elastic

Nutzung von Elastic zur Unterstützung Ihrer Datensicherheits-Compliance

Zusammenfassung

Da die Bedrohungslandschaft der Cybersicherheit immer komplexer wird – mit Cyberangriffen, die immer häufiger, gezielter, unauffälliger und technisch fortschrittlicher werden – war die Notwendigkeit einer robusten und umfassenden Datensicherheit wichtiger denn je. Die rechtlichen Anforderungen und potenziellen Haftungsrisiken im Bereich der Cybersicherheit werden ebenfalls immer komplexer und anspruchsvoller, sodass ein risikobasierter Sicherheitsansatz unbedingt erforderlich ist.

Um mit der ständig wachsenden Liste sicherheitsrelevanter regulatorischer Anforderungen Schritt zu halten, potenziell katastrophale Geschäftsunterbrechungen zu verhindern und sich vor dem Risiko kostspieliger Rechtsstreitigkeiten aufgrund von Sicherheitsverstößen zu schützen, sollten Unternehmen einen ganzheitlichen, strategischen Ansatz für Cybersicherheit verfolgen. Andernfalls drohen den Unternehmen nicht nur erhebliche rechtliche und finanzielle Konsequenzen, sondern auch irreparable Betriebs- und Reputationsschäden.

In diesem Whitepaper erfahren Sie, wie Unternehmen mit Elastic ihre Sicherheitsverpflichtungen erfüllen und eine wahrhaft widerstandsfähige Verteidigung gegen Cyberbedrohungen aufbauen können. Die leistungsstarke, flexible und skalierbare Lösung von Elastic unterstützt Unternehmen bei der Erfüllung vielfältiger und vielschichtiger Anforderungen an Compliance und operative Cybersicherheit. Dazu gehören:

- Erhöhte Sichtbarkeit und Durchsuchbarkeit von Daten über Angriffsoberflächen hinweg
- Vereinfachte Datenabfragen für Compliance-Anfragen
- Optimierte Erkennung und Automatisierung zur Behebung von Bedrohungen
- Überwachung und Darstellung Ihrer Sicherheitslage
- Angereicherte Bedrohungsinformationen

Im Folgenden bieten wir einen Überblick über grundlegende Sicherheitskonzepte, die in allen rechtlichen Frameworks üblich sind, untersuchen die möglichen Folgen einer nicht risikobasierten und nicht konformen Umsetzung dieser Konzepte und veranschaulichen, wie Unternehmen die Plattform und Lösungen von Elastic zur Erfüllung ihrer Compliance-Verpflichtungen und Minimierung von Sicherheitsrisiken nutzen können.

Bitte beachten Sie: *Dieses Whitepaper dient ausschließlich Informationszwecken und stellt keine Rechtsberatung dar. Bitte konsultieren Sie Ihren Rechtsberater, um rechtlichen Rat einzuholen.*

Grundlegende Sicherheitsprinzipien und damit verbundene Compliance-Verpflichtungen

Die moderne Sicherheits-Compliance-Landschaft besteht aus einem Flickenteppich aus jurisdiktionsspezifischen, branchenspezifischen und datenspezifischen Anforderungen. Die Verantwortlichkeiten der Unternehmen unterscheiden sich daher je nach Standort, Geschäftstätigkeit, Art der verarbeiteten Daten und Art der Verarbeitung, einschließlich der Vertraulichkeit dieser Daten und der Art der Geschäftstätigkeit.

Beispielsweise könnte ein globales Finanzinstitut gleichzeitig dem US-amerikanischen Bundesgesetz Gramm-Leach-Bliley Act („GLBA“), der Verordnung zur Cybersicherheit des New York Department of Financial Services („NYDFS“), dem Digital Operational Resilience Act der EU („DORA“) und der zweiten Richtlinie zur Sicherung von Netz-und Informationssystemen der EU („NIS2-Richtlinie“) unterliegen.

