elastic

ERFOLGSGESCHICHTE

Weltmarktführer im Energie- und Bauwesen optimiert den Wert und den Schutz seiner Daten mit Elastic Observability und Security

Ein weltweit führendes Unternehmen der Energie- und Baubranche stärkt seine globale Dateninfrastruktur und verbessert seinen Schutz vor Cybersecurity-Risiken mit Elastic

Region
Frankreich

Branche
Energie- und Versorgungsindustrie

Lösung
Elastic Observability, Elastic Security für SIEM, APM, Schulung und Beratung



Schutz für ein globales Unternehmen
Die Umsetzung der Best Practices für Cybersicherheit von Elastic sorgt für mehr Transparenz und Risikoreduzierung.



Moderne Datenplattform für exponentiellen Wert
Mehr als 1.900 Konzerngesellschaften profitieren von der schnellen Erkennung und Beseitigung von Problemen.



Flexibilität, die unbegrenzte Möglichkeiten eröffnet
Dank der leistungsstarken Analyse- und Visualisierungsfähigkeiten von Elastic wird die Markteinführung signifikant beschleunigt.

 © 2024 Elasticsearch B.V. Alle Rechte vorbehalten.

elastic

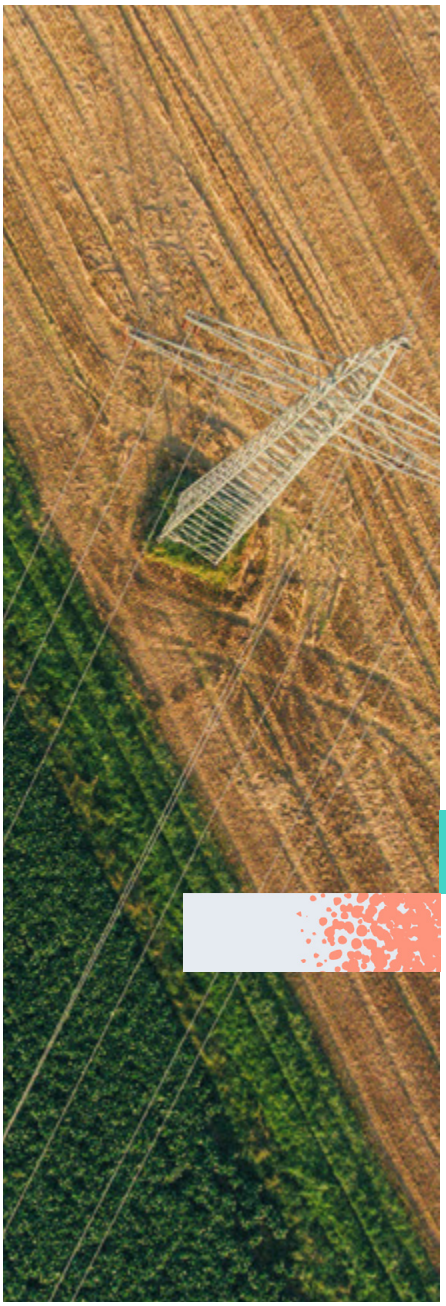
Als Tochtergesellschaft eines großen europäischen Mischkonzerns mit globaler Reichweite ist dieses große Energieunternehmen auf Lieferungen für die Transport- und Energieinfrastruktur, Energieberatung für die Industrie, Nachhaltigkeit und Energieleistung für Gebäude sowie die Unterstützung von Unternehmen bei ihrem digitalen Transformationsprozess spezialisiert. Mit mehr als 97.000 Beschäftigten ist es in über 120 Ländern vertreten.

Mehr als 800 Beschäftigte arbeiten für den stellvertretenden Leiter der Abteilung Systeme und Netze in der globalen IT-Abteilung und verwalten die IT-, Kommunikations- und Management-Tools, die Infrastruktur, die Netze und die Systeme der Gruppe, einschließlich der Sicherheits- und Security Service Edge (SSE)-Tools.

Das Unternehmen ist international tätig, was verschiedene Herausforderungen mit sich bringt: „Die Bedeutung des internen Supports, der rund um die Uhr verfügbar sein muss, erfordert die Fähigkeit und Kapazität, beim zentralen Informationsdienst intervenieren zu können“, sagt der stellvertretende Leiter der Abteilung Systeme und Netze mit besonderem Augenmerk auf die Tochtergesellschaft Energie.

Zu den 1.900 Gesellschaften, die das Unternehmen bereits umfasst, kommen jedes Jahr neue Unternehmen dazu – jeweils mit eigenen Systemen und eigener IT-Kultur. „In diesem Kontext geht es um die Begrenzung von Risiken“, sagt der stellvertretende Leiter der Abteilung Systeme und Netze.

