splunk>

WHITEPAPER

WIE SPLUNK UND MASCHINENDATEN DAS ISO/IEC 27001-FRAMEWORK UNTERSTÜTZEN

Die digitale Transformation, der Aufbau von Kundenvertrauen und ein Flickenteppich aus Gesetzen, Vorschriften und Normen zwingen Unternehmen auf der ganzen Welt dazu, ihre Sicherheitsprogramme zu formalisieren. Viele Jahre lang wurde Sicherheit von Vorständen nur als technisches Problem angesehen. Das hat sich in den letzten Jahren grundlegend geändert, und IT-Governance und die Einrichtung eines Informationssicherheits-Managementsystems (Information Security Management System, ISMS), das auf ISO 27001 aufbaut, haben für Unternehmen heute höchste Priorität.

Der Chief Information Security Officer (CISO) muss Sicherheitsstrategien entwickeln, die sowohl auf das aktuelle als auch auf das zukünftige Geschäft ausgerichtet sind. Der CISO verantwortet darüber hinaus Entwicklung und Betrieb des Informationsrisikoprogramms des Unternehmens. Unternehmen benötigen Sicherheitsrichtlinien, die entwickelt und umgesetzt werden müssen. Außerdem müssen sie neue Prozesse, wie Incident Response-Prozesse einrichten und oftmals auch zusätzliche operative Sicherheitsfunktionen aufbauen.

Dies wird durch Implementierung entsprechender Kontrollmaßnahmen auf der Grundlage des Leitfadens für Informationssicherheitsmaßnahmen (ISO/IEC 27002) erreicht.

Splunk Software gibt Sicherheitsteams jeder Größe die Möglichkeit, die Informationen und Erkenntnisse aus Maschinendaten, die von jedem Netzwerk, jedem System, jeder Datenbank, jedem Webserver, jeder Anwendung und jedem internetfähigen Gerät erfasst werden, zu untersuchen, zu überwachen, zu analysieren und umzusetzen. Sicherheitsteams setzen auf Splunk-Technologie als Process Enabler und Multiplikator der vorhandenen Workforce, um mehr Arbeit in kürzerer Zeit, für weniger Geld und mit höherer Genauigkeit zu erledigen.

Die Splunk Plattform bietet Sicherheitsteams darüber hinaus einen guten Return-on-Investment, indem sie ihnen ermöglicht, Probleme jenseits von Compliance mit denselben Daten zu lösen, die auch für Konformitätprobleme genutzt werden. Die gleichen Maschinendaten können für Teams in IT Operations, Anwendungsentwicklung, Business Analytics und Industrie 4.0/IoT relevant sein.

Das Resultat sind operative und sicherheitsrelevante Informationen, die unter anderem Reputationsrisiken sowie Risiken für Kerngeschäftsfunktionen mit Umsatzauswirkungen sowie für Compliance, die sich auf Reputation, Kundenvertrauen und Geschäftsergebnis auswirkt, betreffen.

Wie Splunk hilft

Die Splunk Software ist eine Big Data-Plattform für Sicherheit und Maschinendaten und unterstützt die ISO 27002 in folgender Weise:

- Bereitstellung von Berichten über Maschinendaten als Kontrollmittel zum Compliancenachweis
- Schutz von Maschinendaten vor unbefugter Einsicht, Änderung oder Löschung sowie Bereitstellung von Audit-Trails
- Tägliche Überprüfung von Systemen zum Abgleich von tatsächlichem Verhalten mit vorgegebenen Richtlinien
- Monitoring von Netzwerkgeräten, Servern, Anwendungen und Transaktionen hinsichtlich operativer und sicherheitsrelevanter Risiken zur Erlangung von Geschäftsresilienz
- Fähigkeit zur Durchführung von Ursachenforschung
- Unterstützung von eDiscovery-Anfragen von Strafverfolgungsbehörden
- Durchführen von HR-Untersuchungen zu Aktivitäten einzelner Mitarbeiter
- Fähigkeit zum Ad-Hoc-Zugriff auf IT-Daten durch Compliance-Mitarbeiter
- Nachweis der Integrität von Audit-Daten

Wie die Implementierung abläuft:

Mythos: Compliance lässt sich durch eine bestimmte Reihe von Berichten erreichen.

Realität: Regulatorische Anforderungen führen fast nie spezifische Berichte auf. Es gibt Berichte, die bei bestimmten Anforderungen hilfreich sein können, z. B. das Erfordernis, fehlgeschlagene Anmeldungen zu überprüfen. Diese benötigen jedoch eine Feinabstimmung für jede einzelne Umgebung. Idealerweise ist eine Reihe von Standardberichten ein guter Ausgangspunkt.

Die einfache Wahrheit ist nämlich, dass die meisten Compliance-Berichtspakete von Produktmanagern entwickelt werden, die Regularien lesen und dann mehr oder weniger raten, welche Berichte hilfreich sein könnten. Der jüngste Trend beim Auditing besteht darin, einen IT-Mitarbeiter zur Durchführung einer Ad-Hoc-Abfrage aufzufordern. Dies kann eine einfache Anfrage oder sogar Anforderung des jeweiligen Auditors sein.

