Thinking Objects

Sophos UTM Troubleshooting mit Elastic Stack

Admin-Unterstützung dank optimierter Datenausgabe

Alle Vorteile auf einen Blick

Zeitersparnis bei der Fehlersuche dank

- Filter-Funktion
- Volltextsuche
- automatischer Konsolidierung

Erhöhung der Übersichtlichkeit durch grafische Auswertung

Steigerung der Detailgenauigkeit mittels Drill-Down

Kostensenkung durch reduzierten Ressourceneinsatz

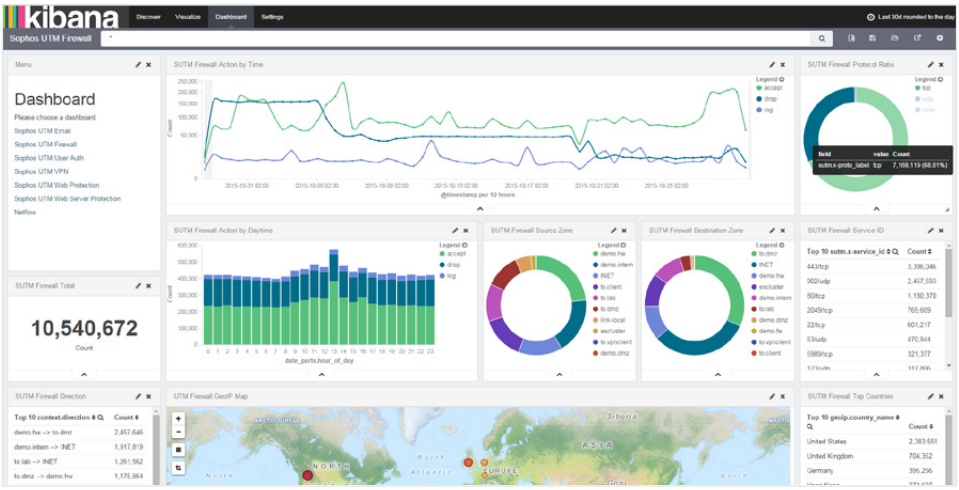
Schneller Return on Investment dank Einrichtung zum Festpreis

Die Herausforderung

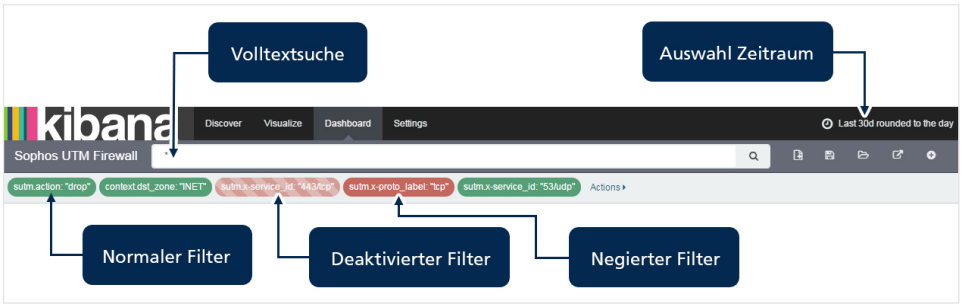
Die Fehleranalyse und -suche in den Logdaten auf der Sophos-UTM sind komplex und zeitlich anspruchsvoll. Die einzelnen kritischen Ereignisse müssen manuell gesucht, konsolidiert und ausgewertet werden. Durch den erhöhten Zeitdruck bei sicherheitskritischen Vorfällen kann hierbei eine vollständige Auswertung nicht gewährleistet werden. Zudem sind die Daten verteilt auf unterschiedlichen Systemen und somit schwer zu finden. Auch die Syntax in der Kommandozeile ist nicht jedem bekannt. Die Folgen davon sind Zeitverlust, Verschwendung wertvoller Ressourcen und damit Entstehung vermeidbarer Kosten. Zusätzlich ist die Qualität der Ergebnisse fraglich, da diese fehlerhaft und unvollständig sein können.