Seit 2015 ist ein dediziertes Team für die kontinuierliche Verbesserung der Cybersicherheit im Konzern zuständig. Eine umsichtige Herangehensweise hat zwar das Risiko verringert, jedoch wurden die Fortschritte durch fehlende Einblicke in Protokolle und die Schwierigkeit ihrer Korrelation begrenzt. Auch das vom Unternehmen genutzte dezentrale Modell erschwerte die Umsetzung eines einheitlichen Informationssystems, das dafür sorgen sollte, dass alle Konzerngesellschaften dieselben Netzwerk- und Sicherheitsstandards anwenden.



„Die wichtigste Herausforderung ist die Datenqualität und Qualitätsdaten sind entscheidend, um allen Beschäftigten des Konzerns Sicherheit zu bieten. Ohne vertrauenswürdige Daten wird es schwierig, Angriffe effektiv zu erkennen und darauf zu reagieren.

Deputy Head of Systems and Networks
Führendes europäisches Energie- und Bauunternehmen

 © 2024 Elasticsearch B.V. Alle Rechte vorbehalten.

Eine flexible Lösung für das gesamte Unternehmen

„Splunk erfüllte unsere anfänglichen Anforderungen, bot jedoch nicht die benötigte Flexibilität. Das Produkt war nicht auf unsere Skalierung ausgelegt, und als unser Datenbestand immer weiter wuchs, stiegen die Kosten enorm“, so der stellvertretende Leiter der Abteilung Systeme und Netze.

Um die Sichtbarkeit zu verbessern und mit dem Datenwachstum Schritt zu halten, erprobte das Team eine Open-Source-Version von Elastic auf einem einzigen Server für ein paar hundert MB an Protokollen pro Tag. Der stellvertretende Leiter der Abteilung Systeme und Netze bekräftigt diese Entscheidung: „Der Name sagt schon alles!“, erklärt er. „Splunk ist einfach nicht so elastisch wie Elastic.“

Dieses große europäische Energieunternehmen entschied sich für Elastic Security, um sich mit einer leistungsfähigen Lösung für Security Information and Event Management (SIEM) gegen Cyberangriffe zu verteidigen, und wählte Elastic Observability als eine verlässliche und skalierbare Referenzlösung für auf den Betrieb ausgerichtete Sichtbarkeit und Analyse.

Andere Teams lernten Elastic dank seiner flexiblen Dashboards und Visualisierungen, einfachen Integration und überlegenen Leistung schnell schätzen. Immer mehr Beschäftigte wollten Zugriff auf die Plattform und waren auch daran interessiert, durch Pay-as-you-Go-Bezahlverfahren den Cashflow zu verbessern.

> Der Name sagt schon alles! Splunk ist einfach nicht so elastisch wie Elastic.

Deputy Head of Systems and Networks
Führendes europäisches Energie- und Bauunternehmen

 © 2024 Elasticsearch B.V. Alle Rechte vorbehalten.

elastic

Effiziente Nutzung von Daten in großem Maßstab dank Elastic

Mit Elastic konnten wir schnell verschiedene Anomalien und ungeeignete Einstellungen identifizieren. Ein Problem, das seit drei Jahren bestand, wurde innerhalb einer einzigen Woche behoben.

Deputy Head of Systems and Networks
Führendes europäisches Energie- und Bauunternehmen

Mithilfe von Elastic konnte das Unternehmen Best Practices und Standards für Cybersicherheit umsetzen. Während das Unternehmen im Bereich Energie seinem zentralen Informationssystem besondere Beachtung schenkt, kann die Überwachung spezifischer Geschäftsanwendungen an Konzerntöchter abgegeben werden.

Um in einem so großen Unternehmen eine optimale Geschwindigkeit und Effektivität zu gewährleisten, müssen die Sicherheitsexperten in den zentralen und lokalen Niederlassungen auf dieselben SecOps-Tools zugreifen können. Vor Elastic mussten für eine manuelle Korrelation alle Beteiligten auf jeder Stufe der Daten-Journey einbezogen werden.

Die Landschaft verändert sich rapide, wobei die technologische Entwicklung mit fortschreitenden Anforderungen an die Sicherheit einhergeht. Die Schnelligkeit von Elastic war entscheidend, um das Team in die Lage zu versetzen, Informationen viel schneller als zuvor abzurufen. Der stellvertretende Leiter der Abteilung Systeme und Netze erläutert: „Beim Durchsuchen langer Zeiträume müssen Sie die relevanten Daten unter Milliarden von Protokolleinträgen finden.“ Mit Elastic ist auch die Erstellung von Dashboards für Zwecke möglich, die andere Lösungen nicht anbieten konnten.

Elastic Observability wird eingesetzt, um die mehr als ein Terabyte an täglich erfassten Protokollen optimal zu nutzen. Durch das Echtzeit-Monitoring mit Elastic können mögliche Bedrohungen gestoppt werden, während leistungsstarke Analysefähigkeiten Daten in verwertbare Erkenntnisse umwandeln.



