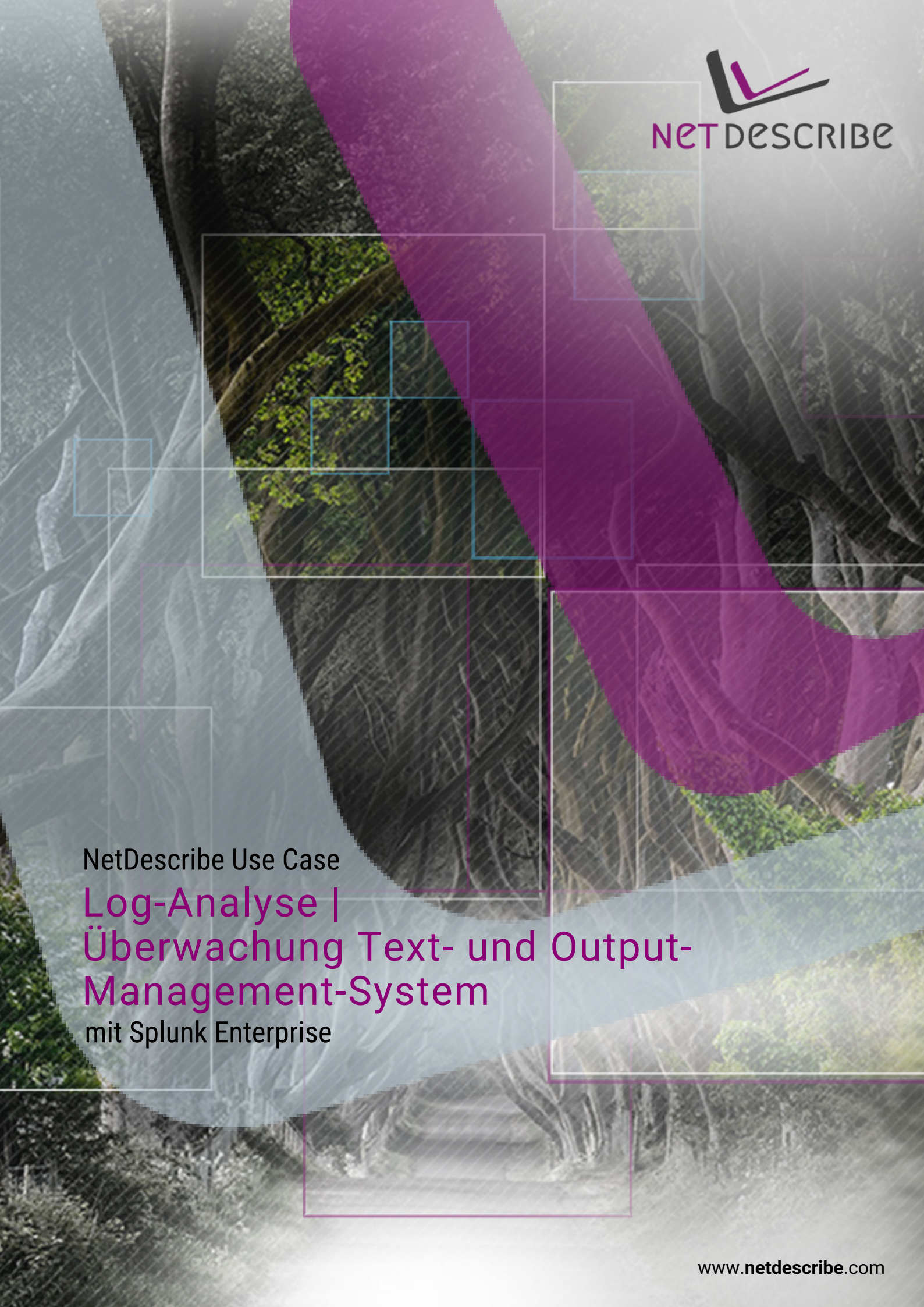


NetDescribe Use Case

Log-Analyse | Überwachung Text- und Output-Management-System

mit Splunk Enterprise

www.**netdescribe**.com

1. Die Ausgangssituation

NetDescribe wurde zunächst beauftragt, basierend auf Splunk, das Logging und die Auswertung der Logs für ein neues Text- und Output-Management-System zu konzipieren und zu implementieren.

