Forescout XDR

eXtended Detection and Response

FORESCOUT

Forescout XDR

eXtended Detection and Response

450-fache Steigerung der SOC-Effizienz dank besserer Erkennung und Entschärfung realer Bedrohungen

Die Teams in Security Operations Centern (SOC) werden tagtäglich mit unvollständigen und unpräzisen Warnmeldungen überflutet, denen wichtige Kontextinformationen fehlen. Viele davon sind Fehlalarme. Infolgedessen übersehen die Analytiker kritische Bedrohungen oder brauchen länger, um sie zu untersuchen und zu entschärfen, was das Risiko von Sicherheitsverletzungen erhöht. Ein typisches SOC erhält 11.000 Warnmeldungen pro Tag oder 450 pro Stunde[1] – und die meisten davon sind wenig zuverlässig oder gar blinder Alarm.

Mit Forescout® XDR reduziert sich diese Zahl auf eine konkrete, handlungsrelevante Erkennung pro Stunde – oder anders ausgedrückt, eine wahrscheinliche Bedrohung, die die SOC-Mitarbeiter wirklich untersuchen müssen.[2]

Die Lösung im Überblick

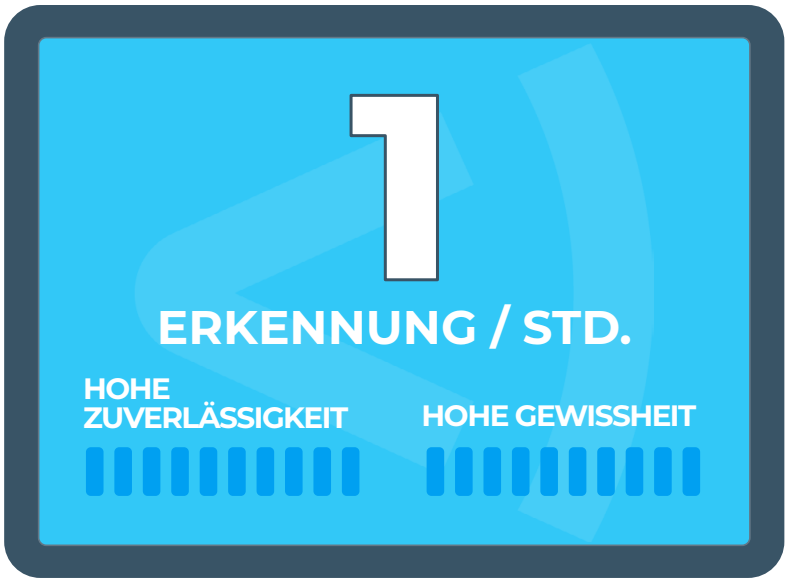
Forescout XDR generiert aus Telemetriedaten und Logs hoch zuverlässige Warnungen vor wahrscheinlichen Bedrohungen, die das SOC konkret verwerten kann.

Die Lösung automatisiert die Erkennung, Suche, Untersuchung und Behebung hochentwickelter Bedrohungen für alle verbundenen Geräte. Dabei umspannt sie IT, OT/ICS, IoT und IoMT und deckt Campus, Rechenzentrum, Cloud und Edge ab. Forescout XDR vereint unentbehrliche SOC-Technologien und -Funktionen in einer einheitlichen, cloudnativen Plattform. Über eine einzige Konsole kann das Team alle Informationen einsehen und umgehend Maßnahmen ergreifen.

Forescout XDR nutzt Daten aus der gesamten erweiterten Unternehmensumgebung und berücksichtigt dabei sowohl verwaltete als auch unverwaltete (agentenlose) Geräte.

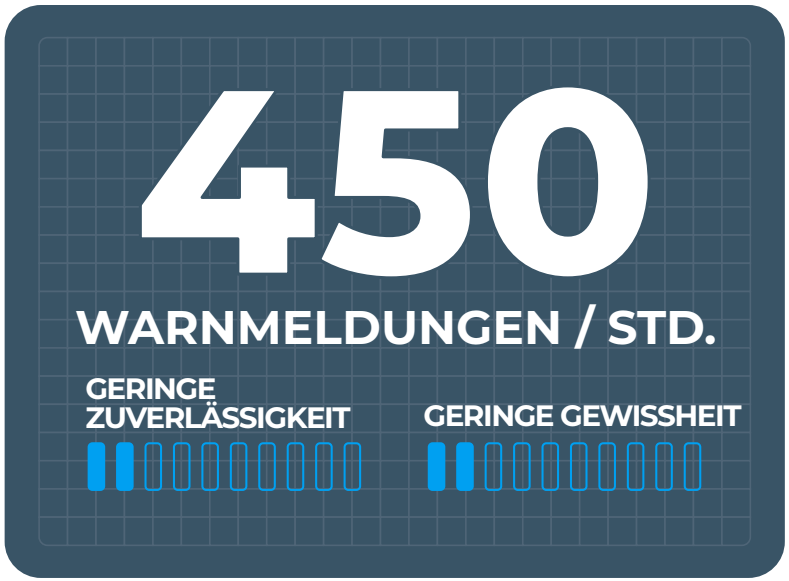
Forescout XDR generiert verwertbare Erkennungen aus Telemetriedaten und Protokollen 450-mal effektiver als ein typisches SOC.

Mit Forescout XDR



VS

Typisches SOC



*** Erkennung: Eine wahrscheinliche Bedrohung, die die SOC-Mitarbeiter manuell untersuchen müssen**

Basierend auf aggregierten, über einen Zeitraum von einem Jahr (Dez. 2021-2022) gemittelten Daten aus 30 unterschiedlich großen Unternehmen aus verschiedenen Branchen.

11.000 Warnmeldungen pro Tag = 450 Warnmeldungen pro Stunde. Quelle: „The 2020 State of Security Operations“, Forrester Consulting

Wie viele Warnmeldungen ein SOC tatsächlich erhält, hängt von vielen Faktoren ab. Dazu zählen beispielsweise die Anzahl, die Art und der Ort der eingesetzten Sicherheitskontrollen, die Feinabstimmung dieser Kontrollen (die wiederum von der Kapazität der Analytiker, der Risikotoleranz und dem Know-how abhängt), die Zahl der Mitarbeiter/Geräte und der Sektor.