Jedes Unternehmen hat seine ganz eigene Risikobereitschaft, die sich sogar von Abteilung zu Abteilung unterscheiden kann. Aus diesem Grund müssen Sicherheitsrichtlinien definiert werden, die einen ergebnisorientierten Ansatz erzwingen. Um die in den Richtlinien für Informationssicherheit eines Unternehmens definierten Kontrollmaßnahmen in Form von SIEM-Anwendungsfällen für ISO 27002 zu implementieren, werden die folgenden Schritte empfohlen:

1) Überprüfen Sie die Richtlinien für Informationssicherheit Ihres Unternehmens und bestimmen Sie, ob Ihre SIEM-Lösung jede der Richtlinien erfüllen kann
2) Bestimmen Sie, welche Fragen beantwortet werden müssen und welche Maßnahmen oder Eskalationsstufen im Unternehmen diesbezüglich ergriffen werden müssen
3) Indentifizieren Sie, welche Systeme, technischen Komponenten oder Anwendungen, relevante Daten enthalten, die für die benötigte Antwort erforderlich sind
4) Sammeln Sie Maschinendaten
5) Untersuchen Sie die Maschinendaten und finden Sie die richtigen Einträge, die die Antwort enthalten
    a) Bestimmen Sie Protokollierungsstandards und stellen Sie sicher, dass die Protokollierungsstufe für die überwachten Datenquellen ordnungsgemäß konfiguriert ist
6) Definieren Sie die erforderliche Berichts-Logik und den eventuell benötigten Erweiterungsbedarf
7) Schreiben Sie die Splunk-Suchabfrage (oder übernehmen Sie sie und passen Sie sie aus vordefinierten Dashboards oder Berichten an)
8) Wählen Sie eine regelmäßige Berichterstellung, Echtzeit-Benachrichtigung über Sicherheitsevents oder beides

Dank Splunks leistungsstarker Suchsprache, der „Schema on the fly“-Funktionen und den mehr als 1.500 Apps in **Splunkbase** mit vordefinierten Dashboards und Berichten, lassen sich die Schritte 5 bis 8 auf Splunk normalerweise in Minuten durchführen.

In der Tabelle unten finden Sie spezifische Möglichkeiten, wie Maschinendaten und die Splunk Plattform Ihre Bemühungen zur Einhaltung der ISO 27002-Kontrollmaßnahmen unterstützen können.

ISO 27002-Kernbereiche	So unterstützen Maschinendaten und Splunk
6.1.2 Aufgabentrennung	Die Implementierung der Trennung kann kleinere Unternehmen vor Probleme stellen. Andere Kontrollmaßnahmen, wie etwa Monitoringaktivitäten und die Durchführung von Audit-Trails, sollten in Betracht gezogen werden. Splunk ermöglicht es kleinen Unternehmen, Audit-Trails zu erfassen und Aktivitäten zu überwachen und anschließend Aufgaben von allen Anwendungen oder digitalisierten Prozessen zu trennen. Es kann eine Aktivitätsanalyse durchgeführt werden, um die Trennung von Aufgaben zwischen Einzelpersonen und/oder festgelegten Rollen sicherzustellen. Splunk Enterprise unterstützt die rollenbasierte Zugriffssteuerung, sodass der Zugriff auf Informationen auf der Grundlage der spezifischen Rolle eines Benutzers erteilt wird. Benutzerkonten in Splunk können zwecks Single Sign-On/SSO in Active Directory oder LDAP eingebunden werden.
6.1.5 Informationssicherheit im Projektmanagement	Splunk ermöglicht dem Projektteam, die von einem digitalen Service erzeugten, unbekannten Maschinendaten frühzeitig zu untersuchen, um notwendigerweise zu berücksichtigende Risiken und Kontrollmaßnahmen zu bestimmen. Es ist wichtig, zu verstehen, was in Maschinendaten sichtbar ist, welche Art von Events/Aktionen möglicherweise fehlen, den Normalzustand zu bestimmen und Empfehlungen auszuarbeiten, wonach im Hinblick auf das Sicherheitsmonitoring im Produktionssystem zu suchen ist.

