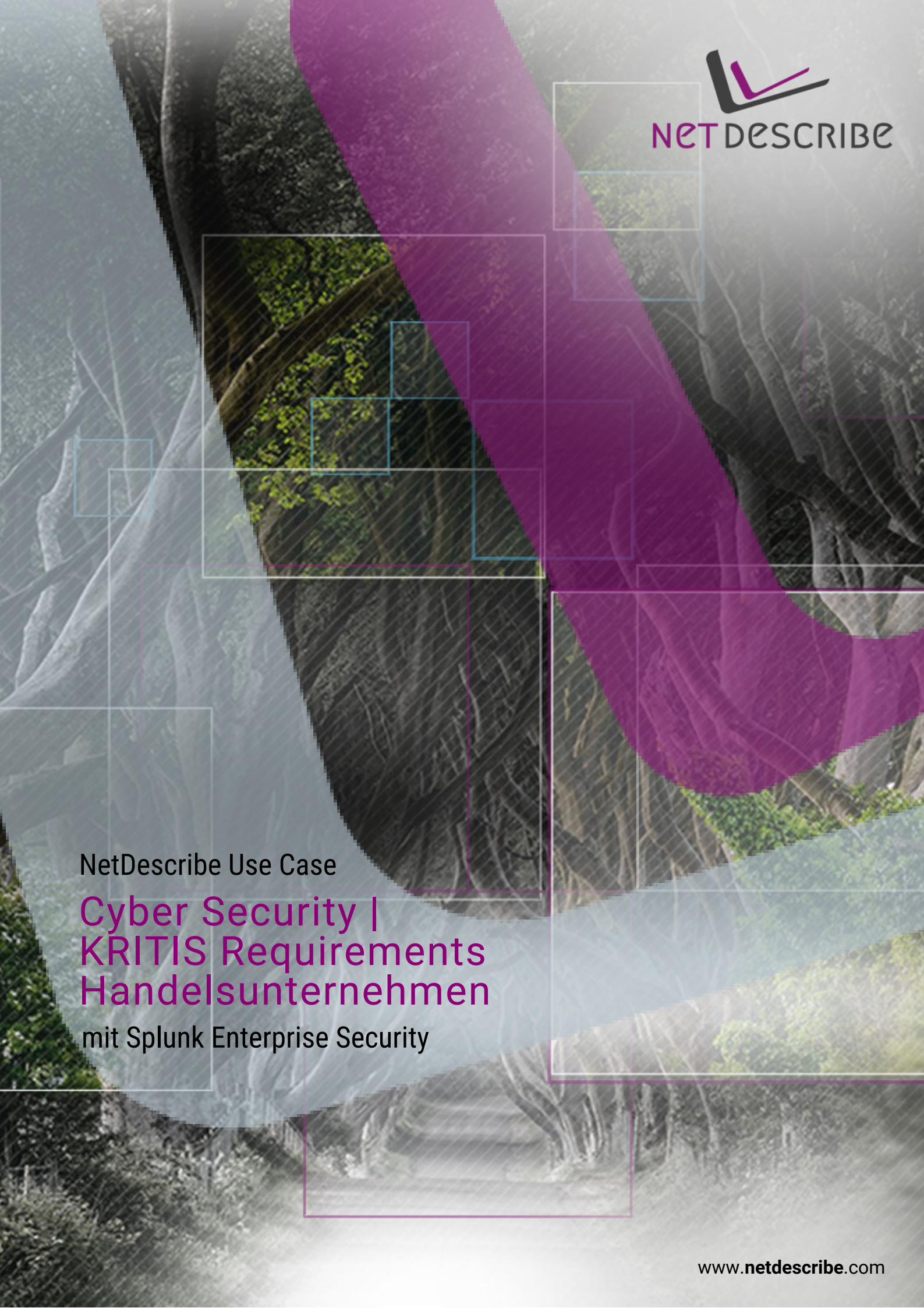


NetDescribe Use Case

Cyber Security | KRITIS Requirements Handelsunternehmen

mit Splunk Enterprise Security

1. Die Ausgangssituation

Unser Kunde unterliegt der KRITIS Verordnung im Bereich Ernährung und muss sicherstellen, dass das erforderliche Niveau von Cyber Security und IT-Sicherheit für die KRITIS Anlagen umgesetzt wird.