Geschäftlicher Nutzen

Reduziert das Geschäftsrisiko

Forescout XDR verringert das Risiko und Ausmaß erfolgreicher Angriffe oder Datenpannen und filtert nahezu das gesamte „Datenrauschen“ heraus. So können die SOC-Teams die unterschiedlichsten hochentwickelten Bedrohungen in der gesamten Unternehmensumgebung schneller und präziser erkennen, untersuchen und entschärfen.

Auf diese Weise trägt Forescout XDR dazu bei, Geschäftsunterbrechungen und Kosten zu vermeiden, die durch einen erfolgreichen Angriff oder eine Sicherheitsverletzung entstehen könnten.

Optimiert die Sicherheitsabläufe

Forescout XDR reichert wichtige Daten automatisch an, normalisiert sie und korreliert Indikatoren, um eine kleine Anzahl hoch zuverlässiger Erkennungen zu generieren, die tatsächlich von einem Analytiker untersucht werden müssen. Die Lösung vereinfacht und beschleunigt komplexe Untersuchungs- und Threat Hunting-Prozesse durch vollständigere, präzisere Informationen und kontextbezogene Daten – all das über eine einheitliche Konsole, die mit anderen Lösungen von Forescout sowie mit SIEMs, Fallmanagement-Systemen und Response-Lösungen von Drittanbietern integriert werden kann.

Forescout XDR bietet vorkonfigurierte, anpassbare Dashboards und Berichte mit Leistungskennzahlen (KPIs), zugeschnitten auf Analytiker/Incident Responder, Techniker, SOC-Manager, Compliance-/Risikomanager und Führungskräfte. Dies verbessert den Überblick über den gesamten Lebenszyklus von Bedrohungen und lässt den SOC-Teams mehr Zeit für höherwertige Sicherheitsaufgaben.

Senkt die Kosten

Die Lösung senkt die SOC-Ausgaben hinsichtlich:

- Lizenzierung und Verwaltung mehrerer isolierter SOC-Lösungen, zum Beispiel Data Lakes; Lösungen für Sicherheitsanalysen; Security Orchestration, Automation and Response (SOAR); User and Entity Behaviour Analytics (UEBA); und Threat Intelligence-Plattformen
- Log-Speicherung
- Burnout bei Analytikern, Fluktuation, Einstellung und Schulung von Mitarbeitern
- Unterstützung für neue Datenquellen
- Erstellung und Anpassung von Regeln

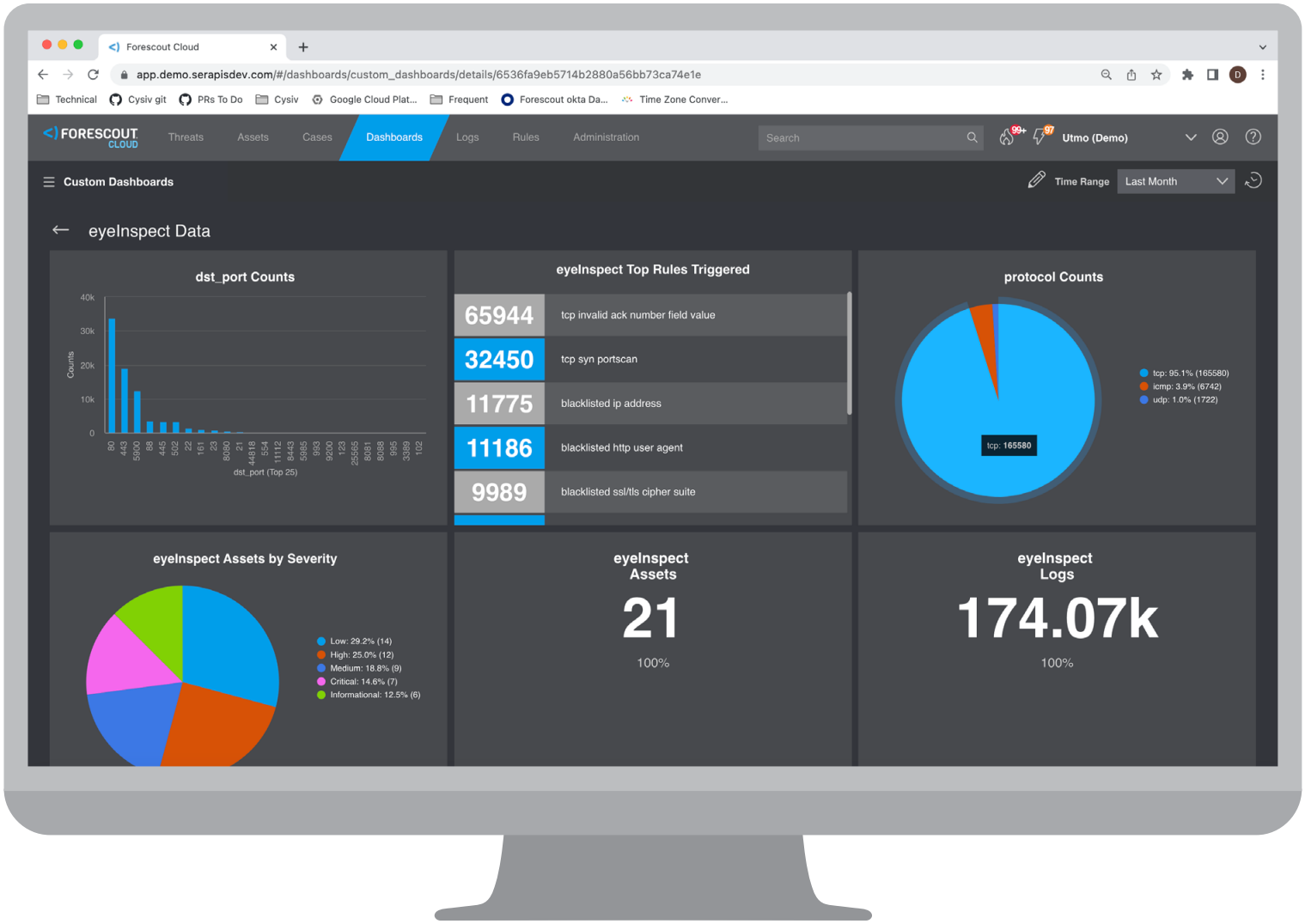
Vereinfacht die Compliance

Mehrere Hot- und Cold-Storage-Optionen, automatische Bedrohungserkennung und Threat Intelligence unterstützen die Einhaltung wichtiger Vorschriften und Standards. Zugleich helfen sie, die potenzielle Lücke zwischen dem Zeitpunkt, an dem eine Sicherheitsverletzung oder Störung bemerkt wird, und dem Zeitpunkt der Reaktion zu schließen.