ISO 27002-Kernbereiche	Unterstützung durch Maschinendaten und Splunk
6.2.1 Richtlinie zu Mobilgeräten	Splunk ermöglicht die Erfassung und Berichterstellung aus Systemen für das Management von mobilen Geräten sowie die Erfassung aus Synchronisierungs-Services mobiler E-Mails, um alle neuen Geräteregistrierungen sowie Aktualisierungsbedarf zu erkennen, die Durchsetzung von Richtlinien zu melden und die erfolgreiche Ausführung von Aktionen zur Remote-Löschung zu dokumentierten, für den Fall, dass ein Smartphone verloren oder gestohlen wird.
6.2.2 Telearbeit	Splunk ermöglicht Unternehmen die Durchführung eines vollständigen Audit-Trails für jede Komponente, die für Telearbeitsaktivitäten verwendet wird. Hierzu gehören unter anderem Anmeldevorgänge über VPN, um über eine Terminalsitzung auf vertrauliche Dateien auf einem Dateiserver zuzugreifen und potenzielle Druckaufträge. Dies hilft bei der Beantwortung von Fragen wie: Wer hat auf was wann und in welcher Weise zugegriffen. Es werden Benachrichtigungen generiert, falls Sicherheitsrichtlinien verletzt wurden.
7.1.2 Beschäftigungs- und Vertragsbedingungen	Splunk hilft bei der Führung einer Liste von Mitarbeitern und Auftragnehmern, die eine Geheimhaltungs- oder Vertraulichkeitsvereinbarung (NDA) unterzeichnet haben und korreliert diese mit Zugriffsprotokollen vertraulicher Informationen. Wenn ein nicht autorisierter Benutzer auf vertrauliche Daten zugreift, kann eine Benachrichtigung ausgelöst werden. Für die Liste der Benutzer kann der automatische Abgleich mit jeder Art von Datenbank oder Anwendungs-API für das Rechts- oder Personalwesen konfiguriert werden. Auf diese Weise kann angezeigt werden, ob ein NDA oder eine Vertraulichkeitsvereinbarung unterzeichnet oder widerrufen wurde.
7.2.2 Informations-sicherheitsbewusstsein, -ausbildung und -schulung	Splunk kann für das Monitoring von E-Learning-Systemen eingesetzt werden, um die Einhaltung der Mitarbeiter-Compliance im Rahmen von Security-Awareness-Schulungen zu bestätigen. Es können weitere Aktionen als Reaktion festgelegt werden, um auf der Grundlage des Verhaltens zusätzliche Benutzerschulung zuzuweisen.
7.2.3 Reaktion auf Verletzungen der Sicherheitsvorgaben	Splunk unterstützt IT- und Sicherheitsteams dabei, Anfragen von Personal- oder Rechtsteams zu bearbeiten, wenn ein Mitarbeiter eine Verletzung der Informationssicherheit begangen hat. Sie können system- und netzwerkübergreifend forensische Untersuchungen durchführen, um den Mitarbeiter zu identifizieren und ggf. zu entlasten, sollte das technische Benutzerkonto offengelegt oder manipuliert worden sein.
7.2.3 Maßregelungsprozess	Durch Erstellen von Verhaltensberichten ermöglicht Splunk dem IT-Sicherheits-Managementteam, Anerkennungen oder Anreize für gutes Verhalten im Hinblick auf Informationssicherheit festzulegen. Es kann beispielsweise festgestellt werden, welche Mitarbeiter besonders häufig Kennwörter ändern oder dem IT-Sicherheitspostfach die meisten Phishing-E-Mails melden.
8.1.1 Inventarisierung der Werte	Splunk unterstützt Teams dabei, Bestandslisten aus mehreren Systemen abzurufen, sie auf Genauigkeit zu vergleichen, fehlende Bestände zu bestimmen und zu aktualisieren. Beispielsweise könnten sie eine Liste aus der CMDB-Datenbank extrahieren, die mit dem Bestand in Active Directory synchronisiert, vom Schwachstellen-Scanner untersucht und mit DHCP-Anforderungen und den Einträgen im Endpoint Protection Management System abgeglichen werden kann.
8.1.2 Zuständigkeit für Werte	Splunk ermöglicht Teams das Führen einer Bestandsliste in Splunk Enterprise Security, die den Besitzer eines Postens/einer Ressource nebst einer Klassifizierung und Anmerkungen zu eventuellem regelmäßigem Aktualisierungsbedarf beinhaltet. Dem Besitzer des Postens/der Ressource kann ein individuelles Dashboard zur Verfügung gestellt werden, mit dem Informationssicherheit skalierbar und leichter verständlich wird.
8.1.4 Rückgabe von Werten	Während des Entlassungszeitraums eines Mitarbeiters oder bei nahendem Vertragsende eines Auftragnehmers sollte ein Unternehmen jede Form von unberechtigtem Kopieren wertvoller Informationen streng überwachen. Splunk kann Benutzer auf eine Überwachungsliste setzen und sie mit unbefugten Kopierereignissen, wie Uploads auf Speicherplattformen im Web (z. B. Google Drive oder Dropbox), dem Senden von E-Mails an private E-Mail-Domänen (@gmail.com) oder der Nutzung von Wechselmedien, korrelieren. Darüber hinaus kann der historische Verlauf forensisch untersucht werden, um jede Form unbefugter Kopien wichtiger Informationen zu identifizieren, bevor das Anstellungsverhältnis eines Mitarbeiters endet.

