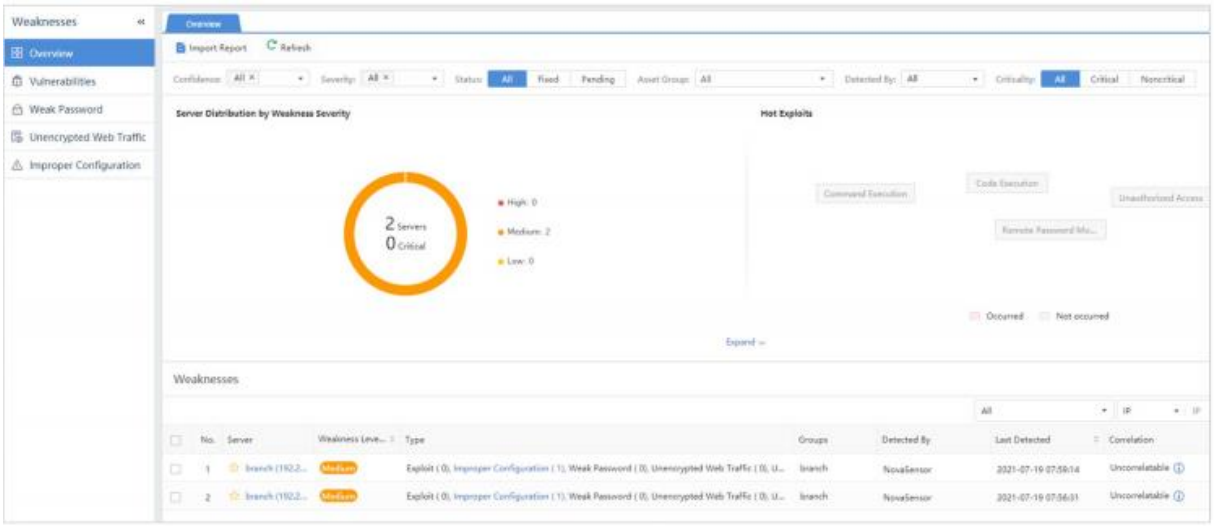

Abbildung 6: Ausschnitt aus der Registerkarte Schwachstellen, einer Asset-Sichtweise aus NovaCommand

Unter dem Tab „Schwachstellen“ werden die wichtigsten Schwachstellen oder Fehlkonfigurationen in der Netzwerk Umgebung aufgedeckt, die behoben werden müssen (siehe Abbildung 6). Diese Funktion unterscheidet NovaCommand von anderen Anbietern im Bereich der Asset-Klassifizierung. Diese Seite bietet Ihnen Details zu den gefundenen Schwachstellen, um zukünftige Sicherheitsprobleme zu vermeiden. In Abbildung 7 sehen Sie den ersten Server, bei dem eine Schwachstelle festgestellt wurde und es wird zusätzlich der Detaillierungsgrad aufgezeigt.