Nutzt bereits vorhandene Sicherheitsprodukte

Forescout XDR steigert den Nutzen Ihrer weiteren Lösungen von Forescout sowie Ihrer Netzwerk-, Endpunkt- und Cloud-Security-Sensoren und Durchsetzungspunkte, gleich von welchem Hersteller. Mit Forescout XDR müssen Sie keine neue, herstellerspezifische Software oder Hardware implementieren.

Wichtige Metriken und Verlaufsdaten zur besseren Steuerung der SOC-Leistung



Vorkonfigurierte und anpassbare, Persona-basierte Dashboards und Berichte liefern relevante KPIs für verschiedene Zielgruppen, darunter Analytiker/IR, Techniker, SOC-Manager, Compliance- und Risikomanager sowie Führungskräfte.


Anreicherung
Infrastruktur
Forescout
Anwendungen
Sicherheit
Cloud/SaaS
DATEN-AUFNAHME
LOGS
Hersteller- und EDR-neutrale Unterstützung für 170+ Datenquellen
LOG-VERARBEITUNG
ANGEREICHERTE LOGS
Normalisierung zu einem CIM und automatische Anreicherung
INDIKATOREN
Stufe 1: Indikatoren, generiert durch eine Kombination aus fünf Techniken
BEDROHUNGS-ERKENNUNG
ERKENNUNGEN
Stufe 2: Erkennungen, generiert aus Sequenzen, Mustern oder zahlreichen Indikatoren
MANUELLE UNTERSUCHUNG
!
Zuweisung der Vorfälle zu einem Fall, um weiter untersucht und behandelt zu werden
VORFÄLLE
REAKTION
SIEM
FORESCOUT LÖSUNGEN
MSSP
Automatisierte Orchestration und Reaktion mit Lösungen von Forescout (eyeControl und eyeSight) sowie via SIEM und MSSPs

Warum Forescout

Gemeinsam mit anderen Lösungen von Forescout bietet Forescout XDR eine einzigartige Kombination aus hersteller- und EDR-neutraler Datenaufnahme, 450-fach verbesserter Erkennung, umfassendem Reaktionsspektrum und proaktiver Risikominimierung – all das zu einem kalkulierbaren, erschwinglichen Preis..

Hersteller- und EDR-neutrale Datenaufnahme

- Unterstützt die Produkte und Lösungen, in die Sie bereits investiert haben
- Kann Daten von jedem verwalteten und unver-walteten Gerät aufnehmen (IT, OT/ICS, IoT, IoMT)
- Gewährleistet eine umfassendere, leistungsfähigere, flexiblere und effektivere Erkennung von Bedrohungen

450-fach verbesserte Erkennung

- Eine hochmoderne Daten-Pipeline setzt ein gemeinsames Informationsmodell (CIM) durch, um die erfassten Daten zu normalisieren und automatisch mit Benutzerinformationen, IP-Zuordnung, Geolokalisierungsdaten und Informationen zu kritischen Assets anzureichern
- Eine 2-stufige Engine zur Bedrohungserkennung setzt eine Kombination aus 5 Techniken ein, um das Datenrauschen zu reduzieren und die Zuverlässigkeit zu erhöhen

Umfassende Reaktionen

- Leistungsstarke Untersuchungswerkzeuge
- Native Integrationen mit Fallmanagement-Lösungen
- Automatisierte Reaktionen mit Lösungen von Forescout, die alle verwalteten und unverwalteten Geräte erreichen

Proaktive Risikominimierung

- Die Integration mit anderen Lösungen von Forescout verkleinert die Angriffsfläche und reduziert die Gefahr, dass sich ein kompromittiertes oder nicht vorschriftenkonformes Gerät überhaupt mit Ihrem Netzwerk verbindet
- Kontinuierliche Überwachung aller vernetzten Assets mithilfe dynamischer Zugriffsrichtlinien

Einfache, kalkulierbare und erschwingliche Preisgestaltung

- Keine Zusatzgebühren, wenn mehr Logs an Forescout XDR übertragen werden – fördert eine bessere Erkennung
- Die Lizenzgebühr basiert auf der Gesamtzahl der Endgeräte (IP-/MAC-Adresse) in Ihrem Unternehmen
- Verschiedene Hot- und Cold-Storage-Optionen sind im Preis inbegriffen, um Ihren geschäftlichen Anforderungen gerecht zu werden

Kernmerkmale

Forescout XDR vereint unentbehrliche SOC-Technologien und -Funktionen in einer einzigen, einheitlichen, cloudnativen Konsole.

Datenaufnahme

Native Unterstützung von Daten aus Forescout eyeSight, eyeInspect und Medical Device Security – und aus mehr als 170 hersteller- und EDR-neutralen Datenquellen, einschließlich:

- **Sicherheit:** Firewalls, Netzwerk-IDS/IPS, EDR, Plattformen für Endpunktschutz (EPP), Server-/Workload-/Container-Sicherheit, Web-Proxys und E-Mail-Sicherheit
- **Infrastruktur:** Windows-Sicherheit, AD-Authentifizierung, IAM, DHCP, DNS, Cloud Audit-Trails und Netzwerk-Metadaten
- **Anreicherung:** Identitäten (LDAP), Asset-Inventarisierung und -Klassifizierung, Konfigurationsmanagement, Resultate von Schwachstellen-Scans, Threat Intelligence (Indikatoren für Kompromittierungen – IOCs)
- **Anwendungen:** Datenbanken, ERP, CRM und APIs
- **Cloud/SaaS:** AWS, Microsoft Azure, Google Cloud, Microsoft 365, Google Workspace und alle anderen SaaS-Anwendungen

Daten-Onboarding

Hilft Ihnen, maximalen Erkenntnisgewinn für Ihre wichtigsten Anwendungsfälle zu erzielen. Die Dateningenieure von Forescout unterstützen Ihr Team bei der Planung und Priorisierung der Datenquellen, die eingebunden werden sollen. Anschließend helfen sie bei der Konfiguration der Daten-Pipeline und stellen sicher, dass Ihre Daten ordnungsgemäß geparst, bereinigt, normalisiert und angereichert werden.