Ziel war die Datenkonsolidierung zur effizienten Steuerung des Systems durch Fehlererkennung, Analyse von Durchlaufzeiten etc.

Was versteht man unter einem Text- und Output-Management-System?

Ein Text- und Output-Management-System ist ein System zur Erzeugung individueller und maschineller Korrespondenzen bis zur Ausgabe dieser an verschiedene Ausgabekanäle wie lokale Drucker, Druckstraßen, Druckdienstleister, Web-Portale, Fax, E-Mail, Dokumentenarchive. Einsatzgebiete sind Massendruck, interaktive Briefschreibung, Formular, zentraler und dezentraler Druck.

Diese Systeme bestehen aus verschiedenen Einzelkomponenten, die Informationen in ihren Log-Files oder Datenbanken ablegen.

Vorausschauend kann die Prozess-Integration bereichsübergreifend auf die gesamten Geschäftsprozesse eines Unternehmens ausgeweitet werden, also auch die Ressourcenplanung, Produktlebenszyklen, Engineering, Office etc. umfassen. Ein Vorteil ist die Erhöhung der Synergieeffekte zwischen den einzelnen Bereichen.

Neue Ansätze in diesem Bereich zielen auf die Bündelung sämtlicher Ausgabeprozesse im Unternehmen in einem zentralen System. Hierbei sollen alle Systemumgebungen, verschiedene Inputformate, sowie alle Output-Kanäle wie Print, Web, Archiv etc. eingebunden werden.

Mit der Lösung von Splunk sollen diese Informationen konsolidiert und ausgewertet werden, um beispielsweise Fehlerzustände analysieren zu können.

Der erste Schritt zur effizienten Überwachung: Auswertung und Analyse aller Maschinendaten!

Woran es oftmals fehlt, sind datengestützte Erkenntnisse für umfassende Sichtbarkeit sowie schnelle Erkennung von Veränderungen, Abweichungen von definierten Prozessen, Angriffen, Fehlern und sonstigen Bedrohungen in einer IT-Landschaft.

Ganz oben auf der Wunschliste der Unternehmen:

- durchgängige Transparenz in allen Ihren Umgebungen,
- schnelle Fehler- und Bedrohungserkennung,
- effiziente Untersuchungen,
- ein offenes und skalierbares System, welches in individuelle Strukturen integrierbar ist und
- jederzeit verfügbare Analysen entsprechend der individualisierten Anforderungen.

2. Der Use Case

Unser Kunde stellt seit 2008 den IT-Betrieb für 17.000 AnwenderInnen von Krankenkassen in Sachsen, Thüringen und Bayern sicher. Die Kernaufgabe ist es, die Transformation bei den Krankenkassen mit aller Kraft voranzutreiben. Das Leistungsspektrum erstreckt sich dabei von der Innovation und Beratung, der Organisation und Realisierung von maßgeschneiderten Lösungen, dem kompletten Betrieb der technischen Systeme bis zum Support, um die Krankenkassen bei der Erreichung ihrer Ziele zu unterstützen.

Das Ziel des Unternehmens war die eindeutige Verfolgbarkeit Ihrer Dokumente, die Analyse von Durchlaufdauern und Verweilzeiten sowie die Installation eines Systems zur Überwachung und Diagnose ihrer branchenspezifischen IT-Lösung.

Die Lösung von NetDescribe

Der Einsatz von Splunk Enterprise ermöglicht Unternehmen verteilte Daten konsequent per Log-Analyse zentral zu überwachen, auszuwerten und zu visualisieren. Wertvolle Erkenntnisse aus den Maschinendaten werden so bereitgestellt.