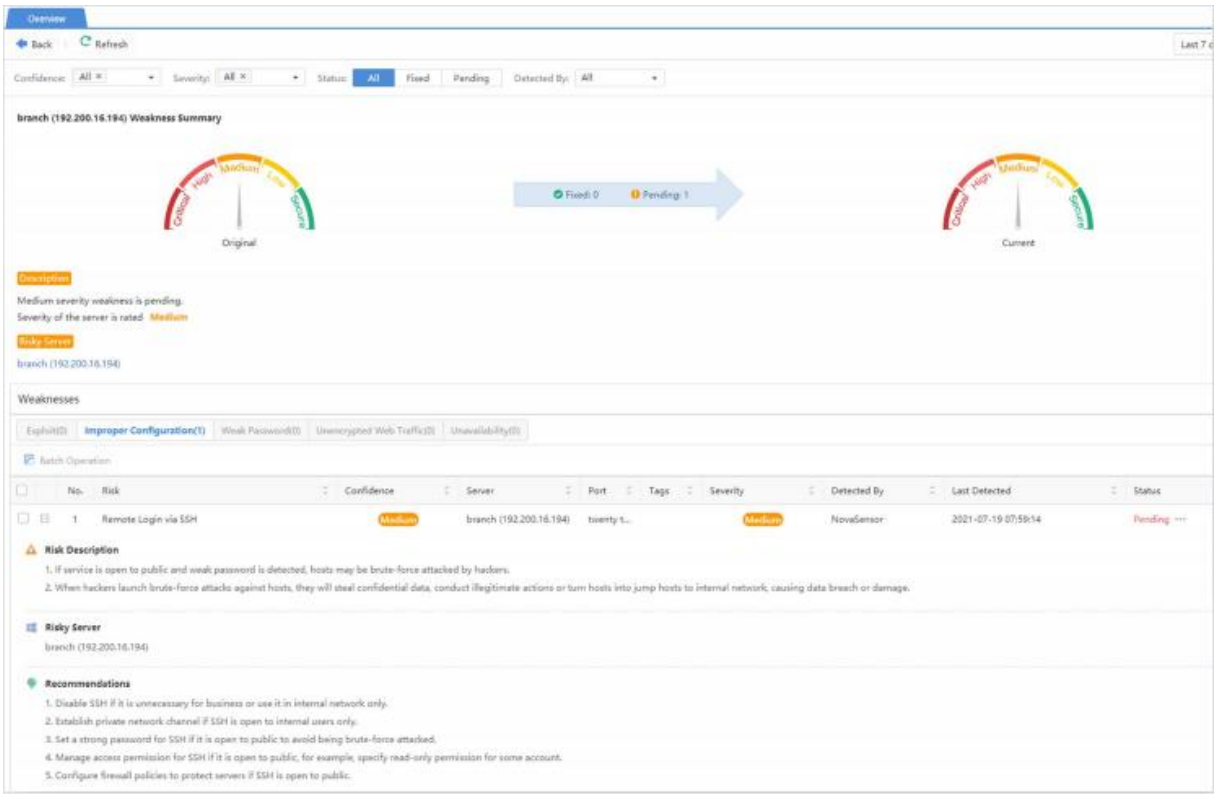

Abbildung 7: Ausschnitt des Weakness Overview Tab für ein Demosystem

Die in Abbildung 7 identifizierte Schwachstelle ist ein offener SSH-Port, der für eine Fernanmeldung in der Umgebung ausgenutzt werden kann. NovaCommand identifiziert hierbei nicht nur die Schwachstelle (die als mittelkritisch eingestuft wird), sondern liefert auch eine Beschreibung der potenziellen Risiken und eine Empfehlung, um die Schwachstelle zu beheben. Diese Daten sind für das Sicherheitsteam von immensem Wert. Wir sind immer an proaktivem Wissen interessiert, das wir nutzen können, um eine Organisation zu schützen. Fehlkonfigurationen, schwache Passwörter oder ein unverschlüsselter Webverkehr sind Beispiele für Dinge, die Sicherheitsteams so schnell wie möglich beheben sollten. Glücklicherweise stellt NovaCommand mehrere Empfehlungen bereit, um jedes Problem zu entschärfen. Dabei empfiehlt NovaCommand nicht einfach "den Port zu deaktivieren“, sondern bietet Anleitungen zu Kontoberechtigungen, Passwortkomplexität und Firewall-Richtlinien. NovaCommand berücksichtigt dabei auch zukünftige Änderungen in einer Systemschwäche (siehe Abbildung 7). Wenn die Fehlkonfiguration behoben ist, wird sich die Kritikalität des Systems im oberen Teil von Abbildung 7 entsprechend ändern. Auch positive Veränderungen in der Umgebung werden automatisch erfasst und dargestellt, indem NovaCommand (auf der Grundlage des beobachteten Datenverkehrs und der Systeminspektion) seine Ranglisten aktualisiert. Das Sicherheitsteam erhält durch diese Funktionen von NovaCommand einen wertvollen und unmittelbaren Überblick über die Organisation und weiß, wie es seine Aufgaben priorisieren kann.

Zusätzlich zu den umfangreichen Datenberichten und -klassifizierungen enthält ForeNova auch eine einfache Berichtsfunktionen. Die Berichte werden bei Bedarf erstellt und enthalten eine Vielzahl an Details zur Unternehmenssicherheit, die leicht exportiert und geteilt werden können (siehe Abbildung 8). Dies ermöglicht es Sicherheitsverantwortlichen und Managern, Sicherheitsschwächen und -muster in der Security Umgebung zu verfolgen und die Aufgaben der Analysten entsprechend zu priorisieren.

Abbildung 8: Muster einer Berichtsliste

Störungsfallerkennung

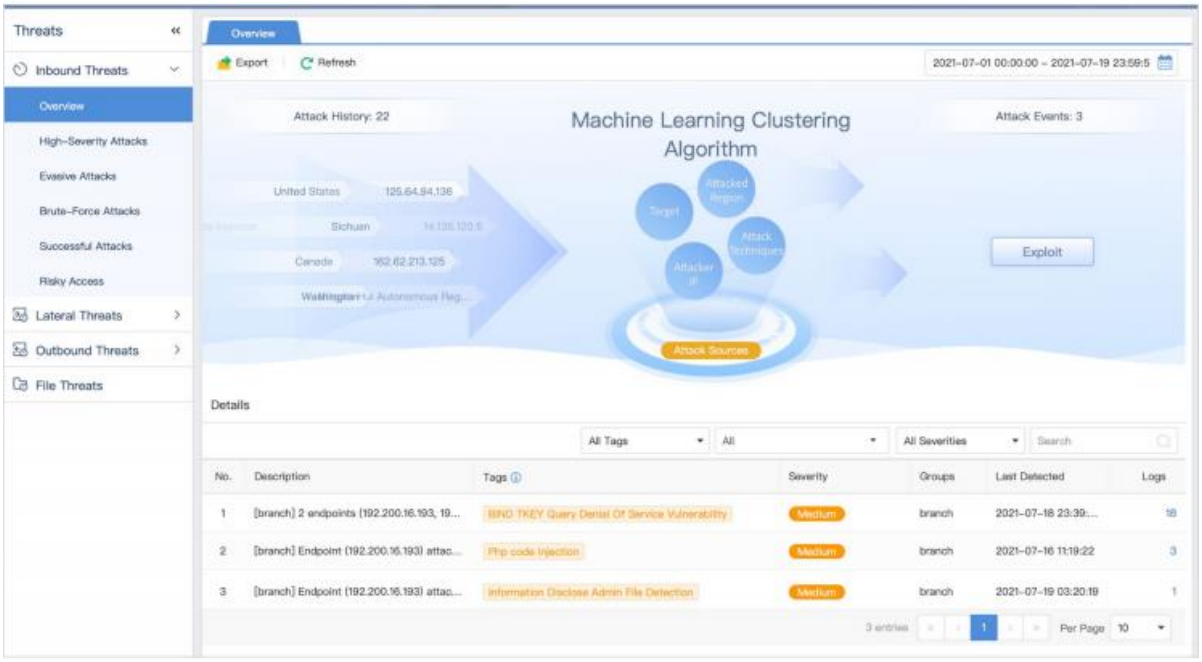

Abbildung 9: Ausschnitt aus dem Detection Screen der NovaCommand Plattform

Table 1. List of NovaCommand Threat Types and the Value to an NDR Platform

	Threat Sub-Types	NDR Value
Inbound	• High-severity • Evasive • Brute-force • Successful • Risky	Attacks that originate from *outside* the network, targeting assets within the organization
Lateral	• Lateral attacks • Unauthorized access • Suspicious activities • Risky access	Attacks that are *entirely internal*, representing lateral movement between enterprise-owned assets
Outbound	• Outbound attacks • APT C&C (C2) • Suspicious activities • Stealth communications • Unauthorized access • Risky access	Attacks that originate from *inside* the network, attempting to reach outbound and/or attack external assets
File-based	N/A	A companion data point, files that are observed within network traffic (regardless of direction) are also extracted and available for further analysis (malware execution, document inspection)

Tabelle 1: Liste der NovaCommand-Bedrohungsarten und der Wert für eine NDR-Plattform

Daten und Erkenntnisse, die dem Sicherheitsteam einen proaktiven Vorteil gegenüber Angreifern verschaffen, sind ebenso wichtig wie die Erkennung und die Behandlung von Zwischenfällen. Glücklicherweise bietet NovaCommand als NDR-Plattform Sicherheitsteams eine leistungsstarke Funktion, um Bedrohungen aus der Netzwerkperspektive heraus zu betrachten. Die Erkennungsfunktion (siehe Abbildung 9) besteht aus einem einzigartigen, animierten (hier nicht gezeigtem) Dashboard, das die Angriffsdetails in übersichtlichen Punkten zusammenfasst.