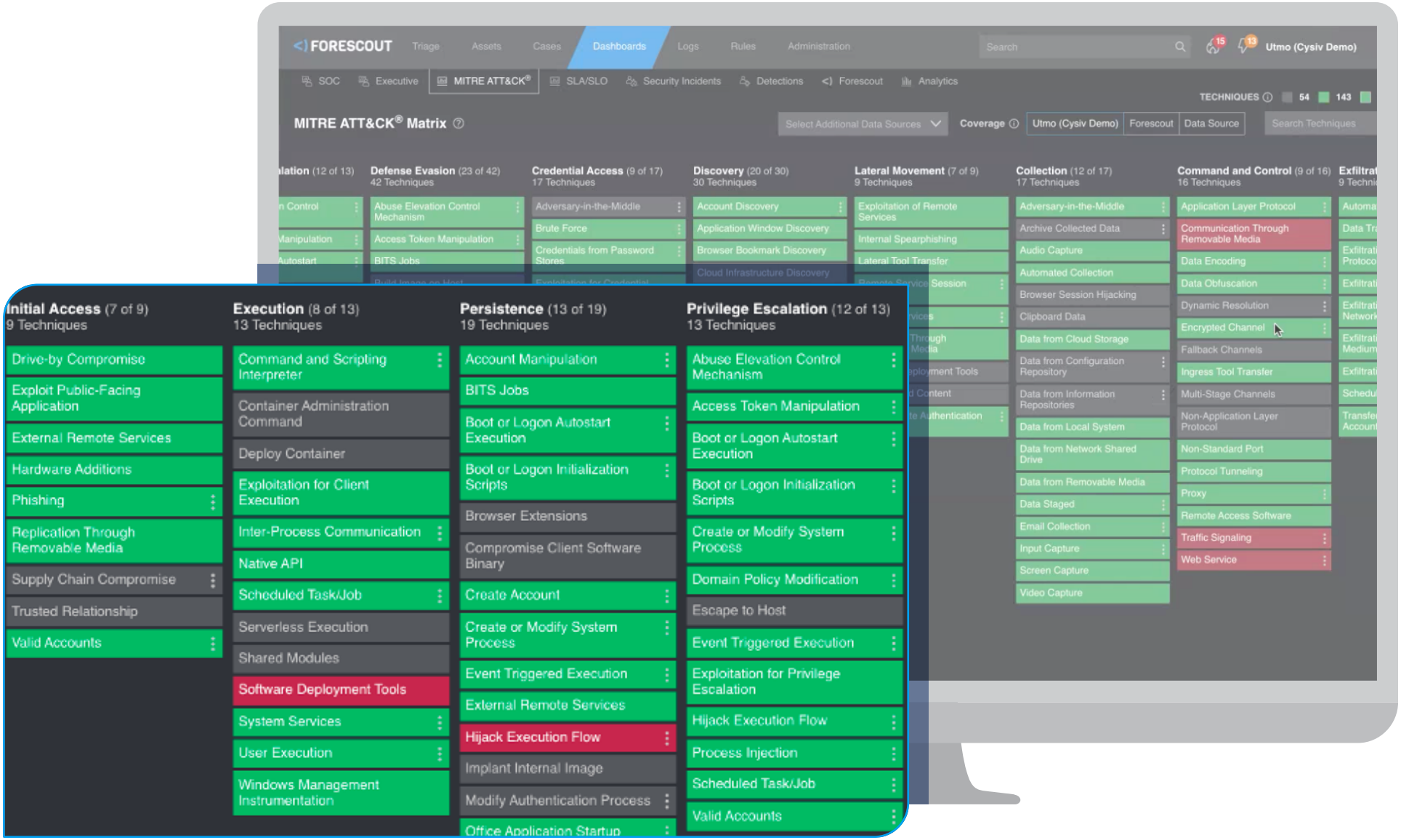
Fortschrittliche Daten-Pipeline

Verwaltet die Daten, die aus Quellen im gesamten Unternehmen in die hochentwickelte Engine zur Bedrohungserkennung eingespeist werden, nach streng datenwissenschaftlichen Grundsätzen. Zunächst erzwingt Forescout XDR ein gemeinsames Informationsmodell (CIM), um die aufgenommenen Daten zu normalisieren. Anschließend reichert die Lösung diese Daten automatisch mit der IP-Adresse, Geolokalisierungsdaten, ADObject-Eigenschaften, Konfigurations- und anderen kontextbezogenen Daten an, um den nötigen Sicherheitskontext bereitzustellen. Dies maximiert den Erkenntnisgewinn und beschleunigt Korrelationen und Threat Hunting über zahlreiche Datenquellen hinweg. Und schließlich wird ein ETL-Prozess (Extraktion-Transformation-Laden) angewandt, der eine schnellere, stabilere und effizientere Datenanalyse ermöglicht als die üblicheren ELT-Prozesse (Extraktion-Laden-Transformation).

Integration des MITRE ATT&CK® -Frameworks

Das MITRE ATT&CK-Framework verfolgt die Taktiken und Techniken von Cyber-Angreifern über den gesamten Angriffslebenszyklus hinweg. Forescout XDR ist mit diesem Framework integriert, sodass Sie sofort sehen können, welche Datenquellen erfasst werden sollten, um eine breite oder spezifische TTP-Abdeckung zu erzielen. Sie können potenzielle blinde Flecken finden, die Angreifer ausnutzen können, und feststellen, welche zusätzlichen Datenquellen die Abdeckung weiter verbessern würden.

Die Integration mit dem MITRE ATT&CK-Framework hilft, potenzielle blinde Flecken zu ermitteln und Möglichkeiten zu finden, um die Bedrohungserkennung durch Hinzunahme weiterer Datenquellen zu verbessern.