ISO 27002-Kernbereiche	So unterstützen Maschinendaten und Splunk
8.3.1 Handhabung von Wechseldatenträgern	Splunk ermöglicht Unternehmen Daten entweder direkt von Endpunkten oder durch Drittanbieter-Schutz-Tools (etwa für Gerätesteuerung/Data Loss Prevention) zu erfassen. Das Kopieren von Daten auf Wechseldatenträger kann überwacht und außerdem als forensischer Beweis gespeichert werden. Mithilfe der eindeutigen Geräteidentifikation von Wechseldatenträgern können potenzielle Infektionen mit Schadsoftware aufgedeckt werden, indem etwa überprüft wird, an welche weiteren Geräte ein bestimmter USB-Stick in der Unternehmensumgebung angeschlossen war. Ferner kann die Gesamtnutzung des USB-Sticks nachverfolgt werden, was im Fall von Mehrfachverwendung einen Hinweis auf Schulungsbedarf der Mitarbeiter im Hinblick auf das Sicherheitsbewusstsein darstellen kann.
8.3.2 Entsorgung von Datenträgern	Splunk unterstützt Unternehmen beim Monitoring und dem Führen eines Audit-Trails für einen Lösch-PC mit geeigneter Löschsoftware, der von IT-Teams zum Überschreiben von Medien per standardisierten Verfahren verwendet wird.
8.3.3 Transport von Datenträgern	Siehe Punkt 8.3.1f zum Überprüfen und Beweisen, ob bzw. dass verschlüsselte Daten auf Wechseldatenträgern gespeichert wurden.
9.1.1 Zugangssteuerungs-richtlinie	Splunk ermöglicht Benutzern das Abrufen von Zugriffssteuerungslisten von Systemen mithilfe von Suchbefehlen oder technischen Add-Ons von Drittanbietern. Snapshots dieser Informationen werden gespeichert und dem zuständigen Besitzer der Informationen auf Dashboards angezeigt. Beispielsweise kann mit dem Splunk-Befehl "sa-ldap search" eine Liste der Mitglieder in einer Gruppe, die zum Zugriff auf geheime Informationen berechtigt sind, abgerufen und gespeichert werden und in dieser Form als Grundlage für Berichte dienen. Dies kann geplant und regelmäßig ausgeführt werden, um die Konfiguration jederzeit aufrecht zu erhalten und auditieren zu können.
9.1.1 Zugriffssteuerungs-Richtlinie	Splunk ermöglicht Benutzern das Erfassen von Audit-Logs von jeder Anwendung und jedem Authentifizierungs- oder Identitätsmanagementsystem, einschließlich der durchgeführten Verwaltungsaktivitäten.
9.1.2 Zugang zu Netzwerken und Netzwerkdiensten	Splunk ermöglicht Benutzern beim Zugriff auf ein Netzwerk oder einen Netzwerksservice das Führen eines vollständigen Audit-Trails jeder beteiligten Komponente. Splunk hilft Unternehmen beim Monitoring der Nutzung von Netzwerkservices. Damit lassen sich Fragen wie diese beantworten: Wer hat wann in welcher Weise worauf zugegriffen. Administratoren können dann eine Benachrichtigung senden, wenn eine Aktivität nicht im Rahmen der Unternehmensrichtlinien lag.
9.2.1 Benutzerregistrierung und deren Aufhebung	Splunk hilft Unternehmen beim Führen eines Audit-Trails über Benutzeraktivitäten, mit dem sie für ihre Aktivitäten zur Verantwortung gezogen werden können. Praktiken wie die gemeinsame Nutzung von Benutzerkonten können ohne weitere Konfiguration mit den Korrelationssuchen von Splunk Enterprise Security aufgedeckt werden. Für Ausnahmen können Genehmigungslisten verwendet werden.
9.2.1 Registrierung und Deregistrierung von Benutzern	Splunk kann mehr als Unternehmen einfach nur zu ermöglichen, Audit-Trails deaktivierter oder entfernter Benutzerkonten zu führen. Splunk kann darüber hinaus Informationen über scheidende Mitarbeiter direkt aus einer HR-Anwendung oder einem Ticket-System anreichern und im Falle fehlender oder fehlgeschlagener technischer Prozesse auf einem der vielen Systeme, auf denen die Registrierung eines Benutzerkontos aufgehoben werden muss, hinweisen.
9.2.2 Zuteilung von Benutzerzugängen	Splunk ermöglicht Benutzern das Erfassen von Event Log-Daten von einem Autorisierungssystem zusammen mit der Meldung, welcher Administrator einer bestimmten Benutzer-ID den Zugriff auf ein bestimmtes Informationssystem oder einen bestimmten Service erteilt hat.
9.2.3 Verwaltung privilegierter Zugangsrechte	Splunk kann Änderungen an Berechtigungen und Änderungen an Metriken sowie die Heraufsetzung von Zugriffsrechten überwachen.
9.2.4 Verwaltung geheimer Authentisierungsinformation von Benutzern	Splunk kann die erstmalige Verwendung von Benutzerkonten nachverfolgen und überwachen, einschließlich der Prüfung, ob ein Standardkennwort geändert wurde.