Als einer der wichtigsten Handlungspunkte wurde dabei die Perimeter Firewall Überwachung identifiziert. Das Element Manager System für das Verwalten der Firewalls bot zeitlich keine ausreichend lange Aufbewahrungs- und Analysemöglichkeit von Log Events.

Wie können die KRITIS-Anforderungen des BSIG in meinem Unternehmen umgesetzt werden?*

Die BSI-Kritisverordnung verpflichtet Betreiber kritischer Infrastrukturen unter anderem, angemessene Vorkehrungen zur Vermeidung von Störungen […] ihrer informationstechnischen Systeme, Komponenten und Prozesse" nach dem "Stand der Technik" zu treffen und dies gegenüber dem BSI nachzuweisen.

"Stand der Technik" ist ein gängiger juristischer Begriff. Die technische Entwicklung ist schneller als die Gesetzgebung. Daher hat es sich in vielen Rechtsbereichen seit Jahren bewährt, in Gesetzen auf den "Stand der Technik" abzustellen, statt zu versuchen, konkrete technische Anforderungen bereits im Gesetz festzulegen. Was zu einem bestimmten Zeitpunkt "Stand der Technik" ist, lässt sich zum Beispiel anhand existierender nationaler oder internationaler Standards und Normen von DIN, ISO, DKE oder ISO/IEC oder anhand erfolgreich in der Praxis erprobter Vorbilder für den jeweiligen Bereich ermitteln.

*Quelle: www.bsi.bund.de

Die Umsetzung dieser gesetzlichen Vorgaben stellt enorme Herausforderungen an die betroffenen Unternehmen und vor allem an die, mit der Ausgestaltung befassten, Teams. Da kann man leicht den Überblick verlieren.

Der erste Schritt zu Rechtssicherheit und Klarheit: Sichtbarkeit der Verfügbarkeit aller Ihrer IT-Dienste!

Woran es oftmals fehlt, sind datengestützte Erkenntnisse für umfassende Sichtbarkeit sowie schnelle Erkennung von Angriffen und sonstigen Bedrohungen in Ihrer IT-Landschaft.

Ganz oben auf der Wunschliste der Unternehmen:

- durchgängige Transparenz in allen Ihren Umgebungen,
- schnelle Bedrohungserkennung,
- effiziente Untersuchungen,
- ein offenes und skalierbares System, welches in Ihre Strukturen integrierbar ist und
- jederzeit verfügbare Analysen entsprechend Ihrer individuellen Anforderungen.

2. Der Use Case

Der Unternehmensverbund aus dem Einzelhandel mit einem Absatzgebiet im Südwesten Deutschlands - über Baden-Württemberg, Rheinland-Pfalz und dem Saarland sowie Teilen Hessens und Bayerns - trägt, einschließlich der Kolleginnen und Kollegen im selbständigen Einzelhandel, rund 47.000 Mitarbeiterinnen und Mitarbeiter, darunter rund 3.000 Auszubildende.

Im Jahr 2022 erzielten sie einen Verbund-Außenumsatz von 10,3 Milliarden Euro. Damit nehmen sie einen der Spitzenplätze im nationalen Handelsverbund ein.

Das Ziel des Unternehmens war die Erfüllung der notwendigen Vorgaben für eine KRITIS-Auditierung, sowie gleichzeitig die Umsetzung zeitgemäßer Sicherheitsstandards zum Schutz vor Ausfällen und Bedrohungen.

Die Lösung von NetDescribe

Der Einsatz von Splunk Enterprise Security ermöglicht Unternehmen verteilte Daten konsequent per Log-Analyse zentral zu überwachen, auszuwerten und zu visualisieren und somit wertvolle Erkenntnisse aus den Maschinendaten bereitzustellen.

Es können Korrelationsregeln und Berichte erstellt werden, um Unregelmäßigkeiten und Bedrohungen sofort zu identifizieren und automatisch Bereiche mit Verstößen zu erkennen.

3. Die Herangehensweise

In einem Proof of Concept wurden die Möglichkeiten von Splunk gemeinsam mit dem Kunden in Bezug auf seine Anforderungen evaluiert. Dabei wurde bereits während dieser Phase die Konfiguration der Splunk Umgebung so ausgerichtet, dass eine spätere nahtlose Überführung in die Produktivumgebung möglich war.