Ein börsennotierter Einzelhändler mit Sitz in den USA hingegen unterliegt möglicherweise einer Reihe anderer Anforderungen, wie beispielsweise dem Payment Card Industry Data Security Standard („PCI-DSS“) für die Sicherheit von Zahlungskarten, dem Sarbanes-Oxley Act of 2002 („SOX“) für die Verlässlichkeit der Berichterstattung und den US-amerikanischen Gesetzen zur Meldung von Datenschutzverletzungen. Natürlich dürfen dabei auch die Datenschutzgesetze und ihre Anforderungen an die Informationssicherheit zum Schutz personenbezogener Daten nicht vergessen werden.

Zusätzlich zu diesen verbindlichen Anforderungen verfügen viele Unternehmen auch über freiwillige Zertifizierungen nach verschiedenen Sicherheitsstandards von Drittanbietern, wie beispielsweise ISO 27001, SOC 2, NIST CSF oder UK Cyber Essentials.

Trotz dieser Unterschiede stimmen gesetzliche, regulatorische, selbstregulatorische und branchenbezogene Frameworks – sowie allgemeine Best Practices für die Sicherheit — weitgehend mit einer Reihe grundlegender Sicherheitsprinzipien überein. Im Folgenden gehen wir auf die wichtigsten Aspekte dieser Grundsätze ein und zeigen anhand von Beispielen auf, wie sie mit verschiedenen Frameworks in Einklang stehen.

Inventarisierung, Mapping und Klassifizierung von Daten

Unternehmen können keine risikobasierten Sicherheitskontrollen einsetzen, ohne zuvor zu verstehen, über welche Daten sie verfügen (ein Prozess, der als Daten-Inventarisierung bezeichnet wird), wo diese Daten gespeichert sind (Daten-Mapping) und wie sensibel diese Daten sind (Datenklassifizierung).

Diese Prozesse sind auch im Falle einer Datenschutzverletzung von entscheidender Bedeutung, damit Unternehmen besser einschätzen können, ob die betroffenen Daten gesetzliche, behördliche oder vertragliche Meldepflichten auslösen. Aus diesen Gründen sind die Inventarisierung, das Mapping und die Klassifizierung von Daten entweder explizit erforderlich oder eine notwendige Voraussetzung für die Einhaltung mehrerer Frameworks. Zum Beispiel:

- Die *FTC-Schutzregel* (16 CFR § 314), die Anforderungen für bestimmte Finanzinstitute implementiert, die dem GLBA unterliegen, verlangt von betroffenen Finanzinstituten, die Vertraulichkeit von Kundendaten im Rahmen ihres Risikobewertungsprozesses zu identifizieren und zu bewerten.
- Die *HIPAA-Sicherheitsregel* (45 CFR § 164.308) verpflichtet ebenfalls die betroffenen Unternehmen zur Inventarisierung und zum Schutz elektronisch gespeicherter geschützter Gesundheitsdaten („ePHI“).
- Gemäß Artikel 30 der Datenschutz-Grundverordnung der EU („DSGVO“) müssen Unternehmen Aufzeichnungen über ihre Verarbeitungstätigkeiten führen, was faktisch eine Dateninventarisierung und ein Daten-Mapping erfordert, um die Einhaltung der Vorschriften nachzuweisen.
- Die Meldepflichten bei Datenschutzverletzungen in den einzelnen US-Bundesstaaten werden in der Regel nur dann ausgelöst, wenn bestimmte Arten sensibler personenbezogener Daten von Einwohnern dieses Bundesstaates kompromittiert wurden. Demnach müssen Unternehmen im Falle einer Datenschutzverletzung in der Lage sein, festzustellen, welche Kategorien von Daten in einem kompromittierten Datensatz enthalten sind.
- Frameworks wie NIST SP 800-53 und die CIS Controls betonen die Datenklassifizierung, um sicherzustellen, dass die Schutzmaßnahmen mit der Vertraulichkeit der Daten übereinstimmen. Durch die Einrichtung eines klaren Inventarisierungs- und Klassifizierungssystems können Unternehmen Zugriffskontrollen sicherer umsetzen, sensible Datenflüsse überwachen, regulatorische Verpflichtungen erfüllen und das Risiko unbefugter Offenlegungen reduzieren.

