Tripwire Log Center

Zentralisiertes Log-Management leicht gemacht

Je raffinierter und hartnäckiger Hacker vorgehen, desto mehr Daten müssen Organisationen analysieren, um Warn- von Fehlmeldungen zu unterscheiden. Der konventionelle Ansatz, kostspielige Tools und SIEM-Lösungen für die Erfassung, Auswertung und Verwaltung von Logdateien und Ereignisdaten einzusetzen, ist leider ineffektiv.

Cyberbedrohungen werden immer ausgefeilter, Tools für Sicherheitsanalysen immer zahlreicher und Compliance-Vorgaben immer strenger. Um dabei den Überblick nicht zu verlieren, benötigen Organisationen eine smartere Lösung zur Verwaltung von Log- und Protokolldateien.

Hier kommt Tripwire® Log Center™ ins Spiel, ein leistungsfähiges Tool für die zentralisierte, zuverlässige und sichere Erfassung, Analyse und Bereitstellung von Log- und Protokolldateien. Log Center lässt sich nahtlos in bereits vorhandene Infrastrukturen integrieren und umfasst zudem eine wachsende Bibliothek von Korrelationsregeln. Somit sind Ihre Sicherheitsteams in der Lage, Bedrohungen in Ihren IT-Umgebungen schnell aufzuspüren und abzuwehren.

Außerdem können Sie diese Daten nutzen, um Ihre Compliance zu verbessern oder um Fehlmeldungen von tatsächlichen Sicherheitsvorfällen zu unterscheiden.

Was Tripwire Log Center auszeichnet

Tripwire Log Center bietet Kunden eine Alternative zu konventionellen Sicherheitsansätzen, indem es eine frühzeitige Angriffserkennung, die Einhaltung gesetzlicher Vorschriften und die sichere, zuverlässige Erfassung von Log- und Protokolldateien unterstützt.

Zentralisierte Forensik

Dank der Integrationsfreundlichkeit von Log Center können Sie Daten aus Tripwire Enterprise und Tripwire IP360™ in das Tool einspeisen und somit verdächtige Sicherheitsvorfälle, Systemänderungen, Konfigurationen mit Verbesserungsbedarf und Schwachstellen einsehen und miteinander in Verbindung setzen. Mit solch umfangreichen Daten lassen sich Risiken schneller erkennen und Sicherheitsinvestitionen effektiver priorisieren. Kunden, deren Sicherheitsinfrastruktur auf den CIS-Controls (Center for Internet Security) basiert, stellen wir kontextreiche Logdateien sowie Tipps zur Fehlerbehebung im Rahmen der ersten sechs kritischen CIS-Empfehlungen zur Verfügung.

Zentrale Verwaltung, lokale Kompetenz

Indem Sie Tripwire Log Center auf Abteilungs- oder Zweigstellenebene bereitstellen, geben Sie den Experten vor Ort – den Systemingenieuren und -administratoren – die Funktionen an die Hand, die sie für eine schnellere Untersuchung und Reaktion auf Vorfälle benötigen. Ein zentralisiertes SIEM- oder Analysetool ermöglicht zwar einen umfassenden Überblick über große Datenmengen, über das Gesamtbild, doch bei der Vorfallsuntersuchung ist ein dezentraler Ansatz effektiver. Tripwire Log Center bietet Ihnen die Vorteile beider Welten: zentralisierte Verwaltung und Überwachung, dezentrale Transparenz.

Effiziente Analyse- und Filterfunktionen

Die meisten SIEM- und Analysetools werden über ein verbrauchsbasiertes Lizenzmodell bereitgestellt – je

nach indexierten Datenmengen oder Ereignissen, die pro Sekunde analysiert werden. Das treibt jedoch die Kosten in die Höhe, erschwert die Budgetplanung und generiert zu viele Falschmeldungen. Mit Tripwire Log Center lassen sich sämtliche Ereignisse erfassen und speichern, doch nur praxistaugliche Daten werden zur Auswertung an die zentralisierte Management-Konsole geschickt. Dadurch sparen Sie Kosten und stärken Ihren Sicherheitsstatus.

Kostengünstige Compliance

Die Erfassung und Speicherung protokollierter Ereignisse gehört zu den grundlegenden Anforderungen vieler Branchenstandards, doch dies kann mit einem zentralisierten SIEM-Tool zu einem teuren Unterfangen werden. Oft müssen auch regionsspezifische Vorschriften für die Speicherung dieser Logdateien eingehalten werden. Tripwire Log Center wurde speziell entwickelt, um Kunden eine kostengünstigere Alternative zu traditionellen SIEM-Tools zu bieten, mit umfassenden Funktionen für das Log-Management, die gängige gesetzliche Compliance-Vorgaben erfüllen. Außerdem lassen sich Log- und Protokolldateien regionsspezifisch bestimmten Teams zuweisen und gleichzeitig von einer zentralen Konsole aus analysieren.

Schnellere Amortisierung: vordefinierte Regeln zur Risikominimierung

Mit Tripwire Log Center können Sie schnell und einfach Korrelationsregeln erstellen und anpassen. Sie können vorbestimmen, welche Reaktion eingeleitet werden soll, wenn auf Basis dieser Regeln eine Korrelation zwischen Logdateien oder Ereignissen identifiziert wird: für die Berichterstellung speichern, Warnmeldung generieren oder sonstige Aktionen vornehmen. Indem Sie Regeln vordefinieren, kann das gesamte Team Log Center ganz einfach bedienen und es entfällt die Notwendigkeit für zeit- und kostenintensive Schulungen.

Damit sich Anwender schnell die erforderlichen Kenntnisse aneignen können, erhalten Sie mit Tripwire Log Center die folgenden Lösungspakete:

Sicherheitslösungen zur Bedrohungsabwehr

» Aufdeckung von Insider-Bedrohungen

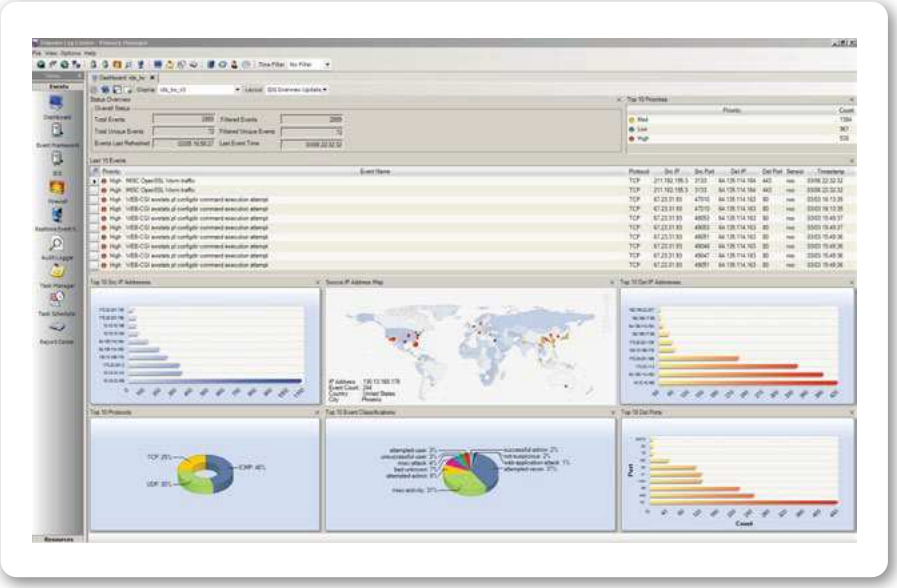

Abb. 1: Mit Sicherheitsdashboards und aktuellen Analyseergebnissen verbessern Sie Ihre Risikoeinschätzung und können Bereiche identifizieren, die eine genauere Überprüfung erfordern.

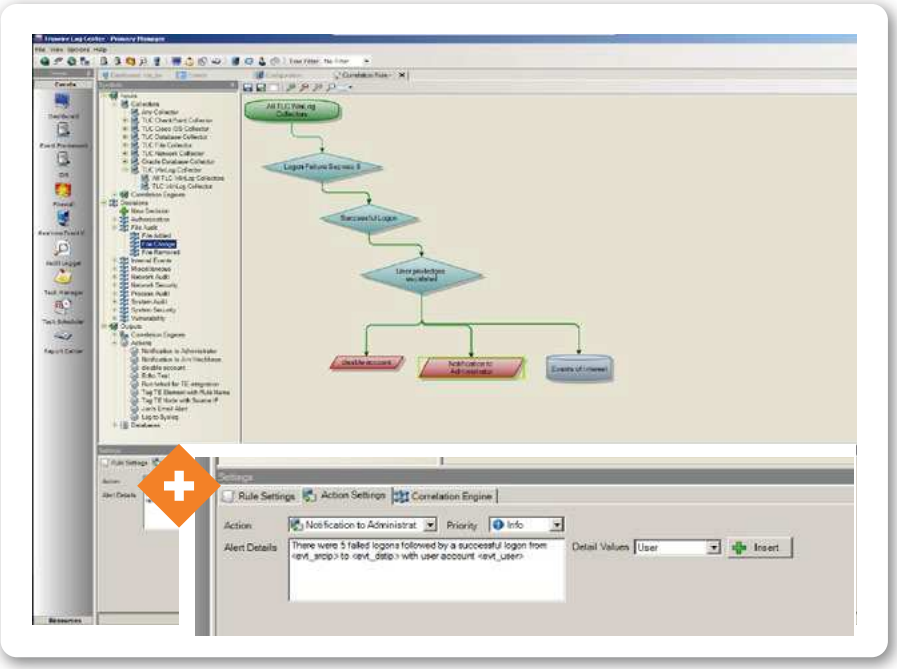

Abb. 2: Behalten Sie mit individuellen, per Drag-and-Drop erstellten Korrelationsregeln im Tripwire Log Center den Überblick über komplexe Verbindungen zwischen Ereignissen.

» Prüfung und Authentifizierung von Nutzern

» Erkennung von Denial-of-Service -Angriffen

» Angriffs- und Bedrohungserkennung

» System- und Netzwerkprüfung

» Integration von Schwachstellenmanagement und Cybercrime Controls-Funktionen

» Prüfung von Datenbanken

Lösungen für Compliance mit

» NERC

» PCI

» NIST 800-53

» HIPAA

Geschäfts- und nutzerbezogene Kontextdaten

Mit Tripwire Log Center lassen sich sicherheitsrelevante Daten ganz einfach erfassen, mit der standardbasierten

Klassifizierungsfunktion in Kategorien einordnen und teilen. Plattformen und Geräte werden nach Logdateien und Ereignissen durchsucht, die dann in Sicherheits- oder Compliance-Berichten zusammengefasst werden können. So erhalten Sie praxistaugliche und präzise Ergebnisse.

Dank dynamischer Korrelationslisten und der Integration mit anderen Tripwire-Lösungen kann Log Center diese Daten automatisch mit einschlägigen Kontextinformationen anreichern. Außerdem können Sie bestimmte Nutzer und Nutzergruppen nach Attributen wie Zugriffsrechten, Gruppen oder Rollen ordnen und überwachen.

Indem Sie geschäfts- und nutzerbezogene Kontextdaten miteinander in Bezug setzen, lassen sich zum Beispiel besonders geschäftskritische Ressourcen und die Nutzer, die darauf Zugriff haben, im Auge behalten. In Kombination mit Tripwire Enterprise, Tripwire Industrial Visibility und Tripwire IP360 können Sie mit Tripwire Log Center Zusammenhänge zwischen verdächtigen Ereignissen aufdecken und Schwachstellen und unerwartete Änderungen schnell erkennen. Das erleichtert die Risikoeinschätzung und Priorisierung von Sicherheitsinvestitionen.

Sichere, zuverlässige Erfassung von Logdateien

Tripwire Log Center erfüllt gängige Compliance-Vorgaben für die Erfassung und Verwaltung von Logdateien und stellt Kunden die Daten zur Verfügung, die sie für umfassende Sicherheitsanalysen und Incident-Response-Maßnahmen benötigen. Kunden profitieren zudem vom leistungsfähigen Tripwire Axon®-Agent zur Erfassung von Log- und Protokolldateien, der beim Ausfall eines Systems, Geräts oder einer Ressource die Daten schützt und aufbewahrt. Log Center ist auch im agentlosen Bereitstellungsmodell verfügbar.

Speicherung, Indexierung und Durchsuchung von Logdateien

Erfasste Log- und Protokolldateien werden vor der Speicherung indexiert, damit Sie schnell die Informationen finden, die Sie benötigen, um Sicherheitsvorfälle aufzuklären. Dabei können Logdateien zentral gespeichert oder über sekundäre Manager an verschiedene Zweigstellen verteilt und dort aufbewahrt werden. Sie können jedoch weiterhin von der zentralen Konsole aus auf diese Daten zugreifen.

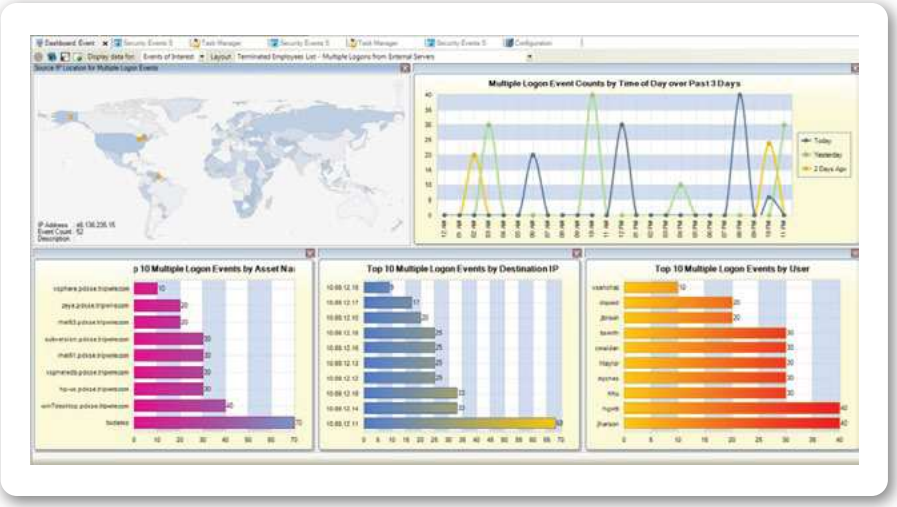

Abb. 3: Ergänzen Sie Ihre Sicherheitstools mit geschäfts- und nutzerbezogenen Kontextdaten, um gängige Anzeichen auf Cyberangriffe schneller zu erkennen.

Abgleich von Ereignisdaten

Mithilfe des Korrelationsmoduls von Tripwire Log Center können Kunden aus den umfassenden erfassten Ereignisdaten Hinweise auf die wirklich wichtigen Sicherheitsvorfälle herausfiltern. Hinzu kommen vordefinierte Korrelationsregeln, die sich auf verschiedenen Plattformen für Compliance- und Sicherheitszwecke einsetzen und sich über eine Benutzeroberfläche per Drag-and-Drop leicht individualisieren lassen.

Ressourcenerfassung

Durch eine granulare Analyse erfasster Logdateien zu Aktivitäten im Netzwerk können Sie mit Tripwire Log Center versteckte Ressourcen identifizieren, die von Netzwerk- und Trafficscans nicht aufgedeckt wurden. Diese „neuen" Ressourcen können anschließend von Log Center erfasst und überwacht werden.

Hochverfügbarkeit

Mit dem integrierten Failover Manager sorgt Tripwire Log Center selbst dann für Hochverfügbarkeit und nahtloses Logging, wenn der primäre Manager-Service ausfällt. Wenn der aktive Manager eine bestimmte Zeit lang nicht reagiert, werden Workloads automatisch auf den Failover Manager übertragen.

Integration mit weiteren Tripwire-Produkten

Jede Lösung im Tripwire-Portfolio bietet für sich genommen wichtige und effektive Sicherheitsfunktionen. Doch die größte Wirkung erzielen Sie, indem Sie unsere Lösungen miteinander verknüpfen. Tripwire Log Center kann zum Beispiel die Schwachstellendaten aus Tripwire IP360 und die geschäftsbezogenen Kontextdaten aus Tripwire Enterprise hinzuziehen, um präzisere, umfassendere Korrelationsinformationen bereitzustellen. Dadurch profitieren Sie von mehr Transparenz, müssen nicht ständig zwischen verschiedenen Tools wechseln, arbeiten effizienter und können Ihre Organisation besser schützen.

Haben Sie Interesse an einer Demo?

Erleben Sie Tripwire Log Center in Aktion und stellen Sie uns Ihre Fragen. Näheres erfahren Sie unter **tripwire.com/contact/request-demo**.

Die umfassende Transparenz und erstklassigen Tools für das Konfigurationsmanagement, die Ihnen Tripwire zur Verfügung stellt, werden durch Tofino Xenon um Funktionen für die Erkennung von risikoreichem Datenverkehr perfekt erweitert.

- Dieses Gerät ist die einzige Appliance für industrielle Sicherheit, die von unautorisierten Personen nicht erkannt und daher nicht umgangen werden kann.
- Durch die Integration mit Tripwire Log Center können Sicherheitsteams den von Tofino Xenon analysierten Verkehr zwischen Ressourcen in Echtzeit verfolgen und erkennen, welche Datenpakete blockiert wurden.
- Erfüllt die Compliance-Anforderungen von NERC CIP, ISA/IEC-62443, IEC 60870-5-104, ATEX, ISA-12.12.01 Class 1 Div.2, EN 50121-4 und DNV GL.

Weitere Informationen erhalten Sie unter tripwire.com.

Tripwire, ein Unternehmen der Belden-Gruppe, ist der ideale Cybersicherheitspartner zum Schutz von IT- und OT-Umgebungen. Unsere Lösungen lassen sich nahtlos mit Ihren vorhandenen industriellen Produkten wie Tofino-Firewalls oder Switches von Hirschmann integrieren.

tripwire

Tripwire stellt Kunden branchenführende Produkte zur Stärkung ihrer Cybersicherheit zur Verfügung. Wir schützen prominente Unternehmen auf der ganzen Welt vor Sicherheitsverletzungen und Cyberangriffen – und weil Hacker immer raffinierter werden, entwickeln auch wir unsere Technologien seit mehr als 20 Jahren ständig weiter. Unsere Lösungen sind sowohl On-Premises als auch in der Cloud verfügbar, wo sie Ihre digitale Infrastruktur schützen sowie Bedrohungen aufdecken und abwehren, ohne den Geschäftsbetrieb oder die Produktivität zu beeinträchtigen – sozusagen als unsichtbare Schutzbarriere für Ihre Systeme. **Weitere Informationen erhalten Sie unter tripwire.com.**

***The State of Security*: Aktuelles, Trends und interessante Einblicke finden Sie unter tripwire.com/blog**
Folgen Sie uns auf LinkedIn, Twitter und Facebook

TLCDS743b 1912