Für die Analyse der Log Events auf typische sicherheitsrelevante Verhalten und Anomalien wurde eine verteilte Splunk Umgebung mit zwei Indexieren, einem Manager Node und einem Search Head etabliert.
Die bereitgestellte Analyseplattform wurde auf den Bedarf Log Daten ein Jahr aufzuheben dimensioniert. Dies ermöglichte dem Kunden, im Gegensatz zum Hersteller Management System, die Logdatei 10 mal länger aufzubewahren und für Analysen bereitzustellen.

Splunk Enterprise Security

Splunk Enterprise zeigt die Verfügbarkeit Ihrer IT-Dienste aus realer Anwendersicht. Sowohl die Verteilung auftretender Probleme jeglicher Art, als auch die schnelle Identifizierung ihrer Ursachen.

Splunk Enterprise wächst mit Ihren Anforderungen und ist unbegrenzt skalierbar. Möglich sind die Lösung einzelner Probleme wie auch ganzheitlicher, strategischer Überwachungs-szenarien, zum Beispiel für Application Delivery, IT Operations, Security Compliance & Fraud, Business Analytics, IoT & Industrial Data.

4. Die Umsetzung

Die erste Präsentation der möglichen Lösung wurde im Februar 2019 für den Kunden im Rahmen einer Operational-Intelligence-Demo durchgeführt, bei der die Splunk Experten von NetDescribe mit den technischen Möglichkeiten von Splunk Enterprise überzeugen konnte.

Anfang März 2019 wurde ein PoC geplant, bei dem dedizierte Use Cases und entsprechende Erfolgskriterien gemeinsam mit dem Kunden vereinbart wurden.

Im April 2019 wurde im Rechenzentrum direkt beim Kunden eine Splunk Infrastruktur aufgebaut, die bereits während der PoC Phase so konzipiert wurde, dass das System nach erfolgreichem Test in den Produktivbetrieb übergehen konnte.

Am 27.05.2019 beauftragt der Kunde 100GB Splunk Enterprise für ein Jahr und Consulting zur finalen Implementierung der Lösung, sowie die Anbindung der geplanten Datenquellen und die Auswertung im Rahmen von Dashboards und Reports.

Trotz massiver Umstrukturierungen im Unternehmen und einem damit verbundenen Ansprechpartner-wechsel, verlängerte der Kunde um ein weiteres Jahr. Zu diesem Zeitpunkt war bereits absehbar, dass eine weitere Niederlassung künftig ebenfalls an Splunk angebunden werden sollte. Neues Management, neue Use Cases und Datenquellen (Windows und Linux Serverlogs) und intensivere Verwendung von Splunk führten dann wieder ein Jahr später zur Verdoppelung der Lizenz.

Im Mai 2022 hatte der Kunde den strategischen Wert von Splunk für sein Unternehmen erkannt und verlängert um weitere 24 Monate, verbunden mit einer Beauftragung von 500GB Splunk Enterprise.