ISO 27002-Kernbereiche	So unterstützen Maschinendaten und Splunk
9.2.5 Überprüfung von Benutzerzugangsrechten	Splunk kann Meldungen zu Benutzerzugriffsrechten bei Anwendungen und Services abfragen und einen automatisierten Bericht für den Asset-Besitzer erstellen. Darüber hinaus kann Splunk durch Vergleich mit einer früheren Berichtsüberprüfung auf jede Änderung an den Benutzerattributen hinweisen.
9.2.5 Überprüfung von Benutzerzugangsrechten	Splunk kann Änderungen an vertraulichen Konten erfassen und melden und die regelmäßige Überprüfung eines Berichts bzw. den regelmäßigen Zugriff darauf durch eigenes Auditing von Splunk dokumentieren.
9.2.6 Entzug oder Anpassung von Zugangsrechten	Splunk kann die Entziehung oder Änderung von Zugriffsrechten überwachen, beispielsweise wenn ein Mitarbeiter in eine andere Abteilung versetzt wird oder ausscheidet. Wenn ein Benutzer hinzugefügt oder entfernt wird, kann Splunk den IT-Betrieb über die Änderung informieren, damit dieser überprüfen kann, ob sie autorisiert wurde.
9.4.2 Sichere Anmeldeverfahren	Splunk unterstützt sowohl beim Monitoring und Reporting von Zwei-Faktor-Authentifizierungs-systemen, beim Monitoring von SSO-Lösungen (Single-Sign-On, einmaliges Anmelden), beim Abfragen von Identitätsanbietern als auch beim Aufzeichnen von Authentifizierungssystemen im Netzwerk.
9.4.2 Sichere Anmeldeverfahren	Splunk ermöglicht Unternehmen das Erfassen von fehlgeschlagenen und erfolgreichen Anmeldeversuchen bei nahezu jeder Art von Anwendung, Service oder System.
9.4.2 Sichere Anmeldeverfahren	Splunk kann Brute-Force-Aktivitäten durch verschiedene Analysemethoden erkennen. Diese reichen von einfachem Zählen über Baselining bis hin zu Machine Learning – einschließlich der Erkennung langsamer Versuche.
9.4.4 Gebrauch von Hilfsprogrammen mit privilegierten Rechten	Die Verwendung von System-Dienstprogrammen kann mit Splunk überwacht und korreliert werden. Es sind erweiterte Erkennungsmechanismen wie die dynamische Peergruppenanalyse/-klassifikation sowie die Messung der Länge von Befehlszeileneinträgen verfügbar.
9.4.5 Zugangssteuerung für Quellcode von Programmen	Splunk kann softwarebasierte Check-In-Systeme auf Zugriff und Trennung zwischen Entwicklungs- und QS-Teams überwachen.
10.1.2 Schlüsselverwaltung	Splunk kann Public-Key-Infrastruktur (PKI) und HSM-Crypto-Appliances überwachen, einschließlich Schlüsselgenerierung, Exportvorgängen, Registrierungen, Überprüfungen oder Aberkennung.
11.1.2 Physische Zutrittssteuerung	Splunk kann für das Monitoring des physischen Zugangs zu Einrichtungen verwendet werden und festgelegte Zugangsmuster auf unbefugten Zugang hin überwachen. Daten aus Active Directory, physische Zugangsdaten und VPN-Daten können korreliert werden, um zu bestimmen, ob sich ein Benutzer durch "Dranhängen" Zugang zum Gebäude verschafft hat.
11.2.1 Platzierung und Schutz von Geräten und Betriebsmitteln	Splunk kann Daten in nahezu jedem Format akzeptieren, einschließlich Daten der HKL-Systeme von Gebäuden, um Temperaturänderungen zu messen und damit verbundene physische Bedrohungen zu überwachen. Splunk kann ebenso Daten von RFID-Systemen und GPS-Informationen akzeptieren und monitoren, sodass es die Verwendung von (mit RFID oder GPS markierten) Firmenfahrzeugen oder -geräten zum Schutz vor Diebstahl überwachen und nachverfolgen kann.
11.2.2 Versorgungs-einrichtungen	Splunk kann jede Art von Sensordaten oder Sicherheitsbenachrichtigungen von Gebäudeeinrichtungen erfassen und IT-Teams darüber informieren, statt die Transparenz auf das Gebäudemanagement zu beschränken.
11.2.8 Unbeaufsichtigte Benutzergeräte	Splunk kann auf Inaktivität von Hosts prüfen und Daten überwachen, die beispielsweise darauf hinweisen, dass ein kennwortgeschützter Bildschirmschoner aktiv ist oder nicht innerhalb einer bestimmten Zeitspanne gestartet wird.