Rollenbasierte Zugriffssteuerungen

Rollenbasierte Zugriffssteuerungen („RBAC“) sind Maßnahmen, die sicherstellen sollen, dass Personen nur Zugriff auf die Systeme und Daten erhalten, die sie zur Erfüllung ihrer Aufgaben benötigen (ein Konzept, das auch als „Least-Privilege-Prinzip“ bekannt ist). Konsequent angewendete RBACs reduzieren das Risiko unbefugten Zugriffs durch böswillige Insider und können dazu beitragen, das Ausmaß eines Angriffs zu begrenzen. Viele rechtliche und branchenbezogene Frameworks verlangen ausdrücklich oder empfehlen nachdrücklich die RBAC:

- Gemäß der DSGVO der EU dürfen nur ordnungsgemäß befugte Personen mit einem Informationsbedarf auf personenbezogene Daten zugreifen. Die Verordnung geht sogar noch weiter und definiert den unbefugten Zugriff als einen Fall von Datenschutzverletzung.
- Die Standards zum Schutz personenbezogener Daten des Bundesstaates Massachusetts (201 CMR 17.04) verlangen von Unternehmen, die in Massachusetts geschäftlich tätig sind, die Implementierung sicherer Zugriffskontrollmaßnahmen, die den Zugriff auf Datensätze und Dateien mit sensiblen personenbezogenen Daten auf die Personen beschränken, die diese Informationen zur Erfüllung ihrer beruflichen Aufgaben benötigen.
- Die HIPAA-Sicherheitsregel schreibt vor, dass der Zugriff auf ePHI auf die Personen beschränkt sein muss, die einen legitimen Informationsbedarf haben.
- Artikel 9 Absatz 4 der EU-Verordnung DORA verpflichtet die betroffenen Finanzinstitute zur Implementierung von Richtlinien, die den physischen oder logischen Zugriff auf Vermögenswerte auf das für legitime und genehmigte Funktionen und Aktivitäten erforderliche Maß beschränken.
- Branchenstandards wie NIST SP 800-53, ISO/IEC 27001 und die CIS Controls (z. B. CIS Control 6) betonen ebenfalls RBAC als grundlegende Praxis für das Zugriffsmanagement.

Protokollierung und Überwachung

Sicherheitsereignis-Logs gehören zu den wichtigsten Ressourcen, die Unternehmen zur Erkennung von Sicherheitsvorfällen haben. Logs, die Informationen wie Datum und Uhrzeit des Zugriffs, durchgeführte Aktionen und den Nutzer, der diese Aktionen durchgeführt hat, enthalten, sind für die Überprüfung, ob der Systemzugriff autorisiert war, und für die Untersuchung potenzieller unbefugter Aktivitäten unerlässlich. Die Überwachung von Logs in Echtzeit oder nahezu in Echtzeit ist auch der Schlüssel zur rechtzeitigen Erkennung und Behebung von Bedrohungen.

Das Log-Management kann jedoch eine Herausforderung für Unternehmen mit komplexen, vielfältigen Systemen sein, die täglich große Mengen an Logs generieren können. Diese Unternehmen müssen sich auf technische Lösungen verlassen, um Protokolle effektiv zu aggregieren und auf ungewöhnliche Aktivitäten zu überwachen. Rechtliche und branchenspezifische Frameworks unterstreichen die Bedeutung der Protokollierung und Überwachung:

- Der Payment Card Industry Data Security Standard (PCI-DSS) verpflichtet alle Unternehmen, die Zahlungskartendaten speichern, übertragen oder verarbeiten, alle Zugriffe auf Systemkomponenten und Karteninhaberdaten zu protokollieren und zu überwachen.
- Die HIPAA-Sicherheitsregel schreibt Auditkontrollen vor, um Aktivitäten in Systemen, die ePHI enthalten, aufzuzeichnen und zu überprüfen.
- Gemäß Abschnitt 404 des Sarbanes-Oxley Act of 2002 sind die Geschäftsleitung und die Wirtschaftsprüfer verpflichtet, die Wirksamkeit der internen Kontrollen öffentlicher Unternehmen im Bereich der Finanzberichterstattung zu bewerten und darüber Bericht zu erstatten. Diese Wirtschaftsprüfer bewerten diese Kontrollen anhand von Frameworks wie COBIT, die ein Audit Logging der Nutzeraktivitäten, des Zugriffs auf Finanzsysteme und der Änderungen an Finanzdaten vorschreiben.
- Die Komponente „Detect“ des NIST CSF schreibt vor, dass Unternehmen Sicherheitsereignisse protokollieren und eine kontinuierliche Sicherheitsüberwachung aufrechterhalten sollten. Dies ist auch unerlässlich für die rechtzeitige Berichterstattung von Vorfällen, die beispielsweise gemäß Artikel 32 der DSGVO der EU, Artikel 23 der NIS-2-Richtlinie der EU oder Artikel 19 des DORA der EU meldepflichtig sind.

Erkennung der und Reaktion auf Angriffsversuche

Leider sind in der heutigen Bedrohungslandschaft alle Unternehmen potenzielle Ziele für Cyberangriffe. Unternehmen müssen Systeme zur Erkennung von Angriffsversuchen und Prozesse zur Reaktion auf Sicherheitsvorfälle für den unvermeidlichen Fall eines versuchten Angriffsversuchs pflegen. Diese Systeme sind wichtig, damit Unternehmen einen Angriff schnell erkennen und darauf reagieren können, bevor er zu einem schwerwiegenden Vorfall eskaliert. Allerdings sind Systeme zur Erkennung von Angriffsversuchen und Incident-Response-Prozesse selten sofort wirksam; vielmehr müssen Unternehmen eine Baseline der Aktivitäten festlegen und die Alerting-Kriterien an die individuellen Attribute des Unternehmens anpassen. Diese Anpassung erhöht die Genauigkeit von Alerts und hilft sicherzustellen, dass Vorfälle angemessen geprüft und entsprechend ihrer Kritikalität behandelt werden. Die Erkennung der und Reaktion auf Angriffsversuche ist ein zentraler Bestandteil zahlreicher rechtlicher und branchenspezifischer Frameworks:

- Die Gesetze zur Meldung von Datenschutzverletzungen auf Bundes-, Landes- und internationaler Ebene verlangen, dass Datenschutzverletzungen innerhalb bestimmter Fristen gemeldet werden müssen. Zwar wird häufig angenommen, dass die DSGVO die kürzeste Frist für die Meldung vorschreibt (innerhalb von 72 Stunden nach Feststellung, dass eine meldepflichtige Datenschutzverletzung vorliegt), doch ist zu beachten, dass gemäß DORA schwerwiegende Vorfälle im Zusammenhang mit Informations- und Kommunikationstechnologie („IKT“) innerhalb von vier Stunden nach ihrer Entdeckung gemeldet werden müssen.
- Gemäß Abschnitt 500.16 der Cybersicherheitsvorschriften der NYDFS müssen regulierte Unternehmen über Incident-Response-Pläne verfügen, um umgehend auf Cybersicherheitsvorfälle reagieren und diese beheben zu können.
- DORA verlangt außerdem von regulierten Finanzinstituten die Entwicklung umfassender Incident-Response-Pläne.
- Das NIST CSF schreibt vor, dass Unternehmen umfassende „Detect“- und „Respond“-Kontrollen einrichten müssen, um Sicherheitsvorfälle zu erkennen und darauf zu reagieren.