Hochentwickelte Bedrohungserkennung

Beispiele für Bedrohungen, die mit Forescout XDR erkannt werden können

- Missbrauch von Anwendungen
- Brute-Force-Angriffe
- Buffer-Overflow-Angriffe
- Scannen von Cloud-Assets
- Fehlkonfigurationen in Cloud-Diensten
- Cloud: Unbefugter Zugriff
- Cloud: Erkennung unsicherer Speicher
- Command & Control-Verbindung
- Compliance-Verstöße
- Cross-Site-Scripting
- Kryptojacking
- Ausschleusen von Daten
- Fehlgeschlagene Dateizugriffe
- Unerlaubter Zugriff auf Ressourcen
- Insider-Bedrohungen
- Seitwärtsbewegungen
- Malware/Malware-Ausbrüche
- Netzwerk-Scans
- Passwort-Cracking
- Phishing-Angriffe
- Port- und Schwachstellen-Scans
- Ransomware
- SQL Injection
- Verdächtiges Verhalten
- Unautorisierter Zugriff auf Systeme
- Unautorisierte Änderung von Firewall-Regeln
- Unautorisierte Neustarts von Diensten
- Unautorisierte Erstellung von Diensten/Prozessen
- Ausnutzung von Schwachstellen
- Fehlkonfiguration von Webanwendungen
- Angriffe auf Webanwendungen (alle Layer-7-Web-Angriffe)
- Ausbruch von Würmern/Viren

Cloudbasierter Data Lake

Hochgradig skalierbarer, speziell entwickelter, indexierter Data Lake mit abgestufter Datenspeicherung (heiß, warm, kalt) und schneller Volltextsuche. Die Lösung ermöglicht eine kosteneffiziente kurzfristige und optional längerfristige (7 Tage bis 1 Jahr+) Speicherung von Protokollen und Verwaltung von Telemetrie-Rohdaten oder angereicherten Daten. So werden Ihre Sicherheits- und Compliance-Anforderungen optimal unterstützt.

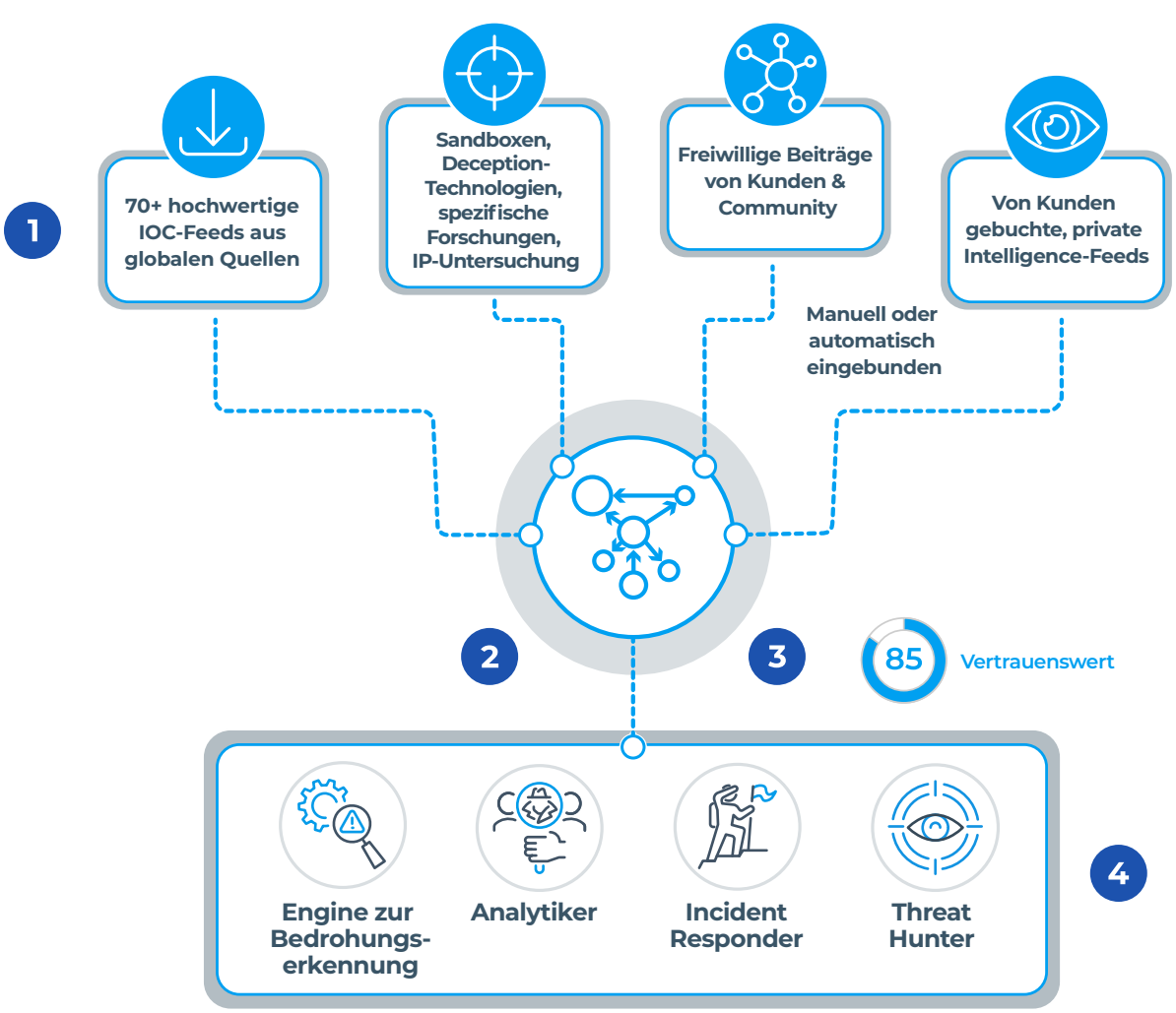
Erkennungsregeln

Die Lösung bietet mehr als 1.500 geprüfte, sofort anwendbare Erkennungsregeln und -modelle für Ihre Datenquellen. Die Regeln wurden an Produktivdaten getestet, um sicherzustellen, dass sie effektiv sind und vom ersten Tag an Mehrwert bieten. Zudem geben Ihnen benutzerdefinierte Erkennungsregeln die Möglichkeit, auf einer geführten Benutzeroberfläche schnell und flexibel Indikator-, Erkennungs- und Zustandsregeln für Ihre spezifischen Anforderungen zu erstellen.