ISO 27002-Kernbereiche	So unterstützen Maschinendaten und Splunk
12.1.1 Dokumentierte Betriebsabläufe	Splunk ermöglicht Organisationen den Aufbau einer Plattform für Maschinendaten, um gleiche Verfahren und Tools für nahezu jede Art von Anwendungsfall zu verwenden. Die Software ermöglicht es Benutzern, für die Bedürfnisse verschiedener Teams unterschiedliche Fragen an die gleichen Daten zu stellen. Dadurch können Teams das gleiche Tool (und die gleichen Daten) für Sicherheitsuntersuchungen, Sicherheitsmonitoring, Compliance-Überprüfung, Bedrohungserkennung, End-to-End-Monitoring von Services und weitere Anwendungsfälle aus den Bereichen SIEM und IT Ops verwenden.
12.1.2 Änderungssteuerung	Splunk kann für das Monitoring von Änderungen an Systemen, des Zeitpunkts ihrer Durchführung, der beteiligten Person(en) und der ausschlaggebenden Gründe verwendet werden. Dies ist nützlich, wenn es darum geht, Notfallsituationen zu verfolgen und mit geplanten Ausfallzeiten für bestimmte Systeme zu vergleichen. Das Risiko kann anhand der Anzahl unbefugter Änderungen bewertet und im zeitlichen Ablauf nachverfolgt werden, um das zunehmende oder abnehmende Risikoniveau für das Unternehmen zu dokumentieren. Die Korrelierung mit Change Management Tickets kann ebenfalls durchgeführt werden.
12.1.3 Kapazitätssteuerung	Splunk kann die CPU-Nutzung und weitere hardwarebezogene Leistungsinformationen innerhalb einer physischen oder virtuellen Infrastruktur überwachen. Es kann Schwellenwerte im zeitlichen Verlauf überwachen, um ein Nachlassen der Leistung frühzeitig zu prognostizieren und zu erkennen. Teilausfälle der Hardware, etwa ein Lüfterausfall oder Speicherfehler, können erkannt und überwacht werden, um die Ressourcenplanung und Entscheidungen zur Hardwarebeschaffung zu unterstützen. Services können bezüglich der Transaktionsleistung über die gesamte IT-Architektur hinweg überwacht werden. Diese Daten können eine Informationsquelle für Untersuchungen der Service Delivery-Architektur darstellen und Metriken zur Kundenzufriedenheit verbessern. Splunk unterstützt Benchmarking für normale Leistung und Warnmeldungen zu allen Teilen des IP-Stacks.
12.1.4 Trennung von Entwicklungs-, Test- und Betriebsumgebungen	Splunk erlaubt den Zugriff auf Logs von Produktionssystemen, um Problembehandlung zu ermöglichen, ohne dass eine Anmeldung bei Produktionssystemen erforderlich wäre. Dies ist eine wichtige Auditanforderungen und verhindert unbefugte Änderungen an Systemen.
12.2.1 Maßnahmen gegen Schadsoftware	Splunk unterstützt die Erfassung von Bestandsinformationen, beispielsweise welche Pakete oder Anwendungen installiert und bereitgestellt wurden. Die Informationen können regelmäßig aktualisiert, und alle Änderungen können gemeldet werden. Splunk hilft bei der Suche nach „bekannten“ und „unbekannten“ Bedrohungen. Splunk überwacht alle Aspekte der Anti-Viren-Bereitstellung, Hostkonfiguration, E-Mail-Sicherheit, Web-Sicherheitsprodukten und Firewalls der nächsten Generation. Diese stellen bekannte Bedrohungen dar, die von signatur- und regelbasierten Systemen gemeldet werden. Splunk kann diese Daten um DNS, DHCP, physische Zugriffsdaten, Logdaten aus Active Directory, Paketerfassungsdaten und Flow Data ergänzen. Die Suche nach zeitbasierten Mustern, die Daten zur Geolokalisierung beinhalten, kann böswillige Insider und hartnäckige Schadsoftware identifizieren. Die Sicherheit kann sich stärker an das Unternehmen anpassen, indem sie sich auf die wichtigsten Datenbestände des Unternehmens konzentriert.
12.2.1 Maßnahmen gegen Schadsoftware	Splunk hilft bei der Erkennung bösartiger Websites, indem es den Datenverkehr von Firewalls oder Webproxys mit Bedrohungsinformationen aus von Drittanbietern gewonnenen URLs korreliert. Splunk kann außerdem Blacklistings- und Vorbeugungs-Events aus bereitgestellten Sicherheits-Appliances melden.
12.2.1 Maßnahmen gegen Schadsoftware	Splunk erlaubt den Zugriff auf Systemlogs, um die Behandlung von Problemen zu ermöglichen, ohne dass eine Anmeldung bei Produktionssystemen erforderlich wäre. Splunk hilft außerdem bei der Überwachung des Malware-Schutzes, generiert Berichte dazu und unterstützt den Wiederherstellungsprozess mithilfe automatisierter Reaktionen wie einer Quarantänisierung des Hosts (Verschiebung in ein VLAN), der Überprüfung, ob eine Bereinigung erfolgreich war und der Sicherstellung, dass bei einem bereinigten Host keine weiteren Anzeichen von Manipulation oder ungewöhnlichem Netzwerkverhalten mehr zu beobachten sind.

