NTT Security

Global Solution Overview

Threat Detection Services

Unternehmen müssen Angriffe hartnäckiger und technisch versierter Hacker abwehren, für die herkömmliche Sicherheitsmassnahmen kein Hindernis sind.

Diese Angriffe sind sehr komplex und werden meist erst spät bemerkt, sodass Hacker viel Zeit haben, in betroffenen Unternehmen Schaden anzurichten. Je länger ein Angriff unerkannt bleibt, desto grösser sind die kommerziellen Auswirkungen für das Unternehmen: Vertrauensverlust, Schädigung von Markenimage und Aktienpreis sowie eine höhere Wahrscheinlichkeit von Bussgeldern und Klagen.

Eine hundertprozentig effektive Lösung oder Erkennungstechnologie für den umfassenden Schutz vor komplexen Angriffen gibt es leider nicht. Doch die Threat Detection Services von NTT Security bieten wichtige Sicherheitsinformationen und einen besseren Schutz durch die Kombination diverser Quellen: kommerziell verfügbare, überwachte Quellen sowie unsere eigenen ausgefeilten Analysefunktionen, die Bedrohungssuche und die Bedrohungserkennung.

Zwei Servicelevel mit modernsten Funktionen

NTT Security bietet zwei Servicelevel zur Bedrohungserkennung an: **Threat Detection Standard** und **Threat Detection Enhanced**. Beide Services bieten moderne Funktionen zur Angriffserkennung und proaktiven Suche nach Bedrohungen rund um die Uhr sowie umfassende Bedrohungsdaten, die vom NTT Security Global Threat Intelligence Center bereitgestellt werden.

Beide Services finden die tatsächlichen Bedrohungen in der grossen Anzahl von Benachrichtigungen (hauptsächlich Fehlalarmen), die von den meisten Sicherheitstechnologien generiert werden, erstellen einen Bericht über Sicherheitsvorfälle und schicken diesen direkt an Sie.

Dabei suchen sowohl unsere Sicherheitsanalysten als auch automatische Systeme proaktiv nach Bedrohungen und analysieren diese, um ihre Auswirkungen abzuschätzen und relevante Informationen über potenzielle Sicherheitsverstösse zu finden. Anschliessend senden wir Ihnen eine detaillierte Zusammenfassung und praxistaugliche Empfehlungen, damit Sie schnell angemessene Massnahmen ergreifen können.

Modernste Analyseverfahren

Hacker nutzen Angriffstechniken, deren Gefahrendinkatoren sich sehr schnell ändern. Deshalb reichen herkömmliche Erkennungstechnologien allein nicht mehr aus. Unsere Services verwenden modernste Analysetechniken, um verdächtiges Verhalten aufzudecken. Mithilfe von maschinellem Lernen, modernsten Korrelationstechniken, Bedrohungsmodellierung und Bedrohungsdaten können wir sowohl bekannte als auch unbekannte Bedrohungen zuverlässig identifizieren.

Threat Detection Standard

Mit diesem modernen, automatisierten Service stellt NTT Security einige grundlegende Funktionen zur Bedrohungserkennung bereit.

Für Bedrohungen, die wir zuverlässig identifizieren konnten, erhalten Sie einen Bericht mit einer präzisen Beschreibung der Sicherheitsverletzung und Empfehlungen für Ihr Incident-Response-Team.

Kunden dieser Serviceversion werden auch über Bedrohungsdaten informiert, die NTT Security fortlaufend zusammenträgt. Sobald Sicherheitsverletzungen identifiziert und als Bedrohung eingestuft wurden, werden diese Bedrohungsdaten aktualisiert und im Rahmen des Service bereitgestellt.

Threat Detection Enhanced

Bei dieser Serviceversion werden moderne, komplexe Angriffe mithilfe von modernsten Analyseverfahren, Bedrohungsdaten und proaktive Bedrohungssuche aufgedeckt.

Verdächtige Aktivitäten und alle relevanten Kontextinformationen werden von qualifizierten Sicherheitsanalysten überprüft, die die Auswirkungen ermessen können. Anschliessend erhalten Sie einen detaillierten Bericht mit einer umfassenden Beschreibung des Vorfalls sowie spezifischen, handlungsorientierten Empfehlungen.

Unsere Sicherheitsanalysten aktualisieren den Incident Report und unterstützen Sie bis zur Behebung des Problems.

