elastic

Optimalen Nutzen aus Ihrer SIEM-Lösung ziehen

elastic.co/de ⟶

Inhaltsverzeichnis

Einführung

Immer mehr Organisationen treiben ihre digitale Transformation voran, um sich an das Marktumfeld anzupassen, müssen dabei jedoch oft auch ihre Sicherheitshaltung neu überdenken. Neue Online-Produkte und -Dienste, mobile Apps und eine steigende Anzahl an Remotemitarbeitern sind allesamt Einfallstore für neue Arten von Cyberangriffen. **Sicherheitsteams müssen sich schnell anpassen können, um mit diesen Angriffen Schritt zu halten**.

Dabei gilt es, Effizienzprobleme zu vermeiden, die den Geschäftsbetrieb trotz größter Anstrengungen des Sicherheitsteams gefährden können. Angesichts zunehmender SaaS-Einführung, Datenschutzgesetze und Vorgaben zum Konsolidieren von Sicherheitsfunktionen tragen noch weiter zur steigenden Komplexität bei.

Um den Überblick zu behalten und auch weiterhin effizient zu arbeiten, benötigen Sie die bereits vorhandenen Daten in Ihrer Sicherheitsinformations- und Ereignisverwaltungsplattform (SIEM). Sicherheitsteams benötigen immer mehr und vielfältigere Daten: Cloud, Internet der Dinge (IoT), mobile Quellen und Observability-Daten, um nur einige Quellen zu nennen. Das Ergebnis ist eine sprunghafte Zunahme der benötigten Ereignisaktivitäten, um für den Schutz des Unternehmens wichtige Einblicke zu gewinnen.

Diese Datenexplosion stellt Unternehmen aufgrund von SIEM-Einschränkungen oft vor betriebliche Herausforderungen. **Möglicherweise ist es an der Zeit, Ihre SIEM-Herangehensweise zu überdenken**, um sicherzustellen, dass Sie bereit für diese neuen Herausforderungen sind.

175 ZB

IDC schätzt das weltweite Datenvolumen bis 2025 auf 175 Zettabyte.

41,6 B

Bis 2025 werden 41,6 Milliarden vernetzter Geräte 79,4 Zettabyte an Daten generieren.

42 B

Die Teilnehmer am PwC's Global Economic Crime and Fraud Survey 2020 meldeten insgesamt 42 Milliarden US-Dollar an Verlusten durch Betrug.

Sicherheitsanforderungen verändern sich ständig

Organisationen orientieren ihre Geschäftsmodelle immer stärker an der Cloud, und Sicherheitsteams müssen sicherstellen, dass die wertvollsten Assets ihres Unternehmens – Nutzer, Anwendungen, Endpunkte und Daten – geschützt sind. Die folgenden Trends erschweren es Sicherheitsteams zunehmend, ihre KPIs und Metriken zu erfüllen.

Personen

Es ist entscheidend, neuen und modernen Angriffsmethoden immer einen Schritt voraus zu sein.

- Sicherheitskenntnisse sind sehr gefragt
- Überlastete Sicherheitsteams bemühen sich, schneller und effizienter zusammenzuarbeiten

Prozess

Angesichts zunehmender Cloud-Initiativen wächst der Druck, Betriebseffizienz und Geschwindigkeit zu erhalten.

- Riesige Datenmengen werden in die Cloud migriert
- Remotemitarbeiter und Partner brauchen Unterstützung für mehr Cloud-Lösungen

Technologie

Unterstützung für umfangreiche Datenquellen ist entscheidend, um Einblicke in Ausweichtechniken und erforderliche Details zur Kontextualisierung von Bedrohungen zu liefern.

- Es ist schwierig, reaktionsschnelle Abfragen und Analysen über lokale und Cloudumgebungen hinweg auszuführen.“
- In vielen Systemen ist der Zugriff auf umfangreiche Datenquellen zu teuer

Den Sicherheitsteams ist es schmerzlich bewusst, dass die Angriffsoberfläche mit der digitalen Transformation zunimmt. Jedes neue vernetzte Gerät und jeder Clouddienst ist ein potenzielles Einfallstor für Angreifer und kann zu schwerwiegenden Sicherheitsproblemen oder Datenpannen führen, die wiederum das Geschäftsrisiko erhöhen. **Die grundlegendste Anforderung dafür ist der richtige Kontext zur richtigen Zeit, um bessere und schnellere Entscheidungen zu treffen**.