Engine zur Bedrohungserkennung

Die zweistufige Engine zur Erkennung von Bedrohungen wendet fünf Erkennungstechniken an, um automatisch und mit hoher Zuverlässigkeit echte Bedrohungen zu identifizieren, die untersucht werden müssen, und gleichzeitig False Positives („Rauschen“) herauszufiltern:

- **Signaturen:** Abgleich von Objekteigenschaften mit einem bekannten schädlichen Objekt, um in Telemetrie-Rohdaten Bedrohungen zu erkennen, zum Beispiel Malware oder Ransomware, die nicht bereinigt werden kann.
- **UEBA:** Sucht nach abweichenden Verhaltensweisen, die einem als schädlich bekannten digitalen Muster, Footprint, menschlichen oder Netzwerkverhalten entsprechen. Beispiele: Ein Vertriebsmitarbeiter lädt Tausende von Datensätzen aus Ihrem CRM-System herunter; ungewöhnliche Aktivitäten außerhalb der normalen Arbeitszeit; Beaconing; unrealistische Ortswechsel eines Benutzers.
- **Statistik und Ausreißer:** Identifizierung ungewöhnlicher Aktivitäten mithilfe von Techniken wie Clustering, Gruppierung, Stacking, Bestimmung von Baselines und Abweichungen, Ausreißererkennung und logistischer Regression. Beispiele: Ausfall von Protokollquellen, Denial-of-Service-Angriffe.
- **Algorithmen:** Verwendung kontextbezogener KI- und ML-Techniken wie überwachtes/unüberwachtes Lernen oder Deep Learning, um bösartige oder ungewöhnliche Aktivitäten zu erkennen oder Angriffe vorherzusagen. Beispiele: Identifizierung von Prozesspfaden oder Domain Generation-Algorithmen (DGA).
- **Threat Intelligence:** Nutzung von mehr als 70 Cyber Intelligence-Quellen, um beispielsweise nach Backdoors und Command-and-Control-Traffic oder nach Personen zu suchen, die bösartige Phishing-Seiten aufrufen.



Threat intelligence

Indikatoren für Kompromittierungen (IOCs) aus über 70 hochwertigen Quellen weltweit, darunter Vedere Labs, dem globalen Expertenteam von Forescout. Diese IOCs werden klassifiziert, erhärtet und bewertet, um wertvolle Erkenntnisse zu gewinnen, die automatisch in den Prozess der Erkennung, Suche und Untersuchung von Bedrohungen einbezogen werden. Die Teams haben Zugriff auf detaillierte Bedrohungsberichte von Forescout-Forschern, die Profile gefährlicher Angreifer und Bedrohungen erstellen. Über ein integriertes, Community-internes Austauschsystem mit Opt-In-Verfahren können anonymisierte IOC-Daten auch zwischen Community-Mitgliedern, einschließlich branchenspezifischer ISACs, ausgetauscht werden.

1. Forescout zieht IOC-Daten aus einem breiten Spektrum zuverlässiger Quellen heran
2. Die Erkenntnisse zu IOCs werden zu einer durchsuchbaren Graphdatenbank „bekannt bösartiger“ Domains, URLs sowie IPv4- und IPv6-Adressen korreliert
3. 3. Jedem IOC wird dynamisch ein Vertrauenswert zugewiesen, der auf einer Qualitätsbewertung der Quelle basiert
4. Diese nach Vertrauenswürdigkeit eingestuften IOC-Informationen werden dann von der Engine zur Bedrohungserkennung und den SOC-Teams der Kunden genutzt, um die Untersuchung und Erkennung von Bedrohungen zu beschleunigen und zu verbessern.

UEBA

Verhaltensbasierte Analysen dienen dazu, signifikante Verhaltensänderungen oder Aktivitäten zu erkennen, die in einem Unternehmen ungewöhnlich sind. Im Lauf der Zeit werden für Benutzer und Hosts Standardprofile und -verhaltensweisen erstellt. Jede Aktivität, die von diesen Standard-Baselines abweicht, wird dann als verdächtig eingestuft.

Dashboards und Berichte

Vorkonfigurierte, anpassbare, Persona-basierte Dashboards liefern relevante KPIs für verschiedene Rollen, darunter Analytiker/IR, Techniker, SOC-Manager, Compliance- und Risikomanager sowie Führungskräfte. Durch die proaktive Verteilung von Berichten und/oder Metriken werden sowohl die für die Abläufe im SOC zuständigen Mitarbeiter als auch die Mitglieder des Führungsteams mit wichtigen Informationen versorgt.

SOAR

Orchestriert mit integriertem Fallmanagement und Benachrichtigungen den gesamten SOC-Prozess, von der Erkennung über die Untersuchung bis zur Reaktion. Forescout XDR automatisiert die Sicherheitsprozesse durch Anreicherung beispielsweise mit IP-Standortdaten, Benutzer- und Asset-Informationen und Korrelation mit zahlreichen Informationsquellen. Die Lösung nutzt Forescout eyeSight und eyeControl für automatisierte Abläufe zur Steuerung und Reaktion, in die jedes verwaltete und unverwaltete (nicht agentenfähige) Gerät in Ihrem Unternehmen einbezogen werden kann. Dank Integration mit Palo Alto Cortex XSOAR und anderen SOAR-Lösungen können Sie auch Ihr bestehendes SOAR weiter nutzen.

Cloudnativ

Keine Implementierung erforderlich – alle zwei Wochen werden neue Funktionen, Korrekturen und Regeln nahtlos bereitgestellt.

SIEM-Integration

Echte Bedrohungen, die Forescout XDR ermittelt hat, können zur zentralen Orchestrierung und Reaktion auf Vorfälle in ein vorhandenes SIEM eingespeist werden.

Kontinuierliche Aktualisierung von Software und Inhalten

Neue Merkmale, Funktionen und Fehlerbehebungen sowie neue Erkennungsregeln und -modelle werden jeweils im Abstand von wenigen Wochen nahtlos bereitgestellt, ohne dass es zu Störungen kommt oder betriebliche Unterstützung benötigt wird.