Wie Abbildung 9 zeigt, liefert NovaCommand nicht einfach nur eine Liste von Entdeckungen. Stattdessen bietet es zusammengefasste Details, die bei Bedarf aufgeschlüsselt werden können. Die Warnungen werden "aufgerollt", und die Analysten können eine Beschreibung, Tags, Schweregrad und Asset-Gruppen im Voraus sehen. Wie auf der linken Seite des Dashboards dargestellt, unterteilt NovaCommand die Bedrohungen auch in Schlüsselkategorien, von denen jede einen spezifischen Wert für eine NDR-Plattform bietet, nach denen man in anderen Sicherheitskontrollen vergeblich sucht. Tabelle 1 enthält eine Auflistung der Bedrohungskategorie und den Wert für eine NDR-Plattform.

Eine sehr nützliche Funktion ist NovaCommand's Kategorisierung von Bedrohungen (siehe Tabelle 1). Bedenken Sie, dass Ihr Team mit einer NDR-Plattform einen netzwerkzentrierten Ansatz gegenüber Bedrohungen verfolgt. Mithilfe direkter High-Level Klassifizierungen können nicht nur Schlüsselkomponenten eines Angriffs analysiert werden, sondern ebenso Prioritäten gesetzt werden, welche Alarme eine sofortige Reaktion erfordern. Die Untertypen der Bedrohung sind ebenfalls dynamisch, was beweist, dass NovaCommand als Plattform richtungsbewusst agiert. Mit diesen Bedrohungstypen und Untertypen stellt NovaCommand Analysten einen einzigartigen Ansatz für die Handhabung zur Verfügung. Metadaten wie die Richtung oder der "Typ" des Angriffs sind oft in eine Warnung eingebettet oder sind ein Bestandteil von konkurrierenden Plattformen. ForeNova rückt diese in den Vordergrund und ermöglicht es, sich auf die C2-Kommunikation oder auf seitliche Bewegungen zu konzentrieren. Dieses Vorgehen spart einerseits Zeit und stellt gleichzeitig sicher, dass Sicherheitsteams die Ressourcen in den richtigen Bereichen einsetzen. Mithilfe von den umfangreichen Metadaten sind bestimmte Angriffe nachzuvollziehen. In Abbildung 10 erhalten Sie einen Einblick in eine Warnung bezüglich einer potenziellen Ausnutzung einer Systemschwachstelle. NovaCommand stellt Analysten auf jedem Bildschirm zusammengefassten Datenpunkten zur Verfügung. Diese bestehen zum Beispiel aus einer grafischen Darstellung der IP-Adressen der Angreifer, aus den Angriffsarten und den angegriffenen Systemen. NovaCommand erleichtert die Arbeit von Analysten, indem es

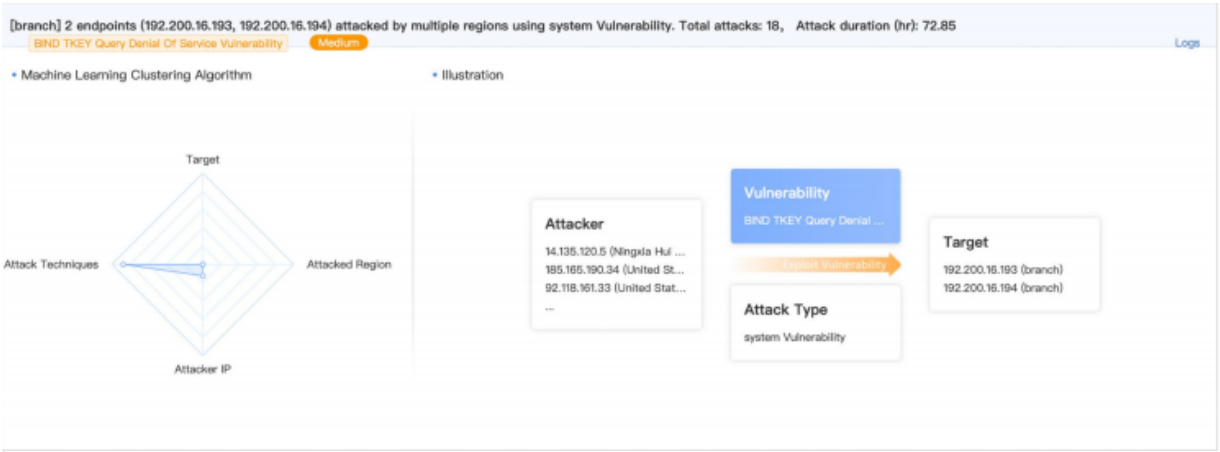

Abbildung 10: Ausschnitt aus einem Angriffsdetail

ihnen benötigte Informationen im Voraus liefert.

Wie auf der linken Seite von Abbildung 10 zu sehen ist, stellt NovaCommand auch seine Clustering-Aktivitäten des maschinellen Lernens für den Benutzer übersichtlich dar. Viele Tools, die das maschinelle Lernen nutzen, arbeiten hinter den Kulissen, um die Alarmierung zu verbessern und die Zuverlässigkeit zu erhöhen. NovaCommand bietet diese Analyse im Gegensatz zu vergleichbaren Plattformen auf der Hauptseite an – damit die beobachtete Aktivität so schnell wie möglich interpretiert und analysiert werden kann.

Eine Schlüsselkomponente von NovaCommand ist die Analyse der Richtung von Angriffen. Eine schnelle Einschätzung der Richtung eines Angriffs - z. B. einwärts oder ostwestlich - kann dabei helfen, Prioritäten zu setzen und zu bestimmen, auf welche Richtungen sich Teams zuerst konzentrieren sollten.

Natürlich können jeder Datenpunkt und jede Angriffsbeobachtung innerhalb der Angriffsbeschreibung erweitert werden. In der Alarmübersicht werden die wichtigsten Alarmdetails zusammengefasst (siehe Abbildung 11). Falls erforderlich, können sie jedoch auch auf die "rohen" Protokolldaten in der Plattform zugreifen, um einen tieferen Einblick zu erhalten. Protokolle können in Tabellen- oder JSON-Formaten angezeigt werden und bei Bedarf für die gemeinsame Nutzung oder zusätzliche Analysen außerhalb der Plattform einfach exportiert werden. Der leistungsstarke Detection-Teil der NovaCommand-Plattform bietet tiefe Einblick in die Organisation.