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

Von besonderem Wert für unseren Kunden waren die **zentrale Sicht** auf ihre gesamte IT-Umgebung auf einer einzigen Benutzeroberfläche, sowie die Möglichkeit der **ad hoc search** in Ergänzung zum Standard-Reporting-Portfolio, um schnelle Antworten auf Abweichungen vom definierten Prozess zu erhalten.

3. Die Umsetzung

Nach Auftragsvergabe wurden im Rahmen eines Kick-off-Workshops die Datenquellen identifiziert:

- JBoss-Logs (Linux: App-Server)
- SFTP (Linux: App-Server)
- sowie weitere Applikation-Logs
- MtextClient (800 - 900 Terminal-Server)

Zeitgleich wurden die Prioritäten für die unterschiedlichen Use Cases

1. Verfolgung von Dokumenten über eindeutige ID über alle Systeme hinweg (zur Fehleranalyse)
2. Durchlaufdauer/durchschnittliche Verbleibzeit von Dokumenten im jeweiligen System (von System A → B → A...)
3. Health Monitor zu oscare®-Systemen (Ampel-Dashboard)

und ein Zeitplan für die Implementierung erstellt.

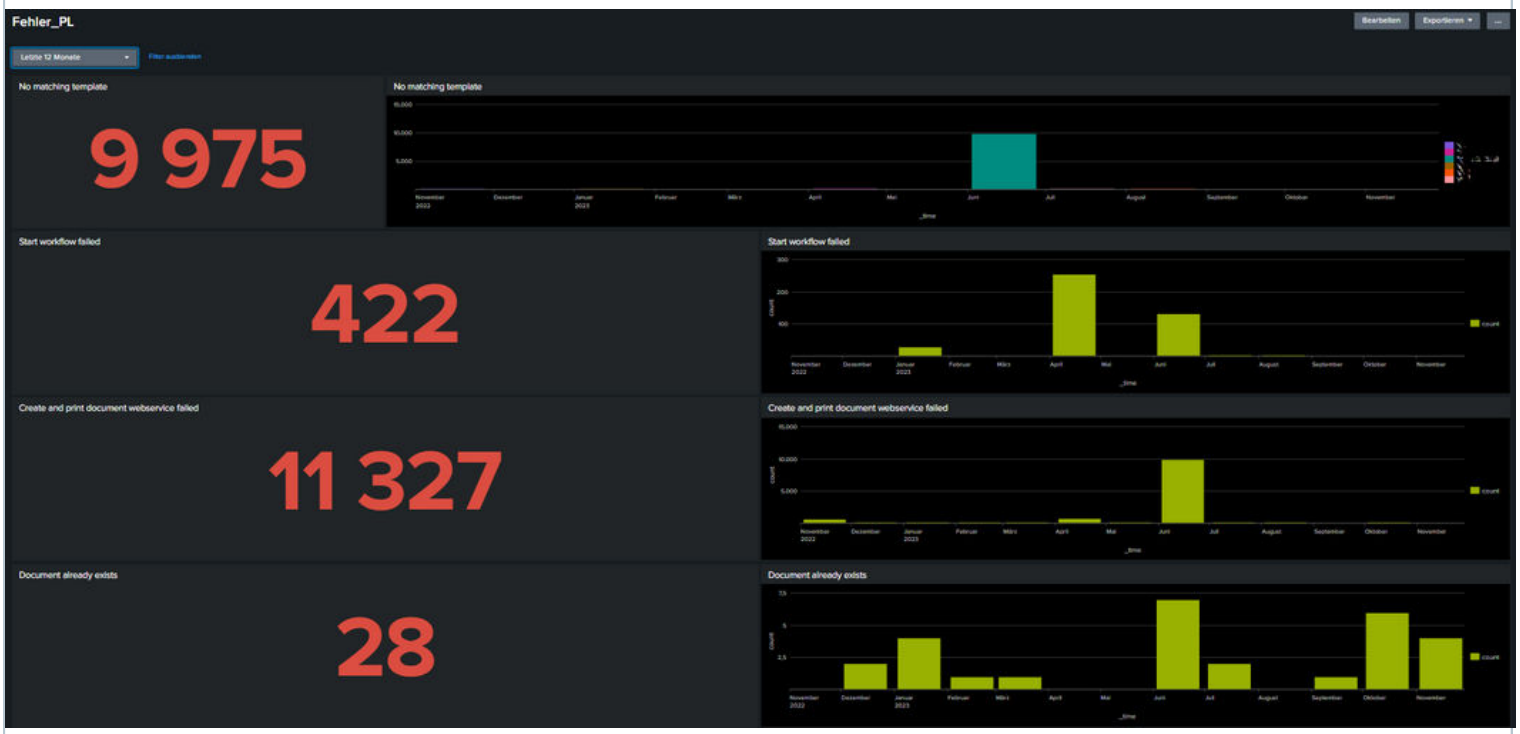
