splunk>

CASE STUDY

# Forschungszentrum Jülich verkürzt Problemerkennung und steigert Effizienz

JÜLICH
FORSCHUNGSZENTRUM

## Kurzfassung

Das Forschungszentrum Jülich mit über 5500 Mitarbeitern ist Mitglied der Helmholtz-Gemeinschaft, einem Zusammenschluss verschiedener deutscher Forschungszentren. Das große IT-Netzwerk des Forschungszentrums unterstützt Tausende von Forschern und beinhaltet das Jülich Supercomputing Center (JSC), das Wissenschaftlern in Europa Supercomputer-Rechenzeit mit höchster Performance bereitstellt. Jülich benötigte ein zentrales Log-Management-System, um Datenanalysen, Benachrichtigungen, Berichte und die Compliance-Umsetzung beschleunigen zu können. Seit der Einführung von Splunk Enterprise zeichnen sich für das Forschungszentrum Jülich deutliche Verbesserung ab, wie etwa:

- Echtzeitüberblick über Operational Intelligence
- Schnellere Untersuchung und Behebung von Problemen
- Verbesserte Compliance

## Warum Splunk?

Das Jülich Supercomputing Center betreibt JUQUEEN, einen der leistungsstärksten Supercomputer der Welt. In Zusammenarbeit mit bekannten Hardware- und Softwareherstellern arbeitet das JSC an den besonderen Herausforderungen bei der Entwicklung von Supercomputern der nächsten Generation. Das Forschungszentrum Jülich unterhält verschiedene IT-Systeme mit rund 12300 Computern und bis zu 7000 IP-Adressen, die permanent im Netzwerk angemeldet sind.

Eine der größten Herausforderungen für das IT-Team war die Vielzahl der unterschiedlichen Autorisierungssysteme. Dadurch standen Logdaten nicht an einer zentralen Stelle zur Verfügung, was Analysen für die Sicherheits- und Netzwerkteams sehr zeit- und ressourcenintensiv machte. Da kein direkter Zugriff auf Logdaten möglich war (Firewall, DHCP und Radius), waren die Teams gezwungen, Logdaten von IT-Administratoren anzufordern, die dann alle relevanten Informationen aus unzähligen Systemen zusammensuchen mussten. Es gab zwar verschiedene Tools für die Log-Analyse, sie lieferten jedoch nicht die gewünschte holistische Sicht.

Das Forschungszentrum Jülich entschied, dass eine neue, effizientere, sichere Lösung gefunden werden musste: eine Lösung, die als zentrales System für die Datenerfassung diente und es erlaubte, Benutzerrollen mit unterschiedlichen Zugriffsrechten zu definieren. Die Lösung sollte große Mengen an Logdaten schnell und effizient verarbeiten können, die

### Branchen

- Technologie

### Splunk Anwendungsbeispiele

- IT Operations
- Anwendungsbereitstellung
- Sicherheit
- Compliance

### Herausforderungen

- Sicherheits- und Netzwerkteams benötigen zentralen Zugriff auf Logdaten, um die Fehler- und Problembehebung zu beschleunigen.
- Es soll mehr Kontrolle und Koordination der Zugriffsrechte auf Supercomputer und andere HPC-Systeme möglich sein.
- Sicherheitswarnungen von internen und externen Quellen sollen korreliert und in Berichten dargestellt werden können.

### Auswirkungen für das Unternehmen

- Echtzeit- und historische Erkenntnisse aus Operational Intelligence aus riesigen Mengen von Logdaten aus völlig verschiedenen Quellen
- Zeit- und Kostenersparnis durch automatisierte Prozesse
- Mehr Sicherheit durch Senkung von MTTI (Mean Time To Investigate) und MTTR (Mean Time To Resolve) bei Sicherheitsvorfällen
- Automatisierte Benachrichtigungs- und Berichterstellung haben das Schwachstellenmanagement optimiert und die Compliance mit Vorschriften verbessert

### Datenquellen

- Firewall-Logs
- DHCP-Logs
- Radius-Logs
- CERT-Benachrichtigungen

### Splunk-Produkte

- Splunk Enterprise
- Splunk for Cisco ASA-App

Korrelation zwischen unterschiedlichen Logdateien garantieren und Ereignisse automatisch verarbeiten. Aufgrund der rapide wachsenden Datenvolumen war Skalierbarkeit ein weiterer wichtiger Faktor. Vor dem Hintergrund all dieser Anforderungen implementierte das Jülicher Team Splunk Enterprise.