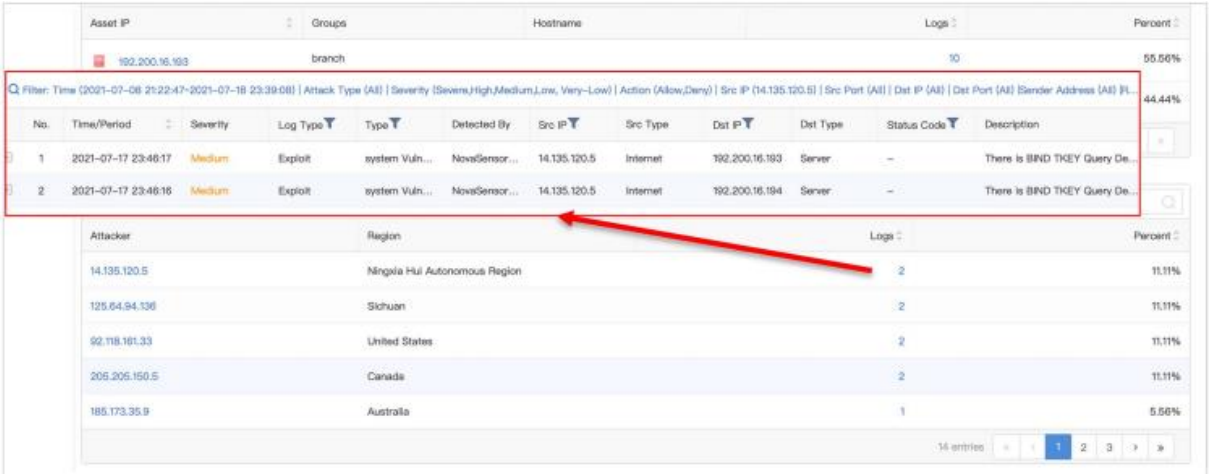

Abbildung 11: Ausschnitt einer detaillierten Alert-Aktivität mit entsprechenden hervorgehobenen Protokollen

Das wichtigste Anliegen ist eine nutzerfreundliche Anwendung. Diese Plattform bietet zusammengefasste Einblicke und Daten, um schnelle und fundierte Entscheidungen treffen zu können. Ist der Verkehr seitlich, eingehend oder abgehend? Wie viele externe IP-Adressen sind an dem Angriff beteiligt? Welche relevante Schwachstelle wird ausgenutzt? All diese kritischen Fragen werden im Vorfeld geklärt. Analysten müssen sich nur dann mit sicherheitsrelevanten Ereignissen befassen, wenn sie es für notwendig halten. Durch die Beantwortung von Schlüsselfragen bietet NovaCommand einen weiteren versteckten Vorteil: Sie müssen keine Zeit mehr mit aufwändigen Erhebungen von Daten verschwenden, da ihnen relevanten Daten auf dem Silbertablett serviert werden. Nehmen wir zum Beispiel eine Warnung über böswillige Seitwärtsbewegungen zwischen zwei verschiedenen Teilnetzen. Sie können Verfahren zur Reaktion um diese Metadatenpunkte entwickeln, anstatt diese mit aufwendig entwickelten Prozessen zu finden. Eine schnellere Entscheidungsfindung bedeutet auch eine schnellere Reaktion und weniger Zeit für Angreifer, um das Netz zu durchstreifen.

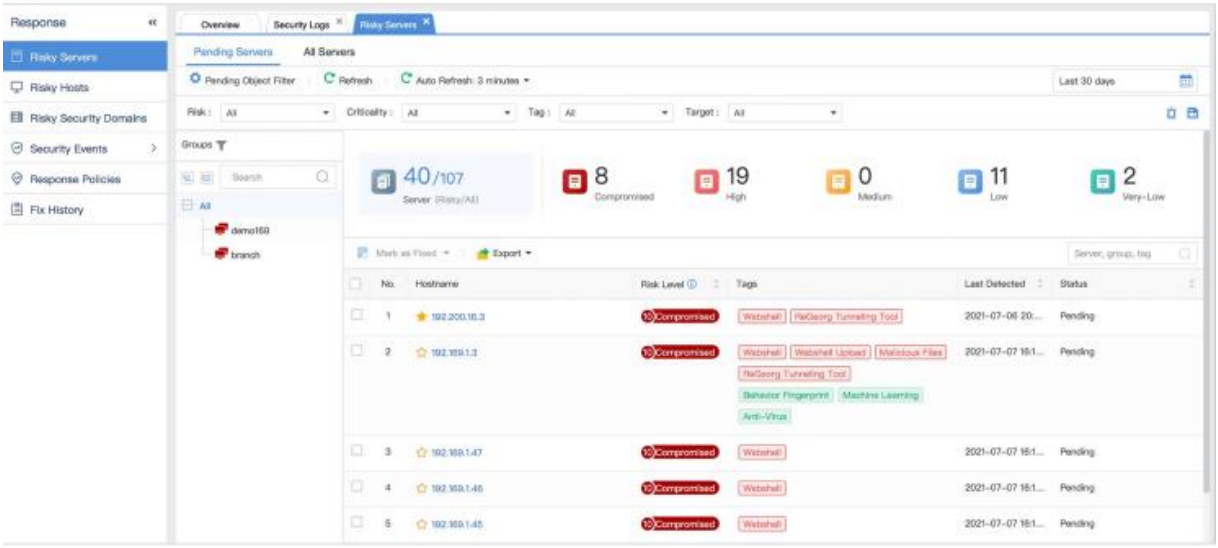

Abbildung 12: Ausschnitt aus der NovaCommand Response Page: Fokussiert auf riskante Server

Reaktion auf Vorfälle

NovaCommand bietet wertvolle Einblicke in die Klassifizierung und Erkennung von Angreifern. Die Reaktionsmöglichkeiten umfassen dabei alle Assets in einem Netzwerk. Der Reaktionsbildschirm von NovaCommand ist ebenso informativ wie andere Dashboards und Startbildschirme. Abbildung 12 zeigt einen Screenshot der ersten Reaktionsseite. Genau wie andere Bildschirme bietet NovaCommand einen eigenen Einblick und eine eigene Klassifizierung. Hosts werden wiederum entsprechend als riskante Server oder Hosts, Domänen und Sicherheitsereignisse kategorisiert. Die Plattform bietet einzigartige Erkenntnisse, durch die der Zustand und die Notwendigkeit von Maßnahmen in der Umgebung beurteilt werden können. In Abbildung 12 sehen Sie zum Beispiel 40 risikobehaftete Server, von denen acht einen gefährdeten Status aufweisen. Unterhalb dieser übergeordneten Metriken sammelt NovaCommand ähnliche Daten, wie sie auf dem Detection Screen angezeigt werden, einschließlich Hostname, Risikostufe, Ereignis-Tags und Zeitstempel. Wie beim Detection Screen sind die meisten Datenpunkte interaktiv, und Analysten können sie nutzen, um sie nach Bedarf aufzuschlüsseln. Die Aufschlüsselung eines bestimmten Ereignisses liefert den Analysten möglicherweise einige der besten Metadaten über ein bestimmtes Ereignis. In Abbildung 13 wird ein kompromittiertes System untersucht, das mit einem Web Shell und einem Tunneling-Tool versehen ist. Abbildung 13 ist unser Lieblingsbildschirm der gesamten Plattform.