Die Kosten der Nichteinhaltung

Ohne die Implementierung konformer und wirksamer Sicherheitskontrollen können Unternehmen, ihre Führungskräfte und ihre Vorstände erheblichen rechtlichen, finanziellen und Reputationsrisiken ausgesetzt sein. Aus praktischer Sicht riskieren Unternehmen mit ineffektiven Monitoring-Tools oder -Prozessen einen längeren unbefugten Zugriff, der es einem Angreifer ermöglicht, das Unternehmen auszukundschaften und autorisierte Aktivitäten besser nachzuahmen, während gleichzeitig Daten offengelegt werden oder die Grundlage für einen Ransomware-Angriff geschaffen wird. Eine unvollständige Protokollierung kann es auch unmöglich machen, festzustellen, ob verdächtige oder unerwartete Aktivitäten autorisiert waren, was sowohl zu einer Über- als auch zu einer Untermeldung führen kann.

Im Falle einer Datenschutzverletzung oder eines Cybersicherheitsvorfalls können unzureichendes Mapping und unzureichende Inventarisierung von Daten zu Schwierigkeiten bei der Identifizierung der betroffenen Daten führen. Dadurch kann es zu Verzögerungen bei der Meldung an betroffene Parteien und Aufsichtsbehörden kommen. Diese Verzögerungen wiederum erhöhen den potenziellen Schaden für die Opfer, verstoßen gegen die vorgeschriebenen Meldefristen und verschärfen die unmittelbare Belastung durch Wiederherstellungs- und Sanierungsmaßnahmen durch zusätzliche Schadensersatzansprüche, behördliche Sanktionen und weitere Durchsetzungs- und Prozesskosten. Für Business-to-Business-Anbieter kann es auch schwieriger sein, festzustellen, welche Kunden von einem Vorfall betroffen waren.

Die Nichteinhaltung positiver Sicherheitsanforderungen, wie sie durch Datenschutzgesetze zum Schutz personenbezogener Daten vorgeschrieben sind, kann zu erheblichen Strafen, Geldstrafen und sonstiger rechtlicher Haftung führen. Alle Unternehmen sehen sich auch dem Risiko von Fahrlässigkeit, Vertragsbruch oder anderen Klagen (oft in Sammelklagen) von Klägern ausgesetzt, deren Informationen bei einem Vorfall kompromittiert wurden. Insbesondere räumt der California Consumer Privacy Act (CCPA) Klägern, deren sensible Daten aufgrund der mangelnden Einhaltung „angemessener“ Sicherheitsmaßnahmen durch ein Unternehmen offengelegt wurden, ein Klagerecht ein. Sanktionen und Schadensersatzforderungen im Rahmen der Vorschriften gemäß HIPAA, CCPA oder DSGVO der EU können schnell siebenstellige Beträge erreichen.

Abgesehen von direkten Strafen für Verstöße kann auch der Reputationsschaden durch mangelnde Sicherheit schwerwiegend sein. Unternehmen, die Opfer einer Sicherheitsverletzung werden oder Sicherheitsvorschriften nicht einhalten, können das Vertrauen ihrer Kunden verlieren, mit öffentlicher Kritik konfrontiert werden, erhebliche Betriebsstörungen erleiden und langfristige Auswirkungen auf ihren Markenwert hinnehmen müssen. Börsennotierte Unternehmen laufen auch Gefahr, dass der Aktienkurs infolge weithin bekannter Sicherheitslücken beeinträchtigt wird. Zu den Risiken gehören die Abwanderung von Kunden und mögliche Schadensersatzforderungen, wenn Kundendaten nicht angemessen geschützt werden, was zu Geschäfts- und Umsatzeinbußen führen kann. Angesichts dieser weitreichenden Konsequenzen sollten Unternehmen das Thema Sicherheit ernst nehmen, indem sie angemessen in die Erfüllung ihrer Compliance-Verpflichtungen investieren und Sicherheitsrisiken minimieren.