ISO 27002-Kernbereiche	So unterstützen Maschinendaten und Splunk
12.2.1 Maßnahmen gegen Schadsoftware	Splunk liefert mithilfe seiner Community und des Splunk Security Research Teams fortlaufend aktualisierte Informationen über neue Bedrohungstaktiken und -techniken, die Erkennung derselbigen und die Reaktion auf sie.
12.3.1 Sicherung von Information	Splunk kann Lösungen zur Datensicherung leicht auf Leistung, Datenintegrität sowie den Datenzugriff auf Sicherungen überwachen.
12.4.1 Ereignisprotokollierung	Splunk kann Sicherheitssysteme auf Konfigurationsänderungen hin in Änderungsfenstern ebenso überwachen wie das Benutzerverhalten. Splunk kann darüber hinaus einen zuverlässigen Nachweis für Compliance-Audits liefern.
12.4.1 Ereignisprotokollierung	Splunk erfasst jede Art von Logdaten, erkennt ob Informationen fehlen, und kann die Daten durch Nachschlagen in verschiedenen Quellen anreichern. Splunk kann auch automatisch einen Zeitstempel hinzufügen und aufzeichnen, von welchem Host das Event Log stammt, falls Metainformationen fehlen.
12.4.1 Ereignisprotokollierung	Splunk erlaubt verschiedene Arten und Verfahren der Anonymisierung und Pseudonymisierung. Von der reinen Präsentationsschicht bis hinunter zu unbearbeiteten Logs, die auf Datenträgern gespeichert sind, ganz nach den Anforderungen des Unternehmens.
12.4.1 Ereignisprotokollierung	Standardmäßig ist Splunk so konfiguriert, dass nichts über die Benutzeroberfläche gelöscht oder geändert werden kann. Es können Warnmeldungen konfiguriert werden, für den Fall, dass Datenquellen das Senden von Event Logs einstellen oder eine Änderung der Richtlinie zur Logerstellung konfiguriert wurde.
12.4.2 Schutz der Protokollinformation	Splunks Benutzerrollenkonzept mit seiner starken Benutzerauthentifizierung stellt sicher, dass nur autorisierte Benutzer mit Event Logdaten arbeiten können. Die Unverfälschtheit kann durch eine Datenintegritätsfunktion nachgewiesen werden, die jeden Teil neu indizierter Rohdaten hasht und in eine Hash-Datei schreibt, die ihrerseits geschützt werden kann. Das Entfernen von Log Events wird in einem internen Audit Log dokumentiert, und das Verhalten beim Erreichen der maximalen Speicherkapazität kann konfiguriert werden.
12.4.2 Schutz der Protokollinformation	Splunk kann als zentrale Plattform eingerichtet werden, die Daten entweder an eine weitere Splunk-Lösung weiterleiten oder ihrerseits als das externe System fungieren kann.
12.4.3 Administratoren- und Bedienerprotokolle	Splunk überwacht alle Benutzeraktivitäten und stellt ein vollständiges Log der Aktivitäten zur Verfügung.
12.4.4 Uhrensynchronisation	Splunk kann Systeme überwachen, um sicherzustellen, dass sie mithilfe des Network Time Protocol (NTP) synchronisiert sind. Splunk erkennt darüber hinaus jede größere Zeitdifferenz in den Zeitstempeln von Datenquellen.
12.5.1 Installation von Software auf Systemen im Betrieb	Splunk kann den Zugriff, die Konfiguration und die Leistung von betrieblicher Software überwachen.
12.6.1 Handhabung von technischen Schwachstellen	Splunk kann die "Halbwertszeit" von Schwachstellen in IT-Architekturen überwachen und sie als Leistungskennzahl für das Patchen von Systemen melden. Die Daten gefährdeter Systeme können mit IDS/IPS-Angriffsdaten korreliert werden, um Versuche zur Ausnutzung gefährdeter Systeme zu identifizieren.
12.6.1 Handhabung von technischen Schwachstellen	Relevante Events können je System und je Schwachstelle erfasst und nachverfolgt werden, bis das Problem behoben, mit einem Patch versorgt oder entfernt ist.