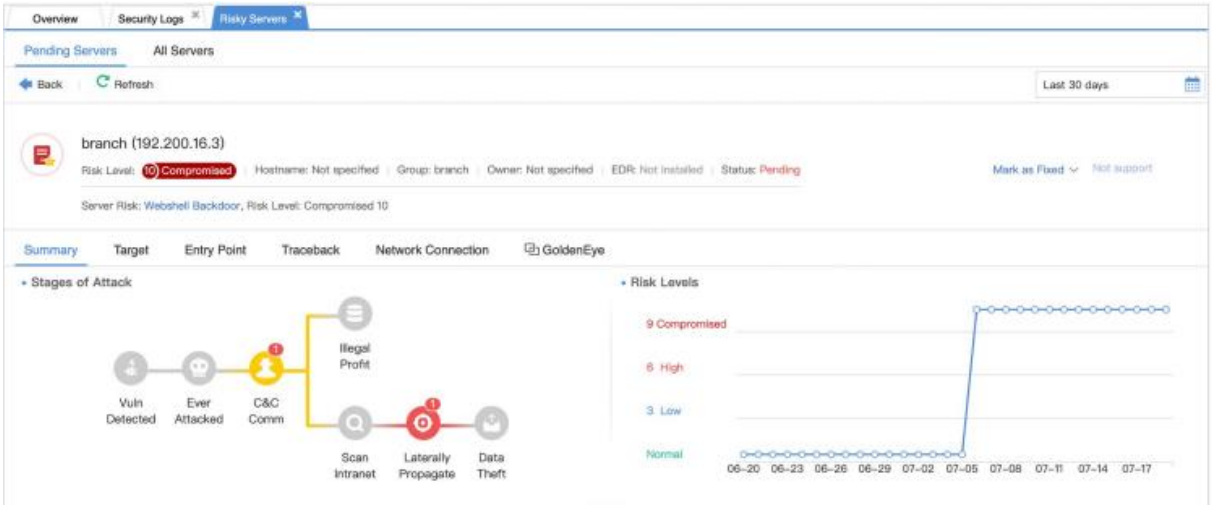

Abbildung 13: Auszug aus einer Kompromittierung: Riskante Server dargestellt im Response Tab

NovaCommand liefert eine immense Menge an Daten über einen Vorfall, einschließlich einer detaillierten Karte der Angriffsphasen, einer Historie der beobachteten Systemkritikalität und die wichtigsten Stufen, die der Angreifer erreicht hat. Wie diese Abbildung zeigt, erkannte NovaCommand, dass der Gegner über eine C2 Kommunikation und seitliche Bewegung in das System eindringen wollte. Auch die Kritikalität des Systems stieg plötzlich an, was darauf hindeutet, dass diese bösartige Aktivität erst vor Kurzem stattgefunden hat. NovaCommand hat daraufhin das System eskaliert. Im Tab Response können Sie ein bestimmtes Ereignis über die Option Ereignis Details (ähnlich wie bei den Protokolleinträgen in Detection) nachverfolgen. Abbildung 14 auf der nächsten Seite zeigt ein Beispiel für die Ereignisdetails einer erkannten Web-Shell.

Abbildung 14: Ausschnitt der Ereignisdetails für ein kompromittiertes System mit einer Web-Shell Erkennung

Die Datenpunkte in Abbildung 14 sind diejenigen, die ein Team bei einer Reaktion auf einen Vorfall sieht, um so schnell wie möglich auf Angriffe reagieren zu können.

Ein letztes wichtiges Feature, das wir in diesem Manual vorstellen wollen, ist NovaCommands einzigartige GoldenEye Traceback-Funktion. Sie besteht aus einem Suchfeld, in das Analysten jeden Netzwerkindikator eingeben können. Außerdem bietet GoldenEye eine ereignisbasierte Link-Analyse für Schlüsselindikatoren eines Angriffes. Abbildung 15 auf der nächsten Seite zeigt einen Ausschnitt aus einem GoldenEye-Traceback.

Wichtige Erkenntnis

Mitarbeiter, die auf sicherheitsrelevante Vorfälle im Netzwerk reagieren, sind es gewohnt, Warnungen zu erhalten und Protokolle, PCAPs und andere Artefakte zu durchforsten, um die ganze Geschichte eines Vorfalls nachvollziehen zu können. Diese Aktivitäten sind sehr zeitaufwendig und sind abhängig davon, welche Daten sichtbar und verfügbar sind. NovaCommand vereinfacht diese Arbeit enorm – es stellt die Historie eines Angriffs zusammen und die Analysten können somit so schnell wie möglich, auf einen Angriff reagieren und gleichzeitig die Zeit eines Angreifers im Netzwerk verkürzen.