Vorteile der Services für Threat Detection von NTT Security

- Ausgefeilte Analysefunktionen, die mithilfe von maschinellen Lernverfahren, Bedrohungsmodellierung und anderen Methoden potenzielle Sicherheitsbedrohungen aufdecken, die von herkömmlichen Mechanismen nicht erkannt werden können
- Unterstützung durch Sicherheitsanalysten mit entsprechend angepasster Workbench im SOC†
- Weiterführende Untersuchung von Vorfällen und Validierung durch erfahrene Analysten, die alle relevanten Informationen zur Hand haben†
- Ereignisgesteuerte Bedrohungssuche†
- Benachrichtigungen mit praxistauglichen Handlungsempfehlungen
- Unterstützung bis zur Behebung des Vorfalls†

†Diese Services sind nur mit Threat Detection Enhanced verfügbar.

Funktionen von Threat Detection Enhanced

Integration von Produkten anderer Anbieter und Spurensammlung

Bei dieser Serviceversion bieten wir die Integration von Produkten anderer Anbieter an. Durch die enge Verzahnung mit Technologien diverser unterstützter Anbieter können Beweismaterialien wie der erfasste Datenverkehr, Aufzeichnungen auf Endpunkten, ausführbare Malware-Traces und Kontextinformationen zusammengestellt werden, die über die standardmässigen Syslog-Ergebnisse hinausgehen.

Event-driven threat hunting

Sicherheitsanalysten führen im Rahmen dieser Serviceversion eine ereignisgesteuerte Bedrohungssuche (Threat Hunting) für diverse Anbietertechnologien durch. Mithilfe der Workbench-Tools von NTT Security können Sicherheitsanalysten alle vom Kunden überwachten Quellen sowie Kontextinformationen und Nachweisdaten einsehen.

Services zur Bedrohungsabwehr

Sicherheitsanalysten von NTT Security sind für Abwehrmassnahmen verantwortlich und stellen sicher, dass der Angreifer sich nicht in der Unternehmensumgebung ausbreiten kann. Beispiele für Abwehrmassnahmen sind die Isolierung kompromittierter Endpunkte und die Blockierung als schädlich bestätigter URLs und IP-Adressen im Netzwerk.

Durch die Kombination dieser Incident-Response-Massnahmen mit unseren ausgereiften Funktionen zur Threat Detection profitieren unsere Kunden von einem umfassenden MDR-Serviceangebot (Managed Detection and Response).

Abbildung 1: Funktionsvergleich für den Threat Detection Standard und Threat Detection Enhanced Service von NTT Security.

Funktion	Services zur Bedrohungserkennung	
	Threat Detection Standard	Threat Detection Enhanced
24/7 Überwachung durch ein Security Operations Center	✔	✔
Unterstützung der Services durch das NTT Security Global Threat Intelligence Center	✔	✔
Kontinuierliche Aktualisierung der Bedrohungsdaten durch aktive Untersuchungen	✔	✔
Modernste Analyseverfahren einschliesslich maschineller Lernverfahren und Bedrohungsmodellierung	✔	✔
Integration von Produkten anderer Anbieter und Beweissammlung für wichtige Sicherheitstechnologien[1]		✔
Detaillierte Untersuchung von Vorfällen durch Sicherheitsanalysten		✔
Event-driven threat hunting		✔
Automatisierte Sicherheitsanalyse und Erstellung von Berichten über Vorfälle	✔	
Berichte zu Sicherheitsvorfällen, die auf detaillierten Untersuchungen und Threat Hunting basieren		✔
Konfigurierbares Webportal	✔	✔
Zugriff auf Event- und Incident-Daten der letzten 90 Tage	✔	✔
[Optional] Suche in unbearbeiteten Logdateien des Kunden		✔
[Optional] Sichere, langfristige Aufbewahrung und Verwaltung von Logdateien		✔
[Option] On-Premises-POD2[2]		✔
[Option] Isolierung kompromittierter Endpunkte durch NTT Security (Remote-IR-Massnahmen)[3] und/oder Blockierung als schädlich bestätigter URLs und IP-Adressen[4]		✔

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. Erfassung und Analyse weiterer Daten von Anbietern, zum Beispiel PCAP-Daten (Packet Capture), Berichte zur Ausführung von Malware und Host-Aufzeichnungen. 2. Für Kunden, die ihre Logdateien vor Ort speichern möchten oder müssen, wird ein On-Premises-POD installiert. 3. Für die Eindämmung eines Vorfalls auf Endpunkten ist eine von NTT Security verwaltete Endpunktlösung erforderlich. 4. Zum Blockieren der URLs/IP-Adressen ist eine von NTT Security verwaltete Netzwerklösung erforderlich.