NetDescribe BUSINESS BONUS

Denken über den Tellerrand hinaus!

NetDescribe bietet **zusätzlich zum reinen Produkteinsatz** eine ganzheitliche und effiziente Lösung, die Sie bei der Konsolidierung und Optimierung ihrer gesamten IT-Prozesse unterstützt.

Welche Schnittstellen und Automatisierungen passen optimal zu Ihren IT-Prozessen? Und wie können Sie damit den gesamten Datenverkehr vom Netzwerk bis zur Cloud sicherstellen, analysieren und visualisieren?

In der Grafik werden die verschiedenen Templates im Versandprozess des Kunden am Beispiel der kompletten Briefkommunikation inklusive Antwortschreiben etc. dargestellt. Dies ermöglicht die Überwachung des vollständigen Kommunikationsprozesses und gibt Aufschluss darüber, ob dieser nach der definierten Prozessvorgabe abläuft.



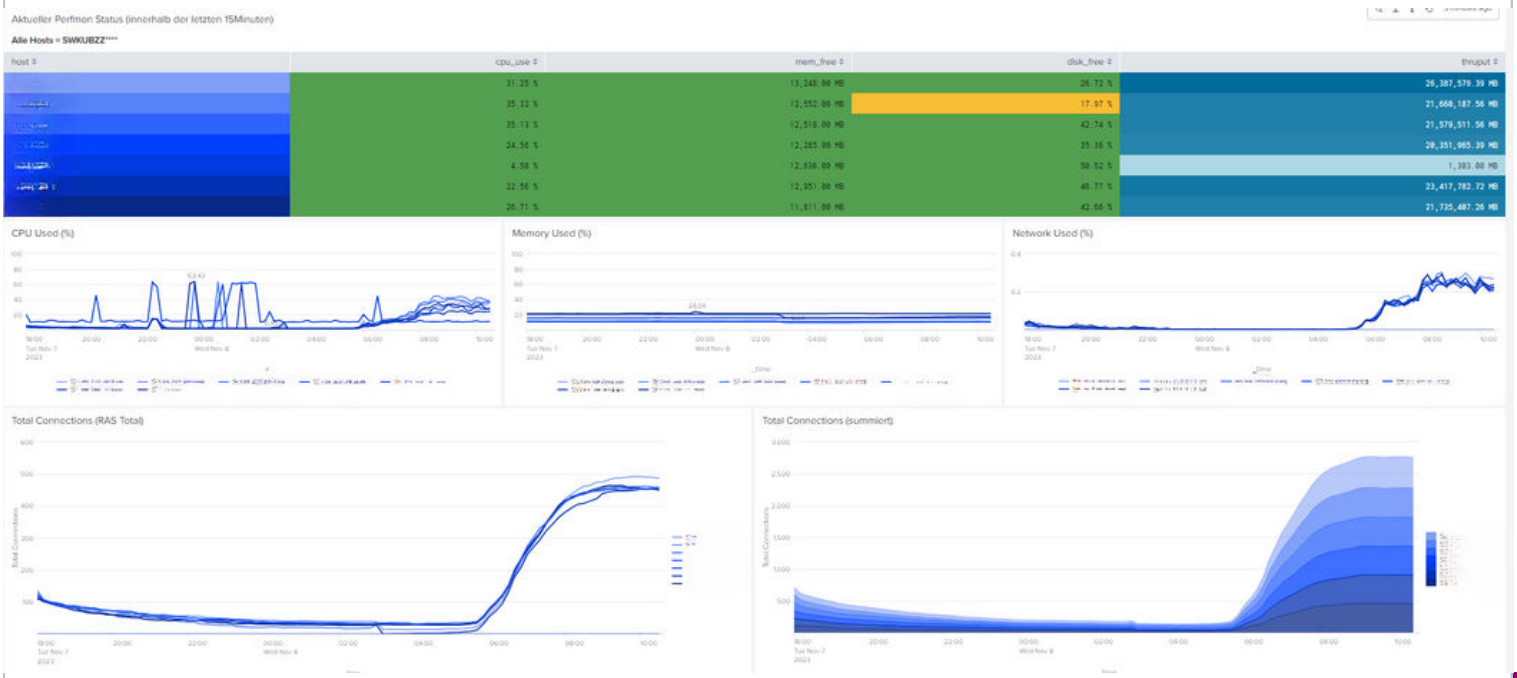
Die zweite Grafik gibt eine Übersicht darüber, was in einem definierten Zeitraum (z. B. 24 Stunden) in den verschiedenen Dokumentengruppierungen eingeht. Dies ermöglicht z.B. eine gezielte Ressourcenplanung.