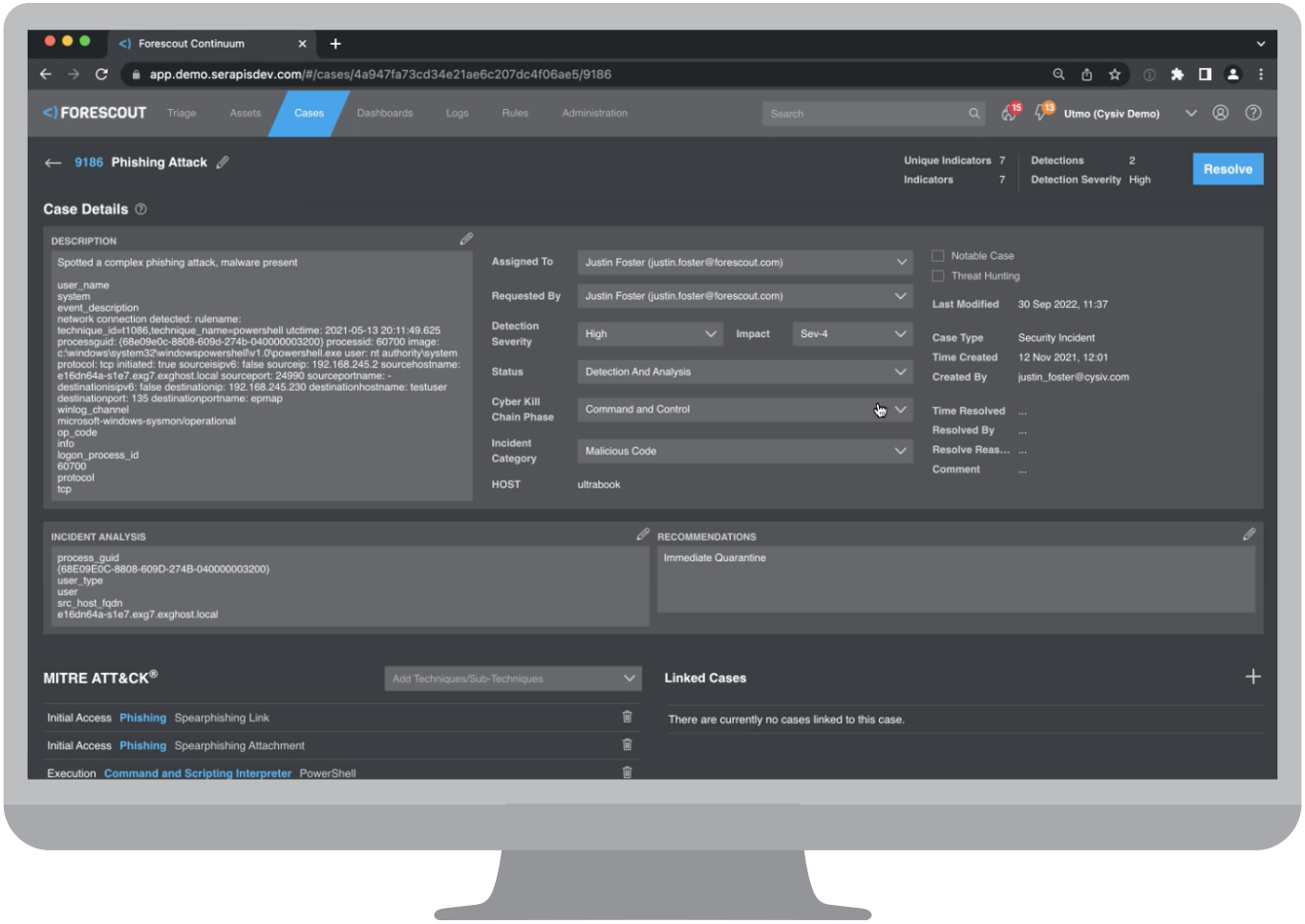
Mandantenfähige Architektur

Sie können leicht logische Trennungen (oder Mandanten) erzeugen, beispielsweise auf Basis von Ländern, Büro-standorten oder Geschäftsbereichen. Sie können auch aggregierte Ansichten erstellen und Abfragen und Analysen über Mandanten und Geschäftseinheiten hinweg durchführen, bis hin zur globalen Ebene. Dies ist besonders für große Unternehmen, multinationale Konzerne, MSSPs und Organisationen mit regionalen SOCs von Vorteil.

Einheitliche, globale Architektur

Datenresidenz- und Compliance-Anforderungen werden problemlos eingehalten und regionale Sicherheits-maßnahmen kostengünstig unterstützt. Sie können festlegen, in welcher der 25 Regionen in Nord- und Südamerika, Europa und im asiatisch-pazifischen Raum Ihre Protokolle gespeichert werden sollen. Unabhängig davon können Sie Ihre Daten jederzeit weltweit einsehen und abfragen.

Das Fallmanagement liefert umfassende Details und ermöglicht schnellere und effektivere Untersuchungen und Reaktionen.