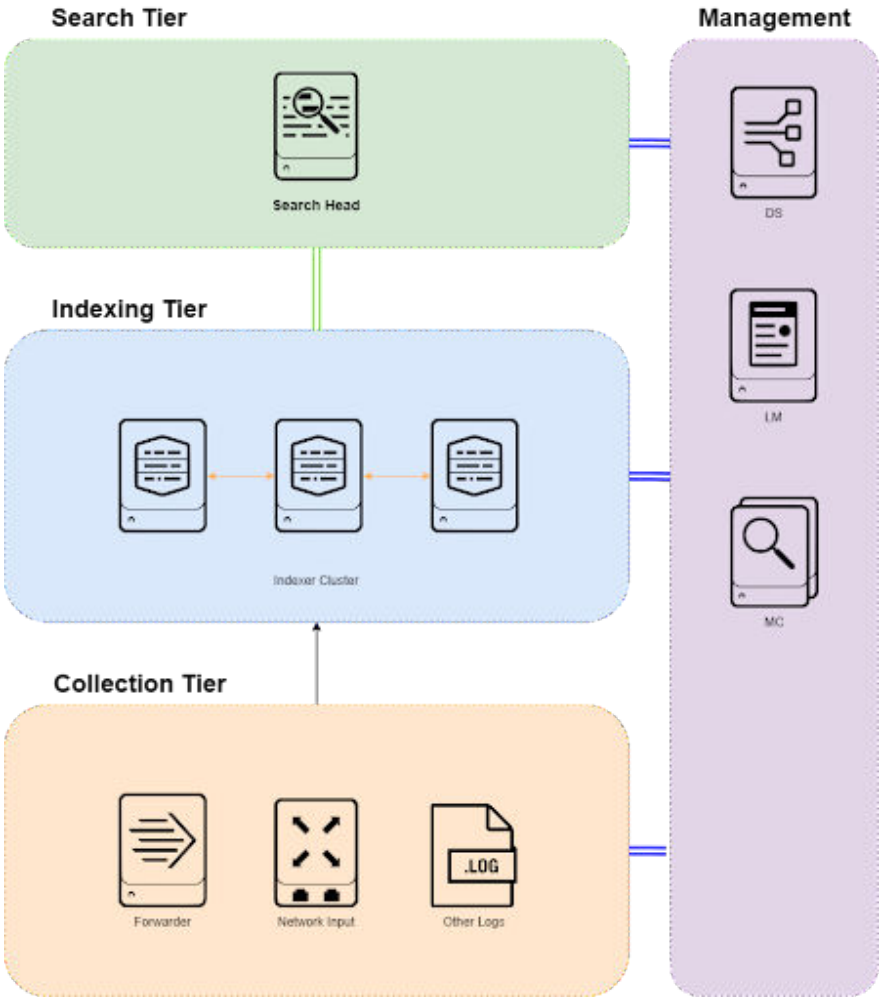
Durch die kontinuierliche und zielführende Beratung der NetDescribe Consultants entschied sich das Unternehmen dazu, den Einsatz von Splunk intensiv auszuweiten, so dass bei der nächsten anstehenden Verlängerung eine weitere Verdoppelung des Volumens geplant ist.

Nach erfolgreichem PoC von Splunk Enterprise Security, wurde auch die SIEM Lösung von Splunk budgetiert und wird im nächsten Geschäftsjahr implementiert.

Splunk SIEM (Security Information and Event Management)

- Volle Transparenz in all Ihren Umgebungen
- Schnellere Bedrohungserkennung und -untersuchung
- Mehr Flexibilität und Kompatibilität unterschiedlicher Tools und Technologien