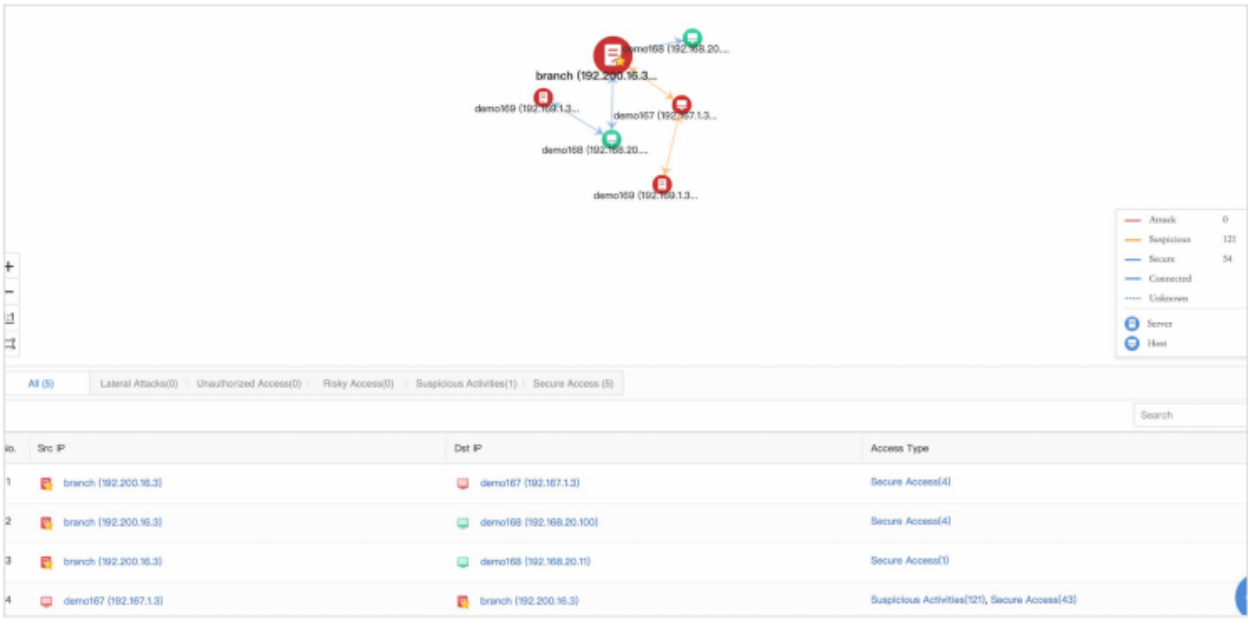

Abbildung 15: Ausschnitt aus einem GoldenEye Traceback einer bösartigen IP-Adresse

Wie Abbildung 15 zeigt, bietet die GoldenEye Funktion einen weiteren interessanten Blickwinkel für Analysten. Die Plattform erkennt automatisch Verbindungen zu anderen Systemen, Angriffen oder Vorfällen in der Umgebung. Dies ist eine sehr nützliche, zukunftsweisende Funktion. Angriffe umfassen oft mehrere Systeme, und der Versuch manuell zu korrelieren, ist ein weiteres „Kaninchenloch“ (rabbit hole), das Analysten nur allzu gut kennen und fürchten. NovaCommand bietet eine einfache, grafische Zusammenfassung, auf die Analysten klicken und direkten Links folgen können – inklusive aller Metadaten und Datenpunkte, die in früheren Beispielen bereits vorgestellt wurden.

Automatisierte Reaktionen

Unter bestimmten Bedingungen macht es Sinn, bestimmte Reaktionsprozesse zu automatisieren. Die Automatisierung setzt ein gewisses Maß an Vertrauen in die eigenen Sicherheitskontrollen voraus. Die Plattform ermöglicht Sicherheitsteams eine manuelle Analyse mit automatisierten Reaktionsrichtlinien. In den Antwortoptionen von ForeNova (siehe Abbildung 16) finden wir unglaublich leistungsfähige Antwortrichtlinien. Reaktionsrichtlinien kombinieren die Bedrohungsdaten von ForeNova und integrieren sowohl Produkte von Drittanbietern als auch Erkennungs- und Reaktionsfunktionen. Sie ermöglichen Reaktionen auf Ereignisse zu automatisieren, und zwar mit der granularen Kontrolle und Transparenz der Assets, die wir in den vorherigen Abschnitten bereits vorgestellt haben. Die Erstellung einer Reaktionspolitik ist so einfach wie die Frage: "Was soll die Plattform im Falle eines Angriffs tun?“ Lassen Sie uns die Erstellung einer Richtlinie durchgehen. Abbildung 17 zeigt einen Ausschnitt der Bedingungen, die bei der Erstellung einer Antwortrichtlinie ausgewählt werden können. Analysten können bestimmte Gruppen auswählen und ein Ereignis auf der Grundlage von Angriffstypen spezifizieren. Das bietet einen erheblichen Vorteil für Verteidiger. Sie müssen keinen Code oder eine Regel schreiben, um zu bestimmen, was ein "Bruteforce-Angriff" sein könnte. Stattdessen können sich Analysten auf die Erstellung wirksamer Richtlinien konzentrieren.