Sicherheitsstrategie überdenken, Daten als Framework verwenden

Es ist oft nicht praktikabel, eine dynamische und ständig wachsende Angriffsoberfläche zu überblicken. Ingestions- oder ereignisbasierte Lizenzierungsmodelle und/oder Architekturen, die keine Cloud-Skalierungsanforderungen erfüllen, können Kompromisse erzwingen. Viele Teams wenden Zeit und Ressourcen für die Entscheidung auf, welche Daten in ihren alltäglichen Betrieb einbezogen bzw. davon ausgeschlossen werden. Dadurch erhält die Organisation weniger Einblicke in ihre SIEM-Lösung, und es entstehen betriebliche Silos: Datensilos, Teamsilos und Prozesssilos.

Anstatt Kompromisse und Einzellösungen für schwer in SIEM integrierbare Daten zu suchen, wie etwa Datenquellen mit hohem Volumen oder historische Daten, verfolgen immer mehr Sicherheitsteams einen Ansatz, der sich an ihren Datenanforderungen orientiert. Moderne SIEM-Lösungen müssen alle Arten von Daten unterstützen und Sicherheitsteams dabei helfen, diese Silos aufzubrechen. **Moderne SIEM-Lösungen bieten skalierbare, schnelle und exakte Suchfunktionen für Sicherheitsteams** in riesigen Mengen unterschiedlichster Daten, egal ob die Datenquellen herkömmlich, ungewöhnlich oder besonders datenreich sind, und zwar für mehrschichtige Ökosysteme. Diese Grundvoraussetzungen bieten Sicherheitsteams ungeahnte Vorteile beim **Verarbeiten beliebiger Sicherheits-Anwendungsfälle in großem Umfang**. Dazu gehören Funktionen für Überwachung und Compliance, Erkennung, Abwehr und Vermeidung von Bedrohungen sowie Incident-Verarbeitung, während sich die Teams gleichzeitig um Betrugsversuche, Datenpannen und andere wichtige Probleme kümmern, die das Unternehmen gefährden können. Dabei ist es für den Sicherheitsbetrieb entscheidend, dass die Teams **Daten möglichst einheitlich erfassen, analysieren und visualisieren und auf gewonnene Einblicke reagieren können**.

SOC-Vorteile mit einem einheitlichen Ansatz

Ein einheitlicher Ansatz bietet zahlreiche Vorteile für Sicherheitsteams. Ein einziger Datenspeicher mit leistungsstarken Sicherheits-, Verarbeitungs- und Datenvisualisierungsfunktionen liefert den erforderlichen Kontext über sämtliche verteilten Umgebungen hinweg, um wertvolle Sicherheitseinblicke aus all Ihren Daten zu gewinnen. Mit den richtigen Security Analytics-Funktionen – verlässliche Erkennungen, validierte Machine Learning-Aufträge und weitere vorkonfigurierte Methoden für lokale und Cloudumgebungen – können Sicherheitsteams ihre Sicherheitshaltung verbessern, bekannte und unbekannte Bedrohungen entdecken und schnell reagieren, um Schäden zu beheben und zukünftige Incidents zu vermeiden. Strategisch gesehen **können Sicherheitsteams schnell auf dynamische Änderungen reagieren**. Fachexperten können ihre Kenntnisse erweitern:

Mehr Kontext nutzen, um Daten besser zu verarbeiten und Handelsvorgänge zu analysieren

Im Team neue Erkenntnisse gewinnen oder neue Erkennungen implementieren

Neue Visualisierungen und Betriebsprozeduren entwickeln

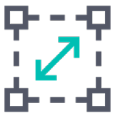
Profile von Angreifern erstellen und das Verhalten von Gegner emulieren

Immer Teams sind für Abwehrtätigkeiten zuständig. Mit starken Integrationsfunktionen auf der Plattformebene können Sie effiziente Prozeduren unterstützen, die sich leichter an neue Bedrohungsarten und neue gesetzliche Vorgaben anpassen lassen.

Mit einem einheitlichen Ansatz kann Ihr SOC komplexe Sicherheitsprobleme für eine Vielzahl von Sicherheitsfunktionen lösen, inklusive Bedrohungsabwehr, SIEM, Bedrohungsforschung, Compliance, Sicherheitsüberwachung und -Untersuchung, digitale Forensik und Incident-Verarbeitung, Endpunktschutz, Betrugsvermeidung und mehr.

Ganzheitliche Transparenz

Sammeln Sie Sicherheits-einblicke aus allen erforderlichen Datenquellen, um Ihre Geschäftsergebnisse zu verbessern.



Cloud-Skalierbarkeit

Nutzen Sie den erforderlichen Kontext aus der gesamten Organisation, um Bedrohungen zu überprüfen, inklusive historischem Kontext über Jahre hinweg.

Hohe SOC-Effizienz

Finden Sie wichtige Probleme schnell und erstellen Sie mühelos Integrationen mit anderen Tools und Technologien für schnellere Untersuchungen und Reaktionen.

Mehrwert für das gesamte Sicherheitsteam

Sicherheitsexperte und Administrator

- Logs, Datenflüsse und Kontextdaten aus der gesamten Umgebung an einem zentralen Ort analysieren, egal, wie unterschiedlich die Datenquellen sind.
- Schnelle, föderierte Suche für schnelle Zugriffe und Suchvorgänge in komplexen, verteilten Umgebungen
- Umfangreiche Datenquellen indexieren und mühelos und kostengünstig abrufen

Sicherheitsanalysten

- Genauigkeit für schnellere Erkennung komplexer Bedrohungen
- Geschwindigkeit für schnellere Abwehr und mehr Effizienz
- Bedrohungsabwehr automatisieren und MTTD minimieren

SOC Manager

- Umfangreiche Einblicke in die gesamte Umgebung erhalten, um die Sicherheitshaltung zu verbessern
- Bekannte Probleme vermeiden und unbekannte Probleme identifizieren
- Sicherheits-KPIs kostengünstig erfüllen

elastic

Werden Sie von Ihrer SIEM-Lösung ausgebremst?

Sicherheitsrelevante Daten stammen heutzutage aus Clouddiensten, Netzwerk- und Benutzeraktivitäten, Endpunkten, Anwendungen, vernetzten Geräten und vielen weiteren Quellen. Wenn viele SIEM-Lösungen versuchen, auf diese Datenquellen zuzugreifen, entstehen „Kaffeepausen“-Analysezeiten oder unnötig teure Deployments.

Manche SIEMs verwenden separate Datenspeicher für unterschiedliche Arten von Security Analytics: je einen Speicher für Machine Learning und für ereignisbasierte Korrelationen. Den Teams bleibt es überlassen, die Daten in einem weiteren Datenspeicher für den Bedrohungsabwehrkontext oder für forensische Beweisaufnahmen abzulegen, und so weiter. Wie bereits erwähnt beeinträchtigen diese Silos die Effizienz der Teams in den Bereichen Kontextweitergabe, Zusammenarbeit, Fallverarbeitung und Bedrohungsabwehr.

SIEM sollte Ihre SOC-Entwicklung eigentlich fördern, aber viele SIEM-Produkte sind weder skalierbar noch flexibel genug, um Sicherheitsteams beim Aufbrechen von Daten- oder Aufgabensilos zu unterstützen. Dadurch entstehen Untersuchungs-Workflows, die durch diese Silos eingeschränkt werden. Das Ergebnis sind betriebliche Silos, die Ihre Sicherheitsteams davon abhalten, schneller, intelligenter und effizienter zu arbeiten.

Einige gängige Hemmnisse für die betriebliche Effizienz mit herkömmlichen SIEM-Lösungen:

- Quellen von Sicherheitsdaten sind nicht konsolidiert und befinden sich in separaten Datenspeichern über das Unternehmen verteilt, was eine ganzheitliche Transparenz erschwert.
- Die Aufbewahrungsfristen sind zu kurz, was zu Kompromissen im Hinblick auf Erkennungen, Analysekontext und Bedrohungsabwehr führt. Es ist schwer, den Umfang von Angriffen mit längerer Verweildauer zu ermitteln.
- Sicherheitsanalysten fehlen die erforderlichen Datenquellen für Kontext zu Aktivitäten, die zwar nicht unbedingt auf komplexe persistente Bedrohungen hindeuten, aber trotzdem eine Gefahr für das Unternehmen darstellen können.
- Wenn SOC-Teams Machine Learning-Tools nutzen wollen, brauchen sie interne Datenwissenschaftler, die Modelle entwickeln, sowie geschulte Bedrohungsjäger, um den Kontext auszuwerten.
- Sicherheitsexperten müssen viel Aufwand in Datennormalisierungsprojekte investieren und/oder ihre das zugrunde liegende Datenschema ihrer SIEM-Lösung ständig anpassen, um neue, kontextbezogene Daten hinzufügen, wie etwa Datenquellen mit hohem Volumen. Sie müssen mit den Daten bereits vertraut sein.
- Forschungsteams wenden unangemessen viel Zeit für die Entwicklung unzuverlässiger SIEM-Regeln auf, die kaum Resilienz gegen Ausweichmaßnahmen bieten und denen zuverlässiger Kontext mit den richtigen Daten fehlt.
- Analysten der Ebenen 1 und 2 verbringen zu viel Zeit mit unnötigen Warnmeldungen, oder benötigen zusätzlichen Kontext aus anderen Datenspeichern, was zu Verzögerungen führt und die Effizienz beeinträchtigt.
- Entwickler verbringen die meiste Zeit damit, Integrationsfehler zu beheben oder Updates von Anbietern zu installieren.

Besserer Schutz mit einer modernen SIEM-Lösung

Moderne SIEM-Lösungen greifen auf alle Sicherheitsdaten zu, unabhängig von Größe, Umfang oder Speicherort. Mit Einblicken in die gesamte Umgebung erhalten Sicherheitsteams umfangreichen Kontext auf historische Abrufzeiträume, können Bedrohungen schneller erkennen und abwehren und ihre Prioritäten zielgenau ausrichten.

Zugriff auf alle Arten von Daten

Echtzeit- und historische Daten

Maximale SOC-Geschwindigkeit

Mehr Betriebseffizienz mit Elastic Security als SIEM-Lösung

Sicherheitsteams verwalten immer mehr Daten und müssen in der Lage sein, Suchen, Analysen und automatisierte Erkennungen in all diesen Daten schnell und exakt durchzuführen. Moderne Bedrohungen erfordern sofortige Korrelation für effektive Untersuchungen, Bedrohungsabwehr, -Profilerstellung und mehr über herkömmliche Sicherheitsdaten, Cloudinfrastrukturen, Anwendungsdaten und historische Daten aus mehreren Jahren.

Mit Elastic Security können Sicherheitsteams auf konsolidierte Daten zugreifen, zusätzlichen Kontext für Bedrohungen und Geschäftsprozesse gewinnen und historische Daten einsetzen, um schnell optimale Lösungen zu finden. Elastic Security bietet Funktionen für SIEM, Endpoint Security, Bedrohungsabwehr, Cloudüberwachung, Betrugserkennung und viele weitere Anwendungsfälle, damit Ihr SOC das Potenzial von Suche und Visualisierung nutzen kann, um das Unternehmen mit einem einheitlichen Ansatz zur Erkennung, Vermeidung und Abwehr von Bedrohungen zu schützen.

Intelligent arbeiten mit Elastic Security

Ganzheitliche Transparenz

Sammeln Sie nach dem Elastic Common Schema normalisierte Daten mit Beats, und indexieren Sie sämtliche sicherheitsrelevanten Daten, um Silos in der Organisation zu eliminieren. Interagieren Sie mit intuitiven vorkonfigurierten Dashboards, und entwickeln Sie per Ziehen und Ablegen benutzerdefinierte Visualisierungen für Ihre Anforderungen mit Kibana, Lens und Canvas.

Sicherheitseinblicke im Handumdrehen

Ingestieren Sie Daten mit Schema-on-Write- und Schema-on-Read-Formaten für eine optimale Abfrageleistung und die Flexibilität, Felder nach dem Ingestieren hinzufügen oder ändern zu können. Mit der Geschwindigkeit, für die der Elastic Stack bekannt ist, erhalten Sie innerhalb von Sekunden Ergebnisse in Ihren Dashboards. Bereiten Sie der Alarmmüdigkeit ein Ende mit priorisierten Korrelationen.

Historische Daten über Jahre hinweg einbeziehen

Nutzen Sie durchsuchbare Snapshots, um kostengünstig möglichst viele Sicherheitsdaten für die Bereiche Bedrohungserkennung und -Abwehr, Untersuchungskontext, Cloudüberwachung und mehr nutzen zu können. Ermitteln Sie den Umfang von Sicherheitsverletzungen mit einer Verweildauer von Monaten oder sogar Jahren.

Verweildauer reduzieren

Automatisieren Sie die Erkennung mit MITRE-gestützten vorkonfigurierten Erkennungen vom internen Elastic-Sicherheitsforschungsteam sowie benutzerdefinierte Erkennungen mit der leistungsstarken und intuitiven intuitive Event Query Language (EQL) für Korrelationen, um Tools, Taktiken und Prozeduren moderner Bedrohungen zu erkennen.

Bösartige auffällige Aktivitäten erkennen

Führen Sie unbeaufsichtigte Machine Learning-Aufträge in beliebigen Datenquellen mit Zeitstempel aus, um eigenständige oder miteinander verknüpfte Anomalien zu erkennen, die eine potenzielle Bedrohung darstellen. Kombinieren Sie beaufsichtigtes und unbeaufsichtigtes Machine Learning, um Methoden wie etwa Domänen generierende Algorithmen (DGAs) mit hoher Genauigkeit zu erkennen.

SecOps-Workflows vereinfachen

Mit dem interaktiven Arbeitsbereich in Elastic Security können Sie in einer interaktiven und intuitiven Zeitleiste Bedrohungen erkennen und abwehren, Ereignisse sortieren und Beweise sammeln. Nutzen Sie die integrierte Fallverwaltung und -Integration mit umfassenden Orchestrierungs-, Automatisierungs- und Abwehrfunktionen im Sicherheitsbereich sowie Workflow-Anbietern, um Abwehr und Behebung zu beschleunigen.

Moderne SOC-Implementierung

Elastic Security wird von Sicherheitsteams in aller Welt als technologisches Fundament eingesetzt. Die offene Elastic-Plattform erleichtert Integrationen, bietet mehr Flexibilität und unterstützt Beiträge und Gemeinschaftsentwicklungen aus der Community, damit sich SOC-Teams schneller weiterentwickeln und bessere und schnellere Entscheidungen treffen können.

Fazit

Sicherheitsteams müssen ihre Organisationen in einer ständig wachsenden Bedrohungsumgebung schützen und dürfen dabei die Betriebseffizienz nicht aus den Augen verlieren. Mit Zugang zu sämtlichen sicherheitsrelevanten Daten und kostengünstigen Zugriffsmethoden für historische Daten können Sie mehr Anwendungsfälle unterstützen, indem Sie Elastic Security als SIEM-Lösung bereitstellen und den allgemeinen Wert Ihres SIEM-Deployments steigern. Führende **Sicherheitsteams setzen Elastic Security als SIEM-Lösung ein, weil sie einen einheitlichen Ansatz für Erkennung, Vermeidung und Abwehr brauchen**.

Elastic liefert ganzheitliche Transparenz für die gesamte Umgebung mit der benötigten Geschwindigkeit und Effizienz zum Identifizieren und Beheben von Problemen. Außerdem erhalten Sie Cloud-Skalierbarkeit für Ihre gesamte Hybridumgebung und können Ihre SOC-Effizienz optimieren, egal wie verteilt Ihre Teams sind oder in wie vielen Silos sie momentan arbeiten. Schützen Sie Ihr Unternehmen mit dem neuen SIEM-Ansatz von Elastic Security.

Möchten Sie Elastic Security selbst ausprobieren?

Testen Sie Elastic Security in der Elastic Cloud (14 Tage lang kostenlos, keine Kreditkarte erforderlich). Oder stellen Sie die Lösung lokal bereit. Diese Variante ist immer kostenlos.

Elastic Security kostenlos testen →

Search. Observe. Protect.

Elastic macht Daten für Anwendungen wie Enterprise Search, Observability und Security nutzbar – in Echtzeit und unabhängig von ihrer Menge. Die Lösungen von Elastic bauen auf einem kostenlosen und offenen Technologie-Stack auf, der überall bereitgestellt werden kann und in kürzester Zeit Einblicke ermöglicht. Das Datenformat ist dabei ebenso wenig eingeschränkt wie die Anwendungsbereiche – vom Finden von Dokumenten über die Infrastrukturüberwachung bis hin zur Jagd auf Bedrohungen. Tausende Organisationen weltweit, darunter Cisco, Goldman Sachs, Microsoft, The Mayo Clinic, NASA, The New York Times, Wikipedia und Verizon, nutzen Elastic zur Unterstützung ihrer unternehmenskritischen Systeme. Elastic wurde 2012 gegründet und die Aktien des Unternehmens werden an der New Yorker Börse (NYSE) unter dem Symbol „ESTC“ gehandelt. Weitere Informationen erhalten Sie unter elastic.co/de.

AMERICAS HQ
800 West El Camino Real, Suite 350, Mountain View, California 94040, USA
Allgemein +1 650 458 2620, Vertrieb +1 650 458 2625

info@elastic.co