ISO 27002-Kernbereiche	So unterstützen Maschinendaten und Splunk
12.6.1 Handhabung von technischen Schwachstellen	Splunk bietet sofort einsatzbereite, out-of-the-box Dashboards, um anfällige Vorgänge zu dokumentieren, etwa durch Aufzeichnen von Scans und Erfassen von Hosts, die zuvor noch nicht gescannt wurden.
13.1.1 Netzwerksteuerungs-maßnahmen	Splunk unterstützt rollenbasierte Zugriffskontrollen für verschiedene Netzwerkteams. Splunk kann die Protokolle HTTP, HTTPS, SSL VPN sowie Protokolle der Anwendungs-schicht von AppFlow oder andere Load Balancing-Daten überwachen. Splunk kann darüber hinaus Metriken bezüglich Konfigurationsänderungen, Netzwerk- sowie Netzwerkhardware-Leistung zur Verfügung stellen. Splunk kann Logdaten verwenden, um Daten während der Übertragung auf Unverfälschtheit zu überwachen.
13.1.3 Trennung in Netzwerken	Splunk kann den Datenverkehr zwischen Netzwerken überwachen und nach Datenverkehr Ausschau halten, der für Netzwerktrennung unzulässig ist.
14.2.6 Sichere Entwicklungsumgebung	Splunk kann alle Änderungen an Entwicklungsumgebungen oder dem darin enthaltenen Codespeicher überwachen.
14.3.1 Schutz von Testdaten	Splunk kann einen vollständigen Audit-Trail des Zugriffs auf Testdaten zur Verfügung stellen.
15.1.1 Informationssicherheits-richtlinie für Lieferantenbeziehungen	Splunk kann den von einem Lieferanten verwendeten Zugangskanal überwachen und alle ausgeführten Aktivitäten dokumentieren.
15.1.2 Behandlung von Sicherheit in Lieferantenvereinbarungen	Splunk fungiert als zentrale Plattform, auf der zum Zweck der Unterstützung und Zusammenarbeit Zugriff auf alle Incidents mit Drittquellen erteilt werden kann. Splunk kann vom Lieferanten zum Bereitstellen von Compliance-Berichten und zum Nachweis der Wirksamkeit von Kontrollen verwendet werden.
15.2.1 Überwachung und Überprüfung von Lieferantendienstleistungen	Wenn ein Unternehmen Zugriff auf Logdaten von seinem Serviceanbieter besitzt, können SLAs mithilfe von Splunk überwacht werden. Ferner kann der Lebenszyklus von Daten, die von Dritten gehostet werden, bis zur Entsorgung überwacht werden. Trends im zeitlichen Verlauf von SLAs können verfolgt werden, um Entscheidungen zum Erwerb von Services zu stützen.
16.1.1 Verantwortlichkeiten und Verfahren	Splunk hilft Sicherheitsteams, schnell, effektiv und geordnet auf Incidents bei der Informationssicherheit zu reagieren und dem Management Feedback über den Umfang und die möglichen Auswirkungen zu geben. Aktivitäten zum Incident-Management können innerhalb von Splunk protokolliert und auf einer Zeitachse angeordnet werden.
16.1.1 Verantwortlichkeiten und Verfahren	Splunk unterstützt Incident Response-Teams bei der schnellen Erfassung von Daten und dem Teilen von Informationen über Incidents mit externen Organisationen, sofern angebracht.
16.1.2 Meldung von Informationssicherheits-ereignissen	Splunk Enterprise Security bietet Management, Benachrichtigung und Berichterstellung für Sicherheits-Events (Security Event Management Alerting and Reporting).
16.1.4 Beurteilung von und Entscheidung über Informationssicherheits-ereignisse	Splunk verhilft Teams zu einer Plattform für die Untersuchung von Sicherheits-Events, auf der sie bewerten können, ob Vorfälle als Informationssicherheits-Incidents klassifiziert werden sollen. Mit Splunk besitzen Incident Response-Teams für Informationssicherheit die Möglichkeit, diese Entscheidungen zu treffen.

ISO 27002-Kernbereiche	So unterstützen Maschinendaten und Splunk
16.1.5 Reaktion auf Informationssicherheits-vorfälle	Splunk bietet die Funktionalität, Incidents nicht nur zu erkennen und zu untersuchen, sondern ermöglicht darüber hinaus das Dokumentieren der Reaktionen in Playbooks für die automatische Ausführung oder die Orchestrierung mit einem Audit-Trail zur späteren Analyse.
16.1.5 Reaktion auf Informationssicherheits-vorfälle	Splunk ermöglicht Benutzern, zurückzublicken und riesige Mengen an Maschinendaten aus potenziell hunderten von verschiedenen Technologien zu identifizieren, um die Quelle eines Incidents für eine Post-Incident-Analyse zu bestimmen.
16.1.6 Erkenntnisse aus Informationssicherheits-vorfällen	Splunk Enterprise Security stellt eine vollständige Aufzeichnung der Incident-Klassifizierung und Besitzwechsel einschließlich sämtlicher Kommentaraufzeichnungen zur Verfügung.
16.1.7 Sammeln von Beweismaterial	Splunk speichert die ursprünglichen, unbearbeiteten Logs, die von beliebigen Geräten oder Anwendungen generiert wurden und kann mittels Durchführung von Event-Hashing beweisen, dass keine Manipulationen stattgefunden haben.
18.1.2 Geistige Eigentumsrechte	Splunk kann verwendet werden, um installierte Software zu melden oder die Lizenznutzung dort zu überwachen, wo keine technische Umsetzung besteht und auf bevorstehende Lizenzverstöße aufmerksam machen. Splunk kann außerdem dazu verwendet werden, eventuell unbenutzte Lizenzen zu identifizieren, um sie wieder in den Lizenzpool einer Organisation einzugliedern.
18.1.3 Schutz von Aufzeichnungen	Splunk schützt Aufzeichnungen durch Clustering und Konzepte für Hochverfügbarkeit, die Unterstützung von WORM-Laufwerken und Dateihashs.
18.1.3 Schutz von Aufzeichnungen	Splunk lässt verschiedene Speichersysteme für Aufzeichnungen zu und ermöglicht Dateihashs ebenso wie die Definition von Log-Aufbewahrungszeiten und Log-Rotation.
18.2.2 Einhaltung von Sicherheitsrichtlinien und -standards	Splunk ermöglicht die Erstellung dynamischer Dashboards, Berichte und Warnungen durch Manager, um den regelmäßigen Überprüfungsprozess zu automatisieren und zu beschleunigen.
18.2.3 Überprüfung der Einhaltung von technischen Vorgaben	Splunk ermöglicht Organisationen, die Überprüfung ähnlicher Systeme zu automatisieren, indem die Informationen über das, nach dem gesucht werden muss, von einer fachkundigen, autorisierten Person erfasst werden. Splunk kann darüber hinaus relevante Messpunkte erfassen und durchgängiges, fortlaufendes Monitoring für Anwendungen des gleichen Typs einrichten, um Konsistenz und Zeitersparnis bei zugleich erhöhter Sicherheit zu erreichen.