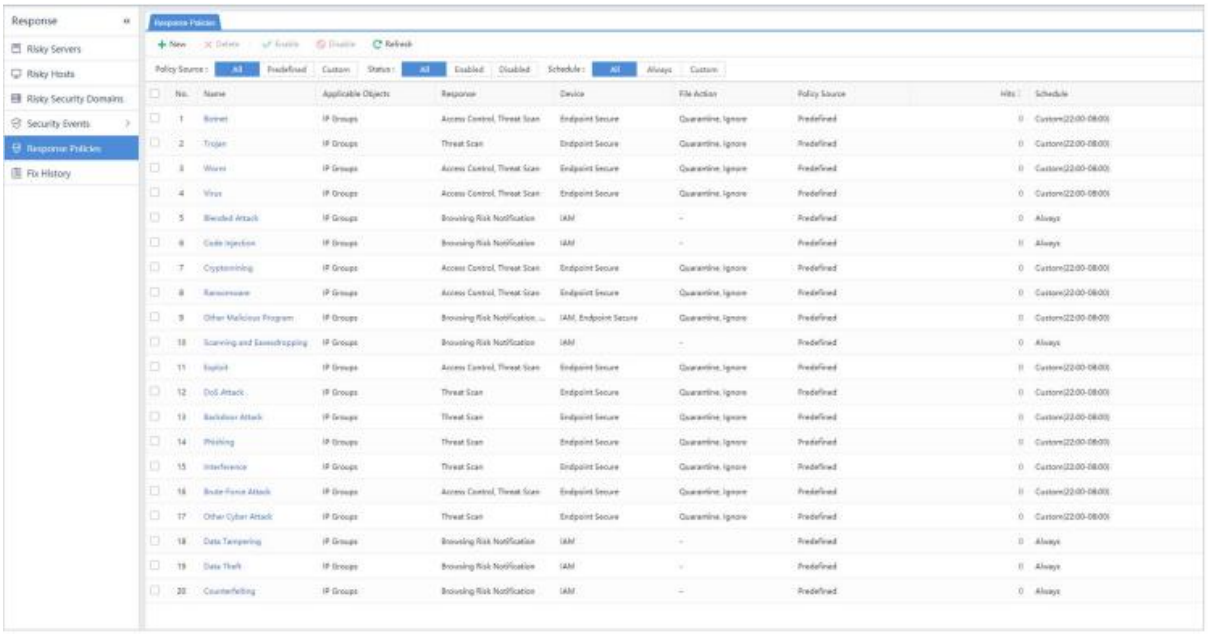

Abbildung 16: Auszug aus ForeNovas Antwortrichtlinien aus dem Response Tab

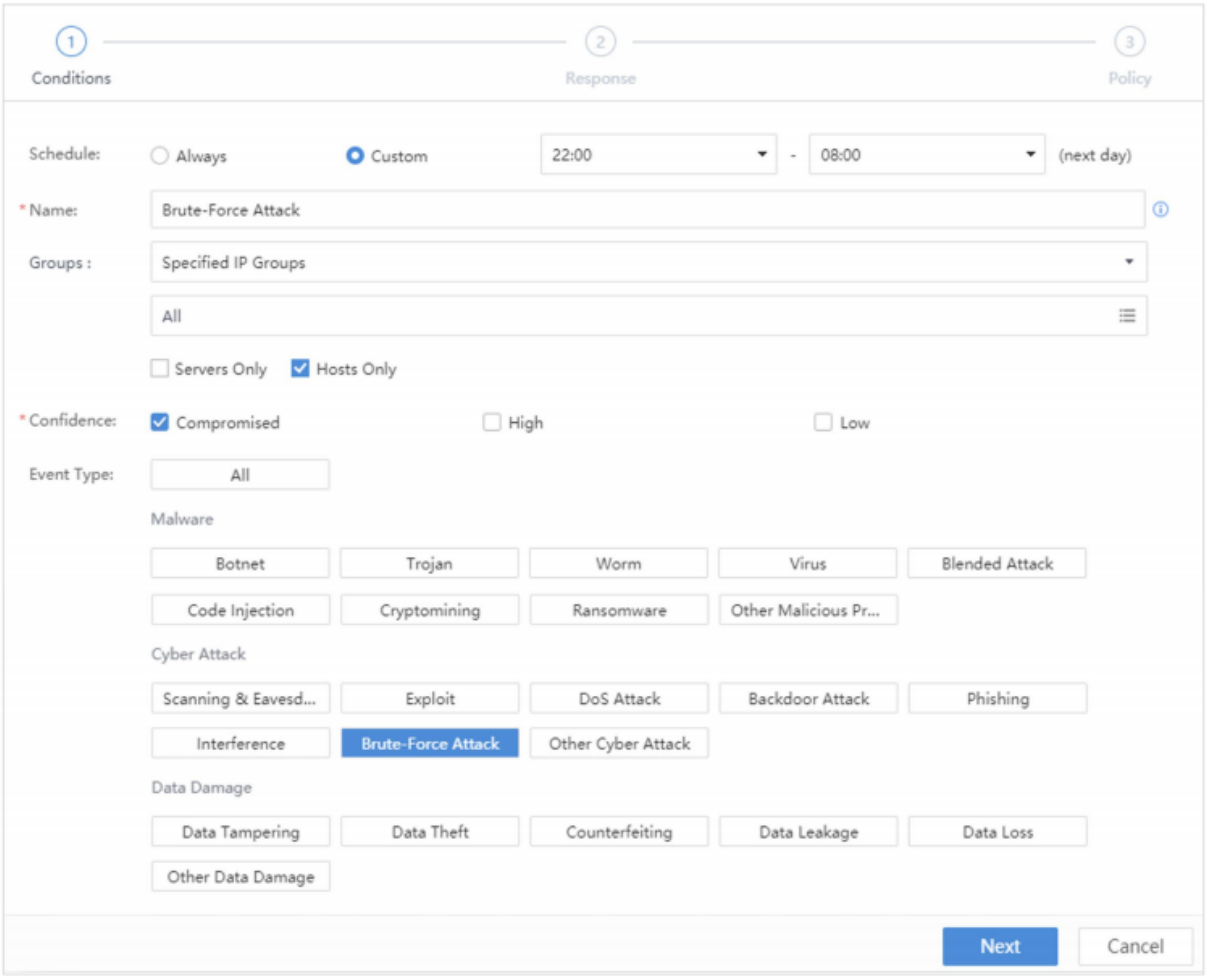

Abbildung 17: Auszug aus dem Condition Tab (Reaktionsrichtlinien)