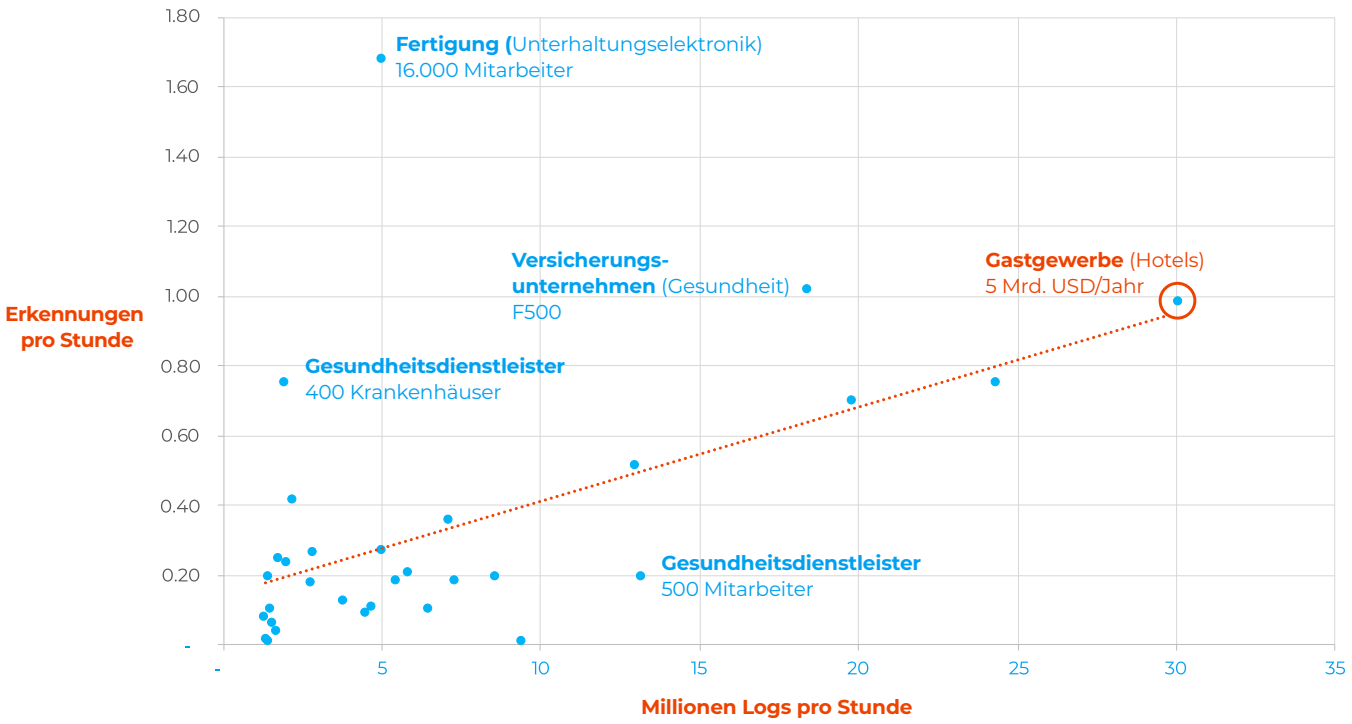


Die Lösung unterstützt Workflows, enge Integration, Transparenz und nahtlose Kommunikation und Kooperation bei der Bearbeitung von Erkennungen und beim Vorfallsmanagement. Forescout XDR basiert auf dem NIST Incident Response Life Cycle und unterstützt Integrationen mit ServiceNow, RSA Archer, Jira Software, ManageEngine ServiceDesk Plus, Palo Alto Cortex XSOAR, TheHive und ConnectWise.

Ergebnisse

Gleich, ob Sie Millionen, Dutzende Millionen oder Hunderte Millionen von Logs haben – Forescout XDR kann die Datenflut schnell und automatisch durchdringen, um eine sehr kleine Zahl hochgradig zuverlässiger Erkennungen zu generieren, die das Eingreifen menschlicher Analytiker erfordern.

Das folgende Diagramm zeigt die Daten von 31 Kunden für den Zeitraum eines Jahres ab 15. Dezember 2021. Beispielsweise konnte ein Unternehmen im Gastgewerbe mit 5 Mrd. USD Jahresumsatz durchschnittlich 30 Millionen Logs pro Stunde auf 0,98 handlungsrelevante Erkennungen pro Stunde reduzieren.



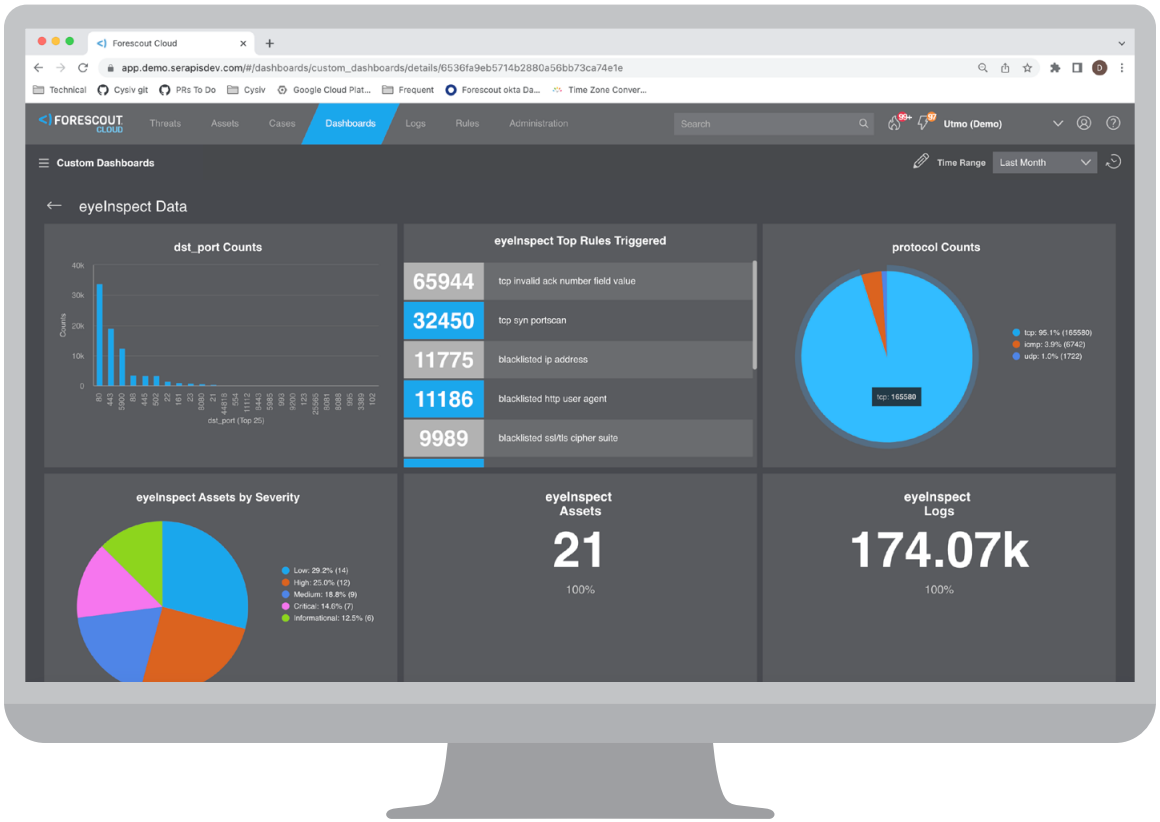
Hinweise:

- Vertreten sind Unternehmen verschiedener Größen und aus verschiedenen Sektoren:
  - Bauwesen
  - Konsumgüter
  - Energie-/Versorgungsunternehmen
  - FinTech
  - Gesundheitswesen
  - Versicherung
  - Produktion
  - Bergbau
  - Verlagswesen
  - Technologie
  - Transport/Logistik
- Die individuellen Ergebnisse können variieren und hängen von verschiedenen Variablen ab, wie etwa Anwendungsfällen, Auswahl der Protokolle, Gesamtzahl der Protokolle und fortlaufende Anpassung von Regeln.

1 The State of Security Operations, Forrester, 2020
2 Endpunkt bezieht sich auf jede MAC- und IP-Adresse auf einem Benutzergerät, Netzinfrastrukturgerät, nicht benutzerbezogenen Gerät oder auf einer Komponente einer Cloud-Infrastruktur.

Forescout XDR

eXtended Detection and Response



SEHEN SIE FORESCOUT XDR IN AKTION

forescout.com/xdr-demo-request

FORESCOUT

Forescout Technologies, Inc.

Gebührenfrei (US) 1-866-377-8771
Tel (intl) +1-408-213-3191
Support +1-708-237-6591

Erfahren Sie mehr auf Forescout.com

Forescout XDR

eXtended Detection and Response

FORESCOUT