



WatchGuard Compliance Reporting

Vereinfachen Sie die Compliance mit automatisierten Kontrollen und Berichten

WatchGuard Compliance Reporting ist eine automatisierte Engine zur Compliance-Berichterstattung für die ThreatSync+ NDR-Lösung von WatchGuard. Es verwendet Hunderte von vorgefertigten, automatisierten Compliance-Kontrollen, die auf den NIST 800-53- und ISO 27001-Frameworks basieren. Da die meisten regulatorischen Gesetze aus dem NIST- und ISO-Framework abgeleitet werden, sind die Zuordnung von Kontrollen und die Erstellung von Berichten zur Erfüllung Ihrer Compliance-Anforderungen einfach und unkompliziert. ThreatSync + NDR fasst mittels KI-gesteuerten Sicherheitsrichtlinien das massive Volumen an Netzwerkverkehr in priorisierte intelligente Warnungen, Untersuchungsansichten und Compliance-Berichte zusammen.

Kontrollen können einfach in ThreatSync + NDR hinzugefügt oder geändert werden. Diese Kontrollen werden automatisch in die WatchGuard Reporting Engine integriert und ermöglichen eine einfache Berichtskonfiguration oder die Erstellung neuer Berichte, indem Sie einfach die erforderlichen Kontrollen auswählen und per Knopfdruck aktivieren.

Sofortige Compliance-Visualisierung

Jeder Bericht enthält eine Compliance-Gesamtbewertung, die auf der Kontrollwirksamkeit des gesamten Kontroll-Frameworks basiert. Der Bericht beschreibt anschließend die Wirksamkeit jeder Kontrolle im Vergleich zu ihren Compliance-Zielen, die Trendlinie der Kontrollwirksamkeit und Hinweise zur Korrektur von Kontrollfehlern.

Umfangreiche Abdeckung

Zu den Berichten gehören ISO-27001, NIST 800-53, NIST-171/CMMC, UK Cyber Essentials sowie leicht konfigurierbare Kontrollzuordnungen und die Erstellung von Berichten für die Einhaltung von Versicherungsaudits sowie von Branchenvorschriften wie das MPA-Framework (Motion Picture Association), die CIS Critical Security Controls und die IEEE-Standards.

Sparen Sie Zeit und Geld

Sicherheitsteams sparen Zeit und Geld mit diesen einfach zu aktivierenden, vorgefertigten Richtlinien und Berichten. Es ist unkompliziert, Kontrollmodelle zu konfigurieren und neue Modelle hinzuzufügen. Threatsync+ NDR-Compliance-Kontrollen und -Berichte beseitigen manuelle Kontrollbewertungen, Validierungen und Berichterstellungen, wodurch Hunderte von Arbeitsstunden eingespart werden.

So erreichen kleine Teams Compliance-Ziele

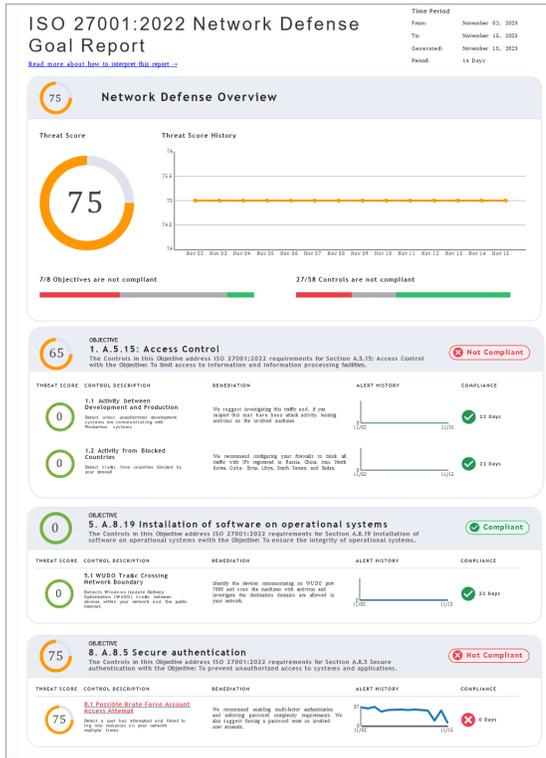
WatchGuard Compliance Reporting in Kombination mit ThreatSync+ NDR bietet eine automatisierte Berichterstattungslösung für die Netzwerk-Compliance, die einfach zu konfigurieren und zu bedienen ist, Geld und Zeit spart und es Unternehmen ermöglicht, sich ändernde Vorschriften und Standards kontinuierlich einzuhalten.