Dieses große Energieunternehmen legt den Schwerpunkt auf nachhaltige Beziehungen im Bereich Infrastruktur, Industrie, Gebäudelösungen und ICT.

 © 2024 Elasticsearch B.V. Alle Rechte vorbehalten.

elastic

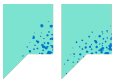
Vielfältige Einsatzmöglichkeiten

In der IT-Umgebung werden Anwendungen durch ein Ökosystem an Diensten, Netzwerken und Sicherheitstechnologien unterstützt. „Unser System für die Ressourcenplanung ist das Herz des Unternehmens“, erläutert der stellvertretende Leiter der Abteilung Systeme und Netze, „aber wir dürfen die Umgebung nicht vergessen: ein mangelhaftes Tool beeinträchtigt unweigerlich das gesamte System.“

Das Unternehmen betreibt eine Mischung aus Cloud- und On-Premises-Systemen. Auch hier kann Elastic durch seine Flexibilität überzeugen. Für die Cloud entwickelte Technologien können auch als On-Premises-Lösung effizient eingesetzt werden. Dank der Elastic-Integrationen sparen die Teams viel Zeit bei der Analyse von Protokollen und können sich auf Aufgaben konzentrieren, die einen höheren Beitrag zur Wertschöpfung leisten. Die Fähigkeiten, Protokolle schnell und einfach abzurufen, war für die Verbesserung der Sicherheitslage des Unternehmens entscheidend.

Administratoren können Daten mit vorgefertigten Integrationen einfach erfassen und verarbeiten, sodass Zeit für wichtigere Aufgaben zur Verfügung steht. Durch die Fähigkeit, diese Protokolle schnell abzurufen, wird die mittlere Reaktionszeit für SecOps- und IT-Teams gleichermaßen verkürzt.

Für Entwickler ist Elastic Teil ihres Alltags geworden. „Mit Elastic ist die einzige Beschränkung unsere Vorstellungskraft“, sagt der stellvertretende Leiter der Abteilung Systeme und Netze und macht dadurch deutlich, dass sich das Unternehmen in vielerlei Hinsicht auf Elastic verlässt.



„Elastic hat für die Flexibilität gesorgt, die wir brauchen, um Daten nahtlos zu integrieren, zu visualisieren und vor allem zu korrelieren. So können wir nun im Handumdrehen Informationen aus Milliarden an Protokolleinträgen in nur wenigen Sekunden extrahieren. Mit Elastic lässt sich mühelos die Nadel im Heuhaufen finden.“

Deputy Head of Systems and Networks
Führendes europäisches Energie- und Bauunternehmen



 © 2024 Elasticsearch B.V. Alle Rechte vorbehalten.

elastic

Erfolg in einer komplexen Umgebung

Laut dem stellvertretenden Leiter der Abteilung Systeme und Netze hat sich Elastic bei der Verbesserung der Sicherheit und Verfügbarkeit als unschätzbar erwiesen. Dank Elastic Security kann das Unternehmen verdächtige Aktivitäten schnell erkennen und die Wahrscheinlichkeit sowie den Schweregrad von Sicherheitsvorfällen reduzieren. Darüber hinaus optimiert die Lösung den Incident-Response-Prozess durch die Bereitstellung eines sofortigen, zentralisierten Zugriffs auf zuvor verlorene oder isolierte Daten.

Mithilfe von Elastic Observability arbeitet die IT-Abteilung effizienter. Beispielsweise hatte das WLAN des Unternehmens immer wieder mit Leistungsproblemen zu kämpfen, die sich auf interne Kunden auswirkten. Durch die Ingestierung von Daten von einigen WLAN-Hotspots gelang es dem Team, ein langjähriges Problem zu beheben.

Alles ist möglich.

Demnächst wird das Energieunternehmen seine Nutzung von Elastic strategisch erweitern, um wichtige Geschäftsanforderungen zu erfüllen. In diesem Zuge werden nicht nur neue Sicherheitsherausforderungen ins Visier genommen, sondern es wird auch die Migration auf Elastic APM (Application Performance Monitoring) geprüft und in Schulungen und Zertifizierungen für Elastic investiert.

Einige Teammitglieder nehmen bereits aktiv an den Schulungs- und Zertifizierungsprogrammen für Elastic teil: Sie melden sich für Kurse wie Datenanalyse mit Kibana an, erkunden eine Vielzahl von On-Demand-Schulungsmodulen und erweitern ihr Fachwissen in Observability und Elastic Security.

Der Einsatz von Elastic hat beeindruckende Ergebnisse erbracht, was auch dem beharrlichen Support des Elastic-Teams und der gemeinsamen Vorstellung einer glänzenden Zukunft zu verdanken ist.

Probieren Sie die Vorteile von Elastic 14 Tage lang kostenlos aus.

Jetzt beginnen

 © 2024 Elasticsearch B.V. Alle Rechte vorbehalten.

elastic