Nutzung von Elastic für die Compliance

Die Elasticsearch Platform ist die Grundlage für die beiden sofort einsatzbereiten Lösungen von Elastic, Elastic Observability und Elastic Security. Unternehmen können die offene und flexible Platform von Elastic nutzen, um ihre Compliance-Verpflichtungen zu erfüllen und wichtige Cybersicherheitsrisiken kanalübergreifend zu bewältigen. Vor allem aber sind die Lösungen von Elastic von Natur aus agil und skalierbar. Sie können auf einer Vielzahl von Systemen und Plattformen eingesetzt werden, um Daten zu erfassen, und ihre Suchfunktionen können für unzählige Anwendungsfälle genutzt werden. Im Folgenden finden Sie einige Beispiele dafür, wie Elastic zur Unterstützung grundlegender Prinzipien eines Sicherheitsprogramms eingesetzt werden kann:

Mapping und Klassifizierung von Daten

Elastic kann Maßnahmen für das Daten-Mapping unterstützen, indem es strukturierte und unstrukturierte Daten umgebungsübergreifend indexiert, sodass Unternehmen einen zentralen Überblick über die Arten und die Speicherorte ihrer Daten erhalten. Mithilfe von nutzerdefinierten Tags, Metadaten und Machine Learning kann Elastic bei der Identifizierung von Mustern in Daten (z. B. personenbezogene Daten, Finanzunterlagen, Systemprotokolle) unterstützen und so die Klassifizierung von Daten anhand ihrer Vertraulichkeit oder regulatorischer Verpflichtungen vereinfachen. Elastic ist zwar keine dedizierte Datenklassifizierungs-Engine, aber die leistungsstarken Such- und Analysefunktionen können in umfassendere Daten-Governance-Programme integriert werden, um Daten in Cloud- und On-Prem-Systemen zu verfolgen und zu inventarisieren.

Rollenbasierte Zugriffssteuerung (RBAC)

Obwohl Elastic kein RBAC-Tool ist, kann die Platform Logs in den Systemen eines Unternehmens ingestieren, um Lücken im Berechtigungsmanagement zu identifizieren. Unternehmen können Zugriffsmuster analysieren, um Systeme zu identifizieren, auf die Nutzergruppen möglicherweise Zugriff benötigen, und diese Informationen für die Zuweisung von Zugriffsrechten nutzen. Elastic unterstützt unsere Kunden auch bei der Erfassung von Gruppenzugriffsrichtlinien aus verschiedenen Systemen, sodass Unternehmen aus diesen Daten Berichte erstellen können, um die Durchsetzung von Zugriffsrechten bei Audits oder Compliance-Untersuchungen nachzuweisen. Und Elastic enthält integrierte RBAC-Features in den Schnittstellen Elastic Security und Kibana. Administratoren können Rollen festlegen, die den Nutzerzugriff auf bestimmte Indizes, Dashboards oder Aktionen (z. B. Anzeigen oder Bearbeiten) einschränken und damit das Least-Privilege-Prinzip unterstützen.

Protokollierung und Überwachung

Eine der größten Stärken von Elastic und einer der häufigsten Anwendungsfälle ist die Aggregation, Speicherung und Analyse von Logs im großen Maßstab. Mit Elastic Agent können Unternehmen Logs von Endpoints, Servern, Cloud-Diensten und Anwendungen erfassen. Diese Logs werden in Elasticsearch indiziert, was eine Analyse und Visualisierung in Echtzeit in Kibana ermöglicht. Elastic unterstützt die langfristige Speicherung von Logs, Alerting und die Erkennung von Anomalien und ist damit eine ideale Lösung für die Log-Aggregation und Sicherheitsüberwachung sowie ein effektives Tool für die Compliance-Berichterstattung. Die Observability-Suite bietet außerdem Monitoring der Anwendungsleistung (APM), Metriken und Uptime-Monitoring für eine ganzheitliche Transparenz der Infrastruktur.

Viele Vorschriften, wie beispielsweise M-21-31 für US-Bundesbehörden, verpflichten Unternehmen zur Speicherung von Logs für einen festgelegten Zeitraum. Die Datenstruktur von Elastic ermöglicht eine kosteneffiziente Speicherung der Daten, basierend auf der Häufigkeit und Geschwindigkeit des benötigten Zugriffs. Der Indexmodus „logsdb“ von Elasticsearch **reduziert den Speicherbedarf von Log-Daten um bis zu 65 %** und verbessert so Transparenz und Compliance, während alle Daten jederzeit für Analysen verfügbar bleiben.