Vorteile

- Der Compliance-Status wird auf Knopfdruck nachgewiesen. Compliance-Berichte für Auditoren, Partner, Lieferanten und Versicherungen können schnell generiert werden.
- Die Compliance-Kosten werden durch die Automatisierung hochmanueller Prozesse reduziert, wodurch die Arbeitsbelastung der IT-Teams reduziert wird.
- Das Compliance-Verhalten wird durch Berichte zur Kontrollwirksamkeit verbessert, um Compliance-Lücken zu erkennen und praktische Behebungsmaßnahmen mit Hinweisen zur Optimierung der Kontrollen zu ergreifen.
- Der Compliance-Prozess wird vereinfacht und umfasst einfach zu konfigurierende, sofort einsatzbereite Kontrollsätze und Berichte, um neue, sich ändernde und wachsende Anforderungen zu implementieren und zu unterstützen.

Einfache Erstellung von Compliance-Berichten

Mit über hundert vorgefertigten Kontrollen (weitere werden monatlich hinzugefügt) und einer einfach zu konfigurierenden Policy-Engine können die wichtigsten Kontrollen innerhalb von ThreatSync+ NDR erstellt, modifiziert und bereitgestellt werden. WatchGuard Compliance Reporting erfasst automatisch alle Kontrollen und Kontrolländerungen, um Berichte mit nur wenigen Klicks zu erstellen. Neue Berichte, die spezielle Anwendungsfälle abdecken, können auch schnell aus den NIST-, CSF- und ISC-Frameworks konfiguriert werden.



Wichtige Funktionen

Compliance-Berichte umfassen:

- **Cyber Essentials** – Die Cyber Essentials-Kontrollsätze decken vier Ziele und sechzig Kontrollen im gesamten Netzwerk ab: DMZ-Datenverkehr, Malware-Schutz, sichere Konfiguration und Standards zum Sicherheitsupdate-Management.
- **ISO 27001** – Der ISO 27001-Kontrollsatz deckt die Jahre 2013 und 2022 über acht Ziele und achtundfünfzig Kontrollen ab, die Netzwerk-, Identitäts- und Anwendungssicherheit abdecken.
- **NIST 800-53** – Der NIST 800-53-Kontrollsatz und -bericht enthält sieben Ziele und achtundachtzig Netzwerk- und Identitätskontrollen zur Unterstützung von Compliance-Programmen.
- **NIST 171** – Der NIST 171-Kontrollsatz und -bericht umfasst sieben Ziele und siebenundachtzig Netzwerke und Kontrollen zur Unterstützung von NIST 171, CMMC 2.0 und DFARS.
- **MPA** – Der Motion Picture Association Defense-Zielbericht schützt das geistige Eigentum von Filmen, elektronischen Spielen und anderen Produktionen, einschließlich drei Zielen und vierundvierzig Kontrollen.

NIST- und ISO-Richtlinienbasierte, KI-gestützte Kontroll-Frameworks unterstützen kontinuierliche Compliance und Compliance-Berichte.

ThreatSync und Firebox ermöglichen die Koordinierung und Automatisierung mehrerer Prozesse und Tools mithilfe der Sicherheitsorchestrierung zur Förderung eines einheitlichen Sicherheitskonzepts.

ThreatSync und ThreatSync+ NDR bieten kostengünstige, umfassende und einheitliche Bedrohungsanalysen