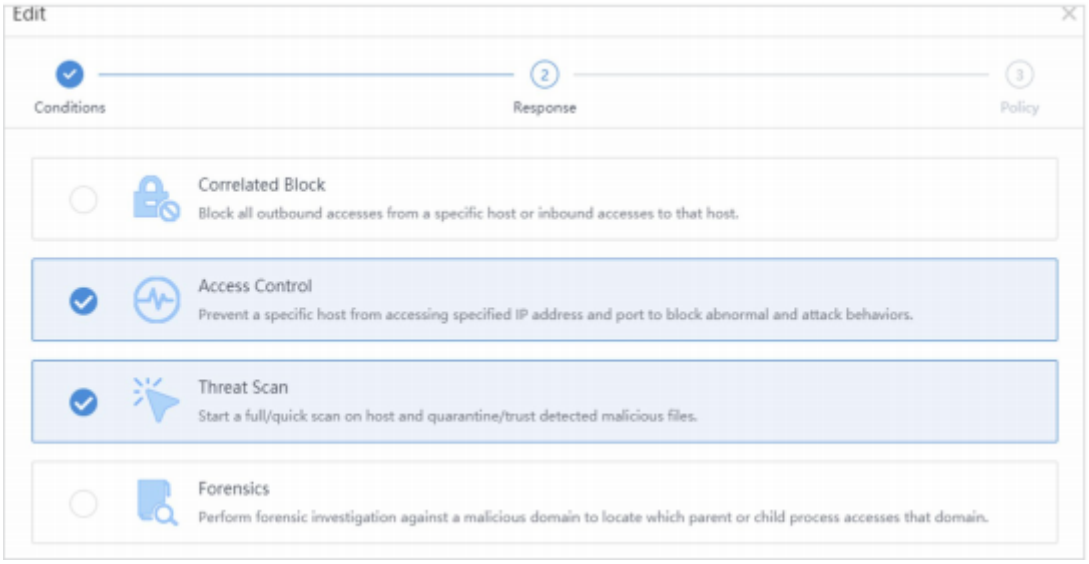

Abbildung 18: Ausschnitt aus dem Response Tab einer Antwortrichtlinie

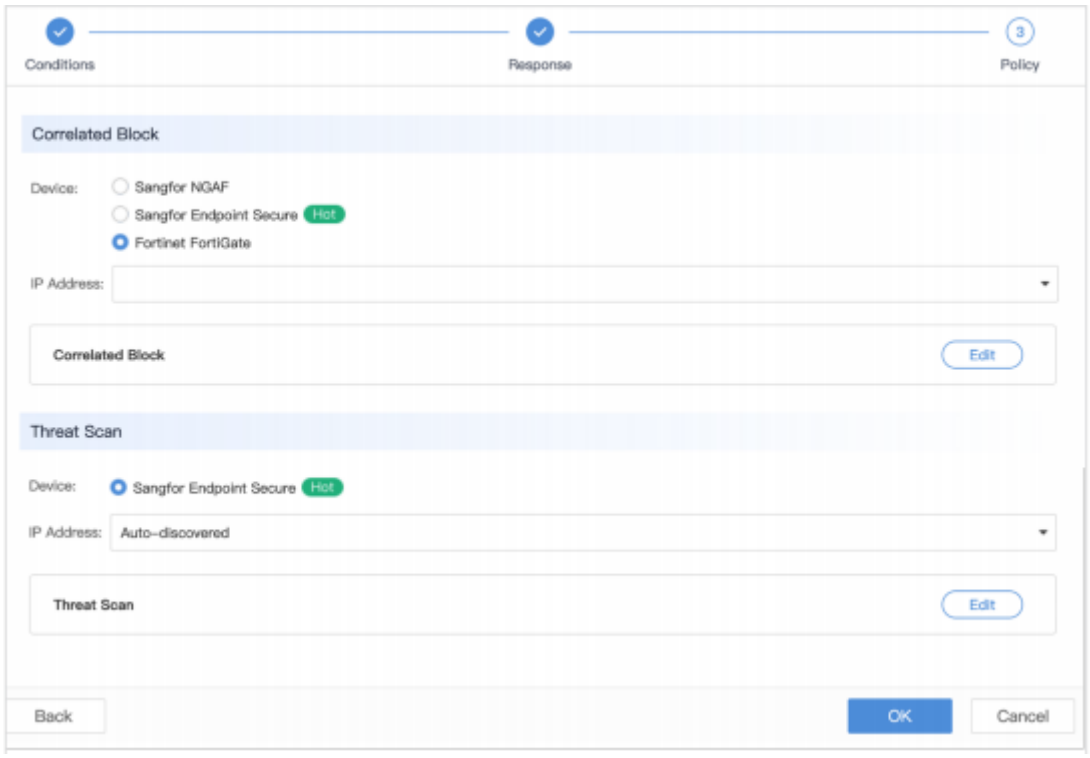

Abbildung 19: Ausschnitt aus dem Policy Tab einer Antwortrichtlinie

In Abbildung 18 wird der nächste Schritt, die automatisierten Funktionen der Plattform dargestellt. Während Analysten möglicherweise daran gewöhnt sind, einfach eine Firewall-Sperre und einen Firewall-Block zu automatisieren, können sie mit ForeNova erweiterte Automatisierungen, wie die Einschränkung von Zugriffskontrollen, einen Bedrohungsscan auf dem System durchführen und sogar automatisch forensische Artefakte abrufen! In Abbildung 19 sehen wir schließlich die verfügbaren Integrationen, um die gewählten Maßnahmen umzusetzen. Durch die Policy Options können automatische Reaktionen weiter ausgebaut werden, indem Tools von Drittanbietern genutzt werden, um

Host-Scans oder die Zugangskontrollen zu implementieren (um nur zwei von vielen Beispielen zu nennen). Hier unterscheidet sich die Plattform von anderen: ForeNova bietet Ihnen die Möglichkeit, mehrere Sicherheitskontrollen zu kombinieren. Der Wert liegt darin, dass eine Organisation, die derzeit über keine NDR-Fähigkeiten verfügt, NovaCommand einfach auf ihrem aktuellen Stack implementieren kann und mithilfe von Netzwerkwarnungen Host-basierte Richtlinien steuern kann.

Abschließende Überlegungen

Netzwerkerkennung und -reaktion sind keine leichten Aufgaben. Es kann ein enormes Unterfangen sein den gesamten Netzwerkverkehr eines Unternehmens zu erfassen und anzureichern. Während wir die NovaCommand Plattform vorgestellt haben, zieht sich ein Thema wie ein roter Faden durch den gesamten Leitfaden: **NovaCommand vereinfacht die Arbeit der Analysten**. Als NDR-Plattform leistet sie hervorragende Arbeit beim Sammeln, Korrelieren und Anreichern, um bösartige Aktivitäten innerhalb eines Netzwerkes zu identifizieren. Durch die automatische Klassifizierung und Anreicherung von Anlagen und Vorfällen, werden jederzeit Prioritäten gesetzt. "Was man nicht sehen kann, kann man auch nicht schützen" ist ein Satz, der im Alltag der IT-Security Teams leider viel zu oft zutrifft. Angreifer haben weiterhin Tag für Tag Erfolg, wobei dieses Jahr ein Rekord an Ransomware-Erpressungsforderungen und Angriffe, die kritische Branchen in mehreren Ländern lahmgelegt haben, darstellt. Wenn es jemals eine Zeit gab, in der man handeln sollte, dann ist es jetzt. Wenn Sie derzeit keine Netzwerkerkennung und -reaktion einsetzen, ignorieren Sie einen entscheidenden Teil zum Schutz ihres Unternehmens.

Über den Autor

Matt Bromiley ist Dozent für digitale Forensik und Incident Response bei SANS und unterrichtet FOR508: Advanced Incident Response, Threat Hunting und digitale Forensik und FOR572: Fortgeschrittene Netzwerk-Forensik: Threat Hunting, Analyse und Incident Response.

Er berät globale Unternehmen zu den Themen Incident Response und forensische Analysen und kombiniert seine Erfahrungen in den Bereichen digitale Forensik, Protokollanalyse, Reaktion auf Vorfälle und Management. Zu seinen Fähigkeiten gehören die Festplatten-, Datenbank-, Speicher- und Netzwerkforensik, die Bedrohungsanalyse und die Überwachung der Netzwerksicherheit. Matt arbeitete mit Organisationen aller Formen und Größen zusammen, von multinationalen Konzernen bis hin zu kleinen, regionalen Geschäften. Seine Leidenschaft gilt dem Lernen, Lehren und der Arbeit an Open-Source-Tools.

Sponsor

SANS would like to thank this paper's sponsor: