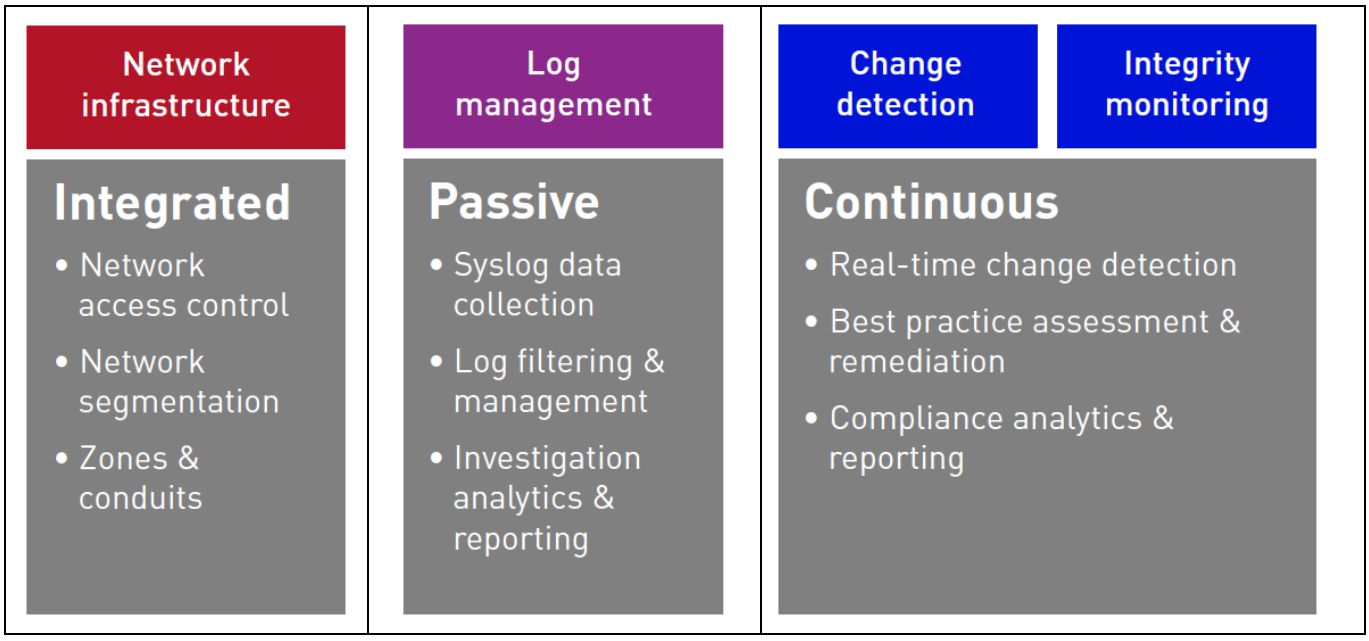
Log- Management in industriellen Produktionsnetzwerken

Einfaches und wirkungsvolles Event Monitoring mit Belden Tripwire® Log Center®.

Eine der grundlegendsten Sicherheitskontrollen ist die Möglichkeit, Geräteprotokolldaten zu sammeln und zu analysieren. Doch der Datenberg, der in einem modernen Netzwerk entsteht, kann die Erkennung der wahren Anomalien und Bedrohungen nahezu unmöglich machen.

Unsere Tripwire® Log Center®- Software von Belden löst dieses Problem, indem es alle Protokolldaten sicher sammelt und diese Daten filtert und analysiert, so dass nur relevante Ereignisse an Ihre dafür zuständigen Mitarbeiter gesendet werden.

Unsere Cybersecurity- Lösungen



Unsere Log-Management- Lösung

	Stabil. Verschlüsseltes, stabiles und hoch performantes System, um Log-Daten zu sammeln, zu speichern und zu indexieren.
	Leistungsstark. Real-Time- Korrelation der gesammelten Log-Daten dank einem äusserst leistungsfähigen Analyse- Algorithmus, der die ermittelten Daten bei Bedarf sogar an übergeordnete Systeme weitergeben kann.

	Übersichtlich. Übersichtliche Darstellung der ermittelten Daten für die schnelle Fehlersuche, für ein umfassendes Reporting und für das einfache Beheben von Vorfällen.

Das zentrale Element unserer Lösung bildet ein Audit-Logger, der die Log-Daten von allen aktiven Netzwerk- Komponenten, aber auch von Datenbanken, Serversystemen, HMI- Stationen oder sogar von Applikationen entgegennimmt und in einer Datenbank abspeichert. Als Suchalgorithmus verwendet dieser Logger den Lucene-Index, der z.B. auch von den Google-Suchmaschinen im Internet verwendet wird.

Der Event-Manager verwendet diese Daten als Grundlage für das Analysieren der Log-Daten, für das Ermitteln von automatisch oder manuell erstellten Korrelationen sowie für das gezielte Melden von festgestellten Unregelmässigkeiten. Dies Daten können bei Bedarf auch an übergeordnete Systeme wie Tripwire® Enterprise® weitergegeben werden

Alle Daten wie grafische Statistiken, Suchergebnisse, festgestellte Vorfälle und Reports werden auf einer zentralen Konsole einfach übersichtlich dargestellt.

Reagieren Sie auf das, was in Ihrer Umgebung passiert

Mit dem Tripwire LogCenter können Sie alle gesammelten Protokolldaten einfach filtern und durchsuchen, um einfache Betriebsausfälle zu untersuchen oder auch um Einblicke in die Beziehungen zwischen verdächtigen Ereignissen, Systemänderungen, schwachen Konfigurationen und Sicherheitslücken zu erhalten. Sie können Ereignisse mit einfach zu erstellenden Regeln korrelieren, um auf schnelle Weise sogenannte "Ereignisse von Interesse" zu identifizieren.

Die Korrelations-Engine von Tripwire Log Center identifiziert und reagiert automatisch auf diese "Ereignisse von Interesse", wobei ein logischer Ablauf, der aus einer oder mehreren Bedingungen bestehen kann, verwendet wird. Aktionen können das Erstellen eines Arbeitstickets, das Senden einer Benachrichtigungs-E-Mail oder das Ausführen eines Befehls umfassen. Das Tripwire Log Center kann auch mit Tripwire Enterprise integriert werden, um Anomalien und verdächtige Aktivitäten noch besser zu erkennen und darauf reagieren zu können.

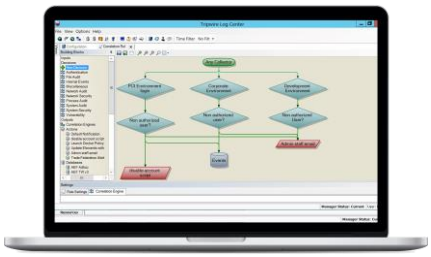
Erstellen Sie zuverlässige Nachweise für Ihre Compliance und Ihre Sicherheit

Mit dem Tripwire LogCenter können Sie sicherstellen, dass Sie allfällige behördliche Anforderungen für die Protokollerfassung und -aufbewahrung erfüllen können. Protokolle werden vor Änderungen geschützt, indem die Protokollnachrichten in ihrem ursprünglichen Format und Inhalt gespeichert werden. Das Tripwire LogCenter ermöglicht Ihnen mittels "Security Solution Packs" ei-

nen schnellen Einstieg für das Erkennen von Bedrohungen, für Benutzer-Audits, für eine Denial-of-Service-Erkennung, für das sichere Erkennen von Sicherheitsverletzungen und für das schnelle Analysieren von Intrusion Detection- Daten. Das Tripwire LogCenter hilft Ihnen bei der Einhaltung von behördlichen Vorgaben zum Beispiel für NERC CIP, PCI und NIST 800-53. Zudem reduzieren die hohen Komprimierungsgrade die Speicheranforderungen an Ihre Hardware und erhöhen die Datenübertragungsraten.

Filtern Sie relevante und umsetzbare Daten

Reduzieren Sie den Aufwand und die Kosten herkömmlicher Security Information and Event-Management- Systeme (SIEMs) und Sicherheitsanalyse-Lösungen. Filtern Sie Daten vorab und identifizieren Sie Anomalien und Muster, von denen bekannt ist, dass sie Bedrohungen und Frühindikatoren für Sicherheitsverletzungen sind. Leiten Sie nur umsetzbare und relevante Daten an entsprechende Mitarbeiter und allfällige Drittanbieter-Tools wie Threat Intelligence- Lösungen weiter.



Wir zeigen Ihnen gerne unsere Lösungen und freuen uns auf Ihre Kontaktaufnahme.