Um nur ein Beispiel zu nennen: Die University of York hat ihr SIEM auf Elastic Security umgestellt, um die Cybersicherheitsfähigkeiten zu verbessern, die betriebliche Effizienz zu steigern und Kosten zu senken. Durch die Bereitstellung von etwa 9.000 Elastic Agents auf Servern, Desktops und Laptops sowie die Erfassung von Logs aus der Hybrid-Cloud-Infrastruktur der Universität, einschließlich Google Cloud, AWS, Azure und On-Prem-Servern, nimmt die Universität 500 Gigabyte Daten pro Tag auf, mit 35 Terabyte Logs im Speicher. Sie verbindet sich auch mit Sicherheitstools wie Palo Alto Networks Firewalls, Cloudflare und Duo, um eine umfassende, plattformübergreifende Überwachung zu gewährleisten. Diese Einrichtung ermöglicht schnelle Suchen in großen Datenmengen und reduziert die Abfragezeiten von Stunden auf Sekunden.

Erkennung der und Reaktion auf Angriffsversuche

Elastic Security umfasst Funktionen wie Endpoint Detection and Response (EDR) und integriert Bedrohungsinformationen zur Unterstützung der Angriffserkennung. Damit können Sicherheitsteams bekannte und unbekannte Bedrohungen mithilfe von Verhaltensanalysen, Angrifffsmapping und benutzerdefinierten Erkennungsregeln überwachen. Mit der zentralen Protokollierung können Analysten Ereignisse schnell systemübergreifend korrelieren, Alerts im Kontext untersuchen und Reaktions-Workflows orchestrieren. Elastic unterstützt auch automatisierte Reaktionen durch Integrationen mit SOAR-Plattformen (Security Orchestration, Automation and Response) von Drittanbietern und ist damit ein leistungsstarkes Tool zur Verbesserung der Bereitschaft für die Reaktion auf Vorfälle und der Bedrohungssuche. Dank dieser fortschrittlichen Funktionen wird die Wahrscheinlichkeit einer Sicherheitsverletzung verringert und die Reaktionszeit im Falle eines erfolgreichen Angriffs verkürzt, wodurch wiederum potenzielle rechtliche Haftungsrisiken im Zusammenhang mit einem Vorfall gemindert werden.

AHEAD, ein führender Anbieter digitaler Plattform- und Transformationslösungen hat seine Fähigkeiten zur Erkennung der und Reaktion auf Angriffsversuche durch die Integration von Elastic Security in seine Managed Security Services deutlich verbessert. AHEAD erfasst nun Kundensicherheitsdaten in Elastic, das auf der Elastic Cloud ausgeführt wird. Dort werden die Daten angereichert, aggregiert und mit Threat-Intelligence-Feeds verknüpft. Elastic dient auch als Datenquelle für das SOAR-System des Unternehmens. Die Sicherheitsanalysten von AHEAD können zudem KI-gestützte Alerts nutzen, die relevante Informationen innerhalb von Sicherheitsereignissen hervorheben. So wird die Zeit für das manuelle Durchsuchen riesiger Datenmengen reduziert und die Belastung durch falsch-positive Ergebnisse verringert.

Fazit

Da die Bedrohungslage im Bereich der Cybersicherheit weiterhin komplexe Herausforderungen für Unternehmen mit sich bringt, wird es auch immer schwieriger, die ständig wachsende Liste der regulatorischen Anforderungen in Bezug auf Sicherheit und Datenschutz einzuhalten und Risiken zu reduzieren. Andernfalls drohen den Unternehmen nicht nur erhebliche rechtliche und finanzielle Konsequenzen, sondern auch Betriebs- und Reputationsschäden. Elastic kann CIOs und CISOs bei der Verbesserung der Compliance ihrer Unternehmen mit diesen verschiedenen gesetzlichen Anforderungen unterstützen, insbesondere in den Bereichen Mapping und Klassifizierung von Daten, RBAC, Protokollierung und Überwachung sowie Erkennung der und Reaktion auf Angriffsversuche.

