Enterprise Security Monitoring Services

Der Druck auf Unternehmen, ihre Daten und kritischen Systeme zu schützen, nimmt stetig zu.

Eine effektive Sicherheitsstrategie muss die Einhaltung der strengen Vorschriften gewährleisten, doch die meisten Unternehmen sind noch weit von einer kontinuierlichen Überwachung der Netzwerke entfernt. In zu vielen Unternehmen müssen interne Teams die Systeme rund um die Uhr überwachen und haben dadurch nicht genug Zeit oder Ressourcen, um Logdateien zu analysieren oder auch nur eine wirklich lückenlose Überwachung zu gewährleisten.

Verordnungen wie PCI DSS, HIPAA und SOX schreiben jedoch die regelmässige Überprüfung von Logdateien vor und bei Verstössen können erhebliche Geldbussen drohen.

Die Enterprise Security Monitoring Services von NTT Security übernehmen die Überwachung und Analyse von Logdateien rund um die Uhr, sodass Sie auch die anspruchsvollsten Vorgaben erfüllen können.

Cloudbasierte Überwachung durch Sicherheitsexperten

Wir überwachen Logdateien von nahezu jedem Produkt, dass diese erstellen kann, von Anwendungen, Datenbanken und Endpunkten über Firewalls, UTM, IDS und IPS bis hin zu Firewalls für Webanwendungen (WAF), Systemen zur Überwachung der Dateiintegrität (FIMs) und anderen Netzwerkgeräten. Wir ergänzen die erfassten Sicherheitsdaten um Kontextinformationen wie Schwachstellen, Ressourcen, GeoIP, schädliche Hosts und Benutzerberechtigungen (privilegiert/nicht privilegiert). So können wir effektiv überwachen, ob Unternehmensrichtlinien, Best Practices für Sicherheitsmassnahmen und gesetzliche Vorgaben eingehalten werden.

Sicherheitsüberwachung für Best Practices und Compliance – zwei Servicelevel mit teilweise identischen Funktionen

Wir bieten zwei Servicelevel an: Enterprise Security Monitoring Standard und Enterprise Security Monitoring Enhanced. Bei beiden wird die Kundeninfrastruktur rund um die Uhr von unseren Security Operations Centern aus überwacht. Dabei werden in beiden Fällen die umfassenden Bedrohungsdaten aus dem NTT Security Global Threat Intelligence Center herangezogen.

Enterprise Security Monitoring – Standard

Dieser Service wurde für Unternehmen konzipiert, die gängige Sicherheitstechnologien nutzen und standardisierte Sicherheitsanforderungen erfüllen müssen. Bei diesem Cloudbasierten Service werden die Sicherheitstechnologien mithilfe standardisierter Erkennungsregeln rund um die Uhr von Analysten in unseren SOCs überwacht. Die Analysten leiten auch erste Abwehrmassnahmen ein, bevor sie Sicherheitsvorfälle zur weiteren Untersuchung oder Beilegung an das Kundenunternehmen melden.

Wir nutzen unsere eigene Plattform, um für eine effektive Compliance-Kontrolle zu sorgen.

Im Rahmen des Standard-Services haben Sie Zugriff auf ein benutzerdefiniertes Portal, in dem Sie Ereignisdaten abrufen, die Services im Dashboard einsehen und Compliance-Berichte für Führungskräfte und technische Mitarbeiter generieren können.

Vorteile der Enterprise Security Monitoring Services von NTT Security

- Stärkung der Compliance durch die aktive Überwachung und die Erstellung detaillierter Berichte über die Einhaltung gesetzlicher Vorschriften und Branchenstandards
- Schutz der Daten und Systeme rund um die Uhr mithilfe Cloudbasierter Überwachungs- und Abwehrmassnahmen
- Ununterbrochene Verfügbarkeit durch den Einsatz mehrerer Security Operations Center (SOC)
- Eskalation von Sicherheitsvorfällen und Versand kontextbezogener Warnmeldungen
- Individuell anpassbare Anwendungsszenarien und Regeln für Warnmeldungen, die den spezifischen Anforderungen Ihres Unternehmens gerecht werden
- Optimiertes Enterprise Security Monitoring durch die NTT Security Enterprise Security Program Services
- Flexible Servicelevel, die an steigende Unternehmens-anforderungen angepasst werden können