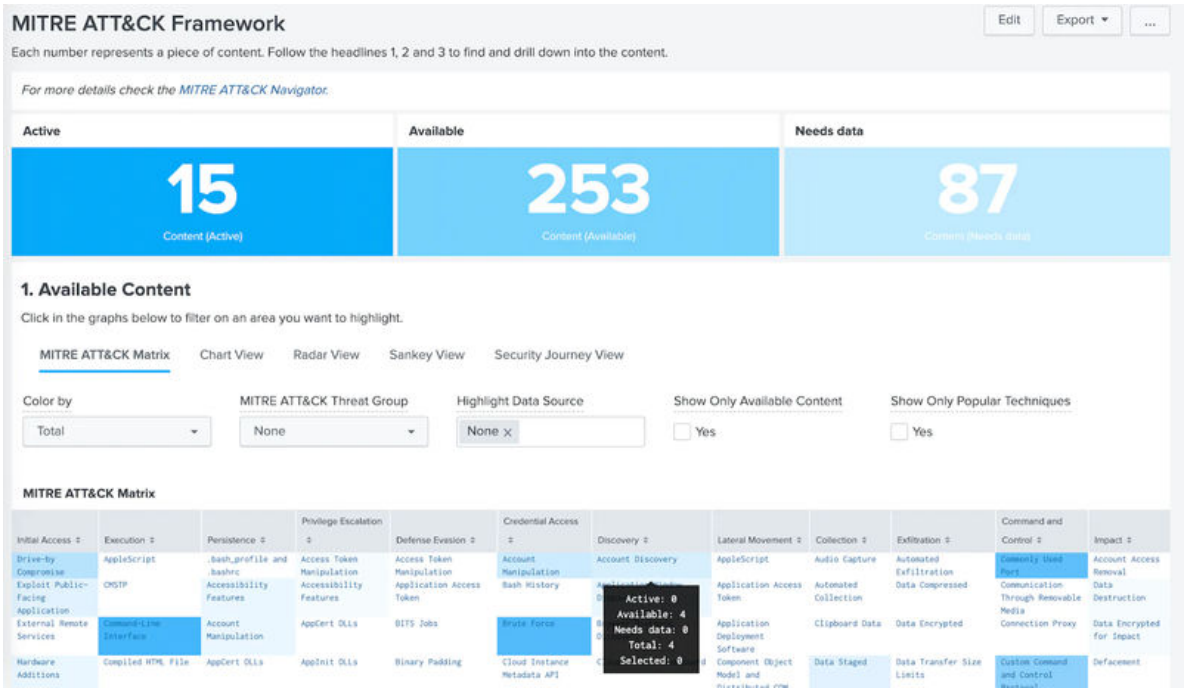
Splunk Architecture*



Use Cases für Splunk PoC:

- Integration der dezentralen Checkpoint Firewalls
  - Checkpoint App
- Integration der Sandblast Systeme
- Integration der 2 Perimeter FW's Firepower
- Vorschläge für Security Monitoring Use Cases
  - Infosec App
  - Splunk Security Essentials App