Die Lösung

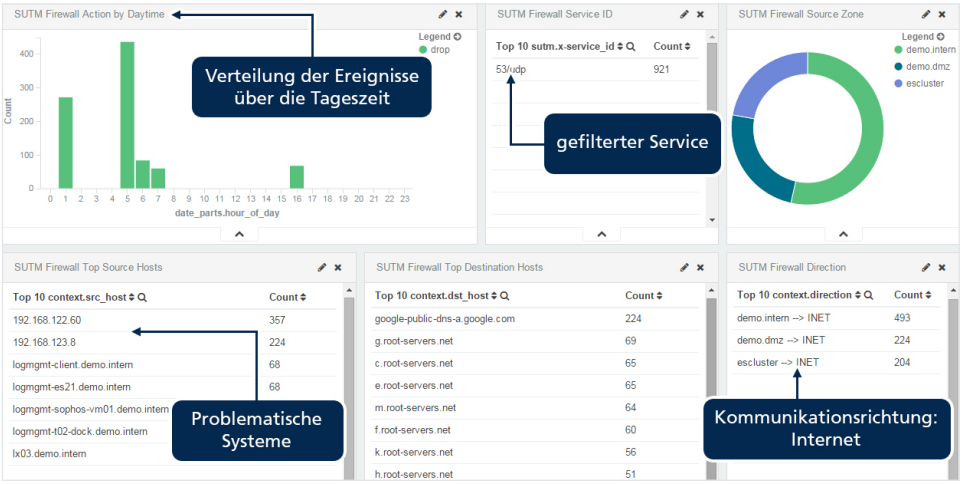
Wir haben die Lösung der bisherigen Probleme durch Verwendung einer Kombination der Open-Source-Komponenten Elastic, Logstash und Kibana entwickelt. Durch Einsatz des sogenannten „Elastic Stack“ (ehemals ELK-Stack) wird Ihr Prozess optimiert, Ihr Zeitbedarf, sowie Ihr Aufwand reduziert und Ihre Kosten gesenkt. Außerdem haben Sie mit unserer Lösung die Möglichkeit kritische Vorfälle noch vor der Problemmeldung durch die Anwender zu erkennen.



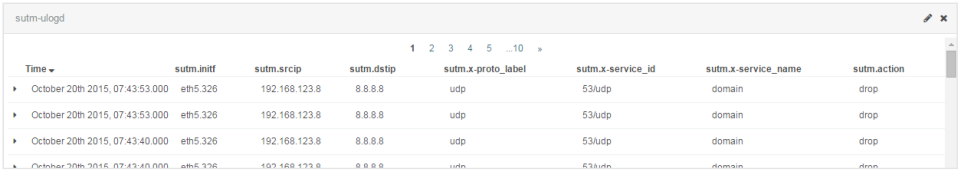
Wir vereinfachen Ihre Fehlersuche durch Ersetzen der Kommandozeile mit einer Suchzeile inklusive Volltextsuche und Filter.



Sie erreichen zudem eine deutliche Zeitersparnis durch automatische Konsolidierung gleichartiger Events sowie eine verbesserte Übersichtlichkeit dank grafischer Auswertungen anhand verschiedener Diagramme.



Ebenso erzielen Sie eine verbesserte Ergebnisqualität aus der gesteigerten Detailgenauigkeit mittels Drill-Down-Funktion innerhalb der einzelnen Panels.



Die Vollständigkeit der Informationen sowie die Minimierung von Fehlern werden durch fortlaufende Analyse und kontinuierliche Auswertung gewährleistet.

Mit unserer Lösung haben Sie die Möglichkeit von Beginn an Ihre zeitlichen und finanziellen Aufwände nachhaltig zu reduzieren und gleichzeitig die Qualität Ihres Fehleranalyseprozesses zu erhöhen. Zudem schaffen Sie die Basis für die Integration weiterer Systeme in die Auswertung und generieren somit weiteres Optimierungspotenzial.

Thinking Objects GmbH
Lilienthalstraße 2/1
70825 Korntal-Münchingen

+49 711 88770400
info@to.com
www.to.com