## Schnell aussagekräftige Erkenntnisse

Zwei Mitarbeiter des Forschungszentrums brauchten nur zwei Stunden, um Splunk Enterprise für einen ersten Test einzurichten. Bereits nach einem halben Tag wurden die ersten Logs nachverfolgt und verarbeitet. Heute werden mit der Splunk-Software mehr als 2000 Syslog-Einträge pro Sekunde verarbeitet! Da die Benutzerrollen jetzt unterschiedlichen Zugriffsberechtigungen entsprechen, können Sicherheits- und Netzwerkverantwortliche ganz leicht auf die notwendigen Daten für ihre Aufgaben zugreifen. Sie können sofort auf Sicherheitsvorfälle wie beispielsweise den Download eines Virus reagieren und einschreiten, bevor die Auswirkungen spürbar werden. Die Logs für die Überwachung auf unbefugten Zugriff auf den Supercomputer und Cluster-Systeme werden jetzt zentral gesammelt und ausgewertet. Dadurch konnten die MTTI (Mean Time to Investigate) und MTTR (Mean Time To Resolve) drastisch gesenkt werden.

## Höhere Effizienz durch automatisierte Benachrichtigungen

Auch aus strategischer Sicht profitiert das Forschungszentrum von der Implementierung der Automatisierungsmöglichkeiten der Splunk-Software. Mit Splunk Enterprise können automatisierte Benachrichtigungen an bestimmte Personengruppen gesendet werden. Durch die gezielte Kommunikation mit dem zuständigen Mitarbeiter können beim Erreichen eines bestimmten Schwellenwerts Schwachstellen schneller aufgedeckt und vermieden werden.

Darüber hinaus werden regelmäßig Sicherheitsberichte vom CERT-Portal (Computer Emergency Response Team) des deutschen Forschungsnetzes automatisch in Splunk Enterprise verarbeitet und mit den

**„Mit Splunk Enterprise können wir ganz leicht Logs aus einer Reihe unterschiedlicher Systeme zentral erfassen und auswerten. Diese Flexibilität und die zuverlässige Performance, selbst in großem Maßstab, haben viele wertvolle Vorteile für das Forschungszentrum Jülich, wie etwa mehr Sicherheit und effizientere Arbeitsabläufe.“**

**Mitarbeiter**

Forschungszentrum Jülich

Maschinendaten des Forschungszentrums verglichen. Jülich berichtet zudem von einem weiteren Vorteil der Verwendung von Splunk-Software für Operational Intelligence: Daten können jetzt innerhalb der vorgeschriebenen Aufbewahrungsdauer verarbeitet oder gespeichert werden, was dem Zentrum die Einhaltung strikter Compliance-Vorschriften ermöglicht.

## Antwort auf die Anforderungen der Forschungsgemeinschaft

Mit Splunk Enterprise konnte das Forschungszentrum Jülich ein robustes, zentrales System für die Verwaltung der riesigen Mengen an Maschinendaten einrichten, die von den Tausenden Computern und sonstigen Geräten der Forschungseinrichtung erzeugt werden. Mit Splunk Enterprise durchgeführte Suchen und Analysen können jetzt gespeichert und von autorisierten Benutzern wiederverwendet werden. Dies spart wertvolle Zeit und beschleunigt die Behebung sicherheits- und leistungsbezogener Probleme.



splunk> SplunkCe@Splunk.com www.splunk.com



CS-Splunk-Julich-A4-102_DE