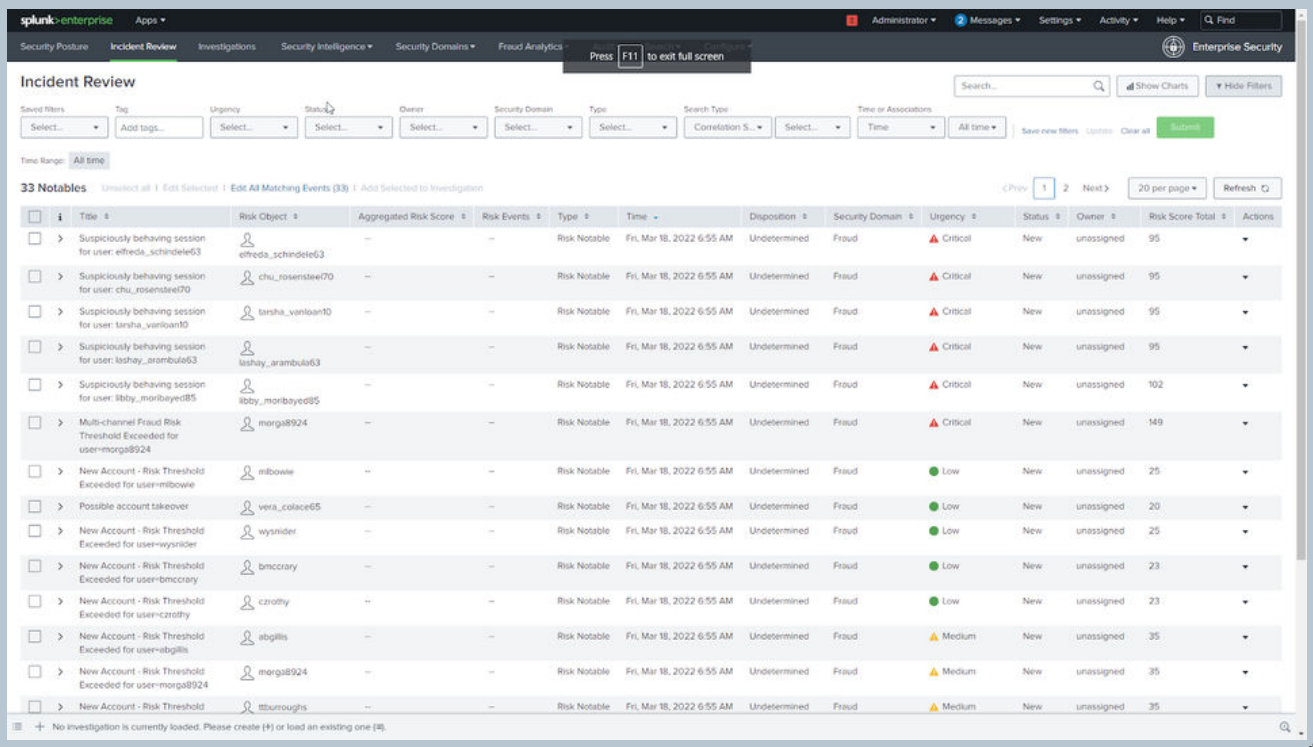
MITRE ATT&CK*



*Quelle: Splunk

Intrusion Detection*

Incident Review*



*Quelle: Splunk

5. Die Ergebnisse

- Eine starke Security Architecture bedeutet weniger Sicherheitsverletzungen für Ihr Unternehmen. Die schnelle und umfassende Implementierung der Lösung gewährleistet, dass die KRITIS Anforderungen im Hinblick auf Auditing und Compliance kontinuierlich erfüllt werden und die Risiken für unseren Kunden drastisch reduziert wurden.

- Analysen und Reports sind immer verfügbar, egal wann und in welcher Form diese benötigt werden - z. B. überzeugende Funktionen zur Auswertung der Firewall Logs unseres Kunden.

- Umstrukturierung und Neugestaltung der Geschäftsprozesse - ein Thema vieler Unternehmen.
  Mit Splunk Enterprise Security und der zielgerichteten Herangehensweise von NetDescribe wurde stets eine vertrauensvolle Zusammenarbeit, trotz wechselnder Ansprechpartner, gewährleistet. Nur so waren die erfolgreiche Implementierung und der Betrieb möglich.

- Kosteneinsparung und Ressourcenschonung durch Business Continuity und Schutz der kritischen Infrastrukturen und Daten.

- Kundenzufriedenheit sowie Steigerung des Vertrauens in das Unternehmen durch Transparenz und fortwährende Sprach- und Reaktionsfähigkeit.

- Durch die Pilotierung von Enterprise Security als SIEM Tool für das sich entwickelnde SOC, kann unser Kunde die nächste Etappe seiner Security Maturity Reise erreichen.

Das Splunk Portfolio

Splunk Plattform.
Splunk Enterprise sammelt und indiziert in Echtzeit alle Maschinendaten, die in physikalischen, virtuellen oder Cloud-Umgebungen erzeugt werden. Dies können Daten aus Applikationen, Servern, Netzwerken, Sensoren oder Telekommunikationsgeräten sein. Die Lösung korreliert komplexe Ereignisse, ermöglicht aussagekräftige Einblicke in Maschinendaten und vereinfacht Analysen.

Splunk für Sicherheit.
Splunk Enterprise Security verbessert alle Sicherheitsprozesse und gibt Ihnen als analysegestützte SIEM-Lösung (Security Information and Event Management) die ganzheitliche Sicht, um erzeugte Maschinendaten (z. B. Angaben über Netzwerke, Endpunkte, Zugriffe, Schwachstellen und Identitätsdaten) sicher nutzen zu können und um Sicherheitsverstöße zu reduzieren.

Splunk für IT- und Business Services.
Splunk IT Service Intelligence (ITSI) visualisiert als Monitoring- und Analyselösung Zustandsdaten und Key-Performance-Indikatoren (KPIs) von kritischen IT- und Business Services. Splunk ITSI nutzt maschinengetriebene (künstliche) Intelligenz, identifiziert bestehende und potenzielle Probleme, priorisiert die schnelle Wiederherstellung geschäftskritischer Dienste und stellt analytisch betriebene IT-Operations bereit.

Operational Intelligence & Security mit Splunk Enterprise und NetDescribe

Die Splunk-Funktionen auf einen Blick

Sammlung und Indizierung von Maschinendaten
Eventerfassung in Echtzeit, universelle Indizierung, Adapterentfall, Verwendung von Metrikdaten, Zeitstempel für Events

Suche und Überprüfung
Echtzeitsuche, Transaktionssuche, interaktive Ergebnisse

Korrelation und Analyse
Machine-Learning-basierte KI, Korrelation komplexer Events, Ereignisanmerkungen, Mustererkennung

Visualisierung und Reporting
Dashboard-Erstellung, Automatisierung von Berichten

Überwachung und Alarmierung
Monitoring von Ereignissen und KPIs, proaktive Benachrichtigungen

Sicherheit und Verwaltung
Verschlüsselter Zugriff auf Datenströme, gesicherter Benutzerzugriff