Quelle Grafik 1 und 2: Anonymisierte Darstellung der Logs des Text- und Output-Management-Systems visualisiert

In Grafik 3 wird die Performance der VPN-Zugänge (global) dargestellt.

Noch während der Umsetzung des initialen Projektes im Bereich Text- und Output-Management-Überwachung trat NetDescribe mit anderen Bereichen (Netzwerk und Server) innerhalb der Kundenorganisation in Kontakt, von denen bekannt war, dass zwei weitere Splunk basierte Insellösungen existieren.

Dieser spezielle Use Case kam während der Pandemie zum Einsatz, als die Home-Office-Nutzung sprunghaft anstieg und dient als Beispiel für die vielfältigen Nutzungsmöglichkeiten von Splunk Enterprise.



Quelle Grafik 3: Anonymisierte Darstellung der Network Policy Server Logauswertung und -Visualisierung

4. Die Ergebnisse

Nach Umsetzung des Projektes Text- und Output-Management-Überwachung wurde NetDescribe beauftragt, die zugehörigen Splunk Lizenzen zu liefern.

Durch weitere Use Case Workshops identifiziert unser Kunde immer mehr Datenquellen, die mit Splunk überwacht und ausgewertet werden sollen. Hinzu kommen Windows- und Linux-Server, Firewalls und andere Netzwerkkomponenten sowie Daten aus der Container-Umgebung des Kunden.

Aufgrund der guten Referenz im Bereich Text- und Output-Management-Überwachung und der Unterstützung der Projektleitung konnten alle drei Bereiche mit Splunk Insellösungen von einem Gesamtkonzept überzeugt werden, das eine zentrale, einheitliche Splunk-Architektur für künftige Anforderungen vorsah.

Die langfristige Betreuung und vertrauensvolle Zusammenarbeit mit dem Kunden führte dazu, dass auch die benötigte Splunk Lizenz über die Jahre immer wieder erweitert wurde.

Heute analysiert unser Kunde täglich insgesamt knapp 500GB Daten mit Splunk.
Die Auswertung der Daten wurde forlaufend automatisiert und in Dashboards grafisch aufbereitet.
Die Splunk Eigenschaften ermöglichen eine ad hoc Suche nach Fehlern, um einem Problem schnell auf den Grund zu gehen.

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.

Automatisieren Sie Ihre Datenauswertung und Visualisierung. 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