Enterprise Security Monitoring – Enhanced

Dieser Service ist für Unternehmen mit speziellen Sicherheitsanforderungen in diversen Sicherheitstechnologien gedacht. Er unterstützt komplexe Anwendungsszenarien, darunter die Erstellung von Korrelations- und Benachrichtigungsregeln zur Erfüllung bestimmter Unternehmensanforderungen und derzeit mehr als 200 unterschiedliche Technologien verschiedener Anbieter.

Kundeninfrastrukturen werden rund um die Uhr von unseren Global Security Operations Centern aus überwacht. Die Teams dort identifizieren Sicherheitsvorfälle und leiten sie zur Überprüfung und Bestätigung an erfahrene, zertifizierte Level-1- und Level-2-Sicherheitsanalysten weiter. Anschliessend senden wir Ihnen einen Bericht zur weiteren Analyse des Sicherheitsvorfalls zu.

Die Enhanced Services werden durch das NTT Security Global Threat Intelligence Center unterstützt und Kunden haben Zugriff auf ein konfigurierbares Portal, in dem sie Ereignis- und Vorfallsdaten abrufen, die Services im Dashboard einsehen und Compliance-Berichte für Führungskräfte und technische Mitarbeiter generieren können.

Abbildung 1: Vergleich der Funktionen von Enterprise Security Monitoring – Standard und Enterprise Security Monitoring – Enhanced.

Funktion	Enterprise Security Monitoring - Standard	Enterprise Security Monitoring - Enhanced
Überwachung rund um die Uhr durch ein Security Operations Center	✔	✔
Unterstützung durch NTT Security Global Threat Intelligence Center		✔
Standardprofil zur Einhaltung von Sicherheitsauflagen	✔	
Benutzerdefiniertes Profil zur Einhaltung von Sicherheitsauflagen für zahlreiche, sehr unterschiedliche Ressourcen		✔
Von Analysten überprüfte Berichte zu Sicherheitsvorfällen[1]	✔	✔
Konfigurierbares Webportal	✔	✔
Anpassbare Überwachungs- und Compliance-Berichte	✔	✔
Zugriff auf die Ereignis- und Vorfallsdaten der letzten 90 Tage	✔	✔
[Optional] Suche in unbearbeiteten Logdateien		✔
[Optional] Sichere, langfristige Aufbewahrung und Verwaltung von Logdateien	✔	✔

Über NTT Security

NTT Security ist das auf Informationssicherheit und Risikomanagement spezialisierte Unternehmen der NTT Group (Nippon Telegraph and Telephone Corporation), einem der grössten IKT-Unternehmen weltweit. Der Experte für IT-Security steht für ein ganzheitliches Sicherheitskonzept und die Bereitstellung ausfallsicherer Lösungen, die den Anforderungen der Kunden vor dem Hintergrund des digitalen Wandels gerecht werden. Mit zehn globalen SOCs, sieben Zentren für Forschung und Entwicklung sowie mehr als 1.500 Sicherheitsexperten unterstützt NTT Security Unternehmen auf sechs Kontinenten bei der Reaktion auf Hunderttausende Sicherheitsvorfälle pro Jahr.

NTT Security bietet Kunden die richtige Mischung aus Beratung, Managed Services und Technologien, indem lokales Know-how optimal mit globalen Ressourcen kombiniert wird. Weitere Informationen finden sich unter **nttsecurity.com/ch**.

1. Bei ESM Standard wird versucht, Ereignisse automatisch zu bestätigen. Ausgewählte Ereignisse, für die dies nicht mit einem hohen Grad an Gewissheit möglich ist, werden von Sicherheitsanalysten bestätigt.