DELTA THREAT

DeltaThreat - Scheda prodotto

Indice

01 Network Detection and Response

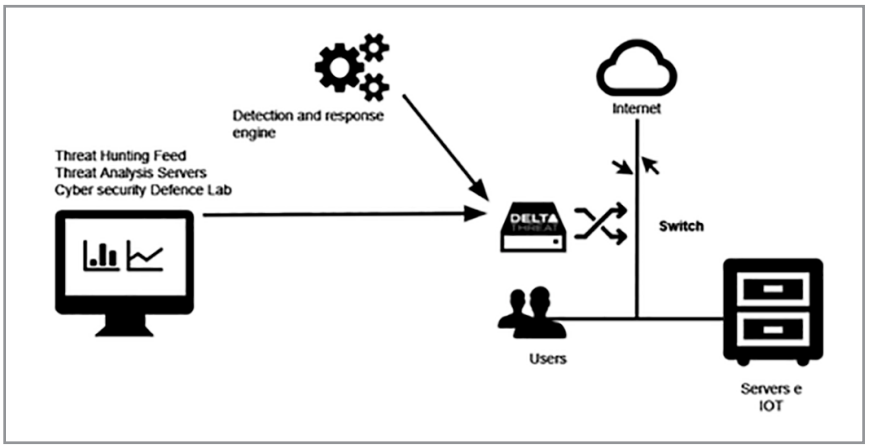
Soluzione NDR

DeltaThreat NDR è una soluzione che Identifica, Classifica e Blocca tutte le minacce e anomalie riscontrate a livello di rete attraverso i suoi motori di identificazione e Response integrati:

- Signature
- Artificial Intelligence
- Threat Intelligence
- Response

Tutte le minacce e il traffico sospetto sono mostrati tramite la dashboard integrata e notificati tramite email.

Nello specifico un prodotto di Network Detection and response (NDR) è una soluzione di sicurezza informatica che monitora costantemente il traffico della rete dell'azienda per rilevare minacce informatiche e comportamenti anomali. DeltaThreat NDR è un'appliance fisica che si posiziona tra lo switch ed il firewall e tramite una porta di Mirroring analizza il traffico di rete in modo passivo. Nello specifico, DeltaThreat riceve il traffico da analizzare tramite una porta di span, collegata ad una porta dello Switch (del cliente) configurata per effettuare il mirroring del traffico di rete che il cliente desidera monitorare.



02 Network Traffic Monitoring

L'appliance DeltaThreat copre la maggior parte dei protocolli di rete. Tutti i seguenti protocolli sono supportati dal Motore di monitoraggio del traffico:

Transport Layer:

• **TCP (Transport Control Protocol):** Il protocollo TCP è uno standard di comunicazione che consente ai programmi e ai dispositivi di scambiare informazioni attraverso una rete. È progettato per inviare

pacchetti attraverso la rete e verificare l'effettiva consegna di dati e informazioni. È utilizzato per trasmettere dati da protocolli di alto livello, questi includono protocolli di condivisione peer-to-peer come File Transfer Protocol (FTP), Secure Shell (SSH) e Telnet. È anche usato per inviare e ricevere email tramite Internet Message Access Protocol (IMAP), Post Office Protocol (POP), e Simple Mail Transfer Protocol (SMTP), e per l'accesso web attraverso il Hypertext Transfer Protocol (HTTP). Questo protocollo è affidabile, grazie alla conferma della ricevuta dei messaggi attraverso il processo di "Handshake", e orientato alla connessione.

● **UDP (User Datagram Protocol):** UDP è un protocollo di trasporto Connectionless (livello 4) nel modello OSI, fornisce un servizio di messaggistica semplice e poco affidabile per i servizi orientati alle transazioni. Il protocollo UDP è più veloce ma meno affidabile del TCP. In una comunicazione attraverso protocollo TCP, due computer iniziano la comunicazione stabilendo una connessione tramite un processo automatizzato chiamato "handshake". Solo una volta che questo passaggio è stato completato, un dispositivo effettivamente trasferire pacchetti di dati all'altro. Le comunicazioni UDP non passano attraverso questo processo, invece un computer inizia semplicemente a inviare dati ad un altro dispositivo senza verificare l'avvenuta consegna. Il protocollo UDP è fondamentalmente un'interfaccia tra IP e processi di livello superiore, è utile in situazioni in cui i meccanismi di affidabilità come il protocollo TCP non sono necessari.

Application Layer:

HTTP (Hyper Text Transfer Protocol): HTTP è un protocollo a livello applicativo per sistemi di informazione ipermedia distribuiti e collaborativi. HTTP è un protocollo di comunicazione basato su TCP/IP, che viene utilizzato per fornire dati (file HTML, file di immagini, risultati di query, ecc.) attraverso Internet. La porta di default per questo protocollo è la porta 80, in listening per protocolli TCP. Il protocollo HTTP specifica come i dati delle richieste dei client saranno costruiti e inviati al server, e come i server risponderanno a queste richieste.

HTTP/2: HTTP/2 è più efficiente del protocollo di rete HTTP utilizzato dal World Wide Web. Si basa sul protocollo SPDY e possiede tutti i concetti fondamentali del protocollo http, tuttavia modifica il modo in cui i dati vengono formattati (framed) e trasportati tra server e client, entrambi i quali gestiscono l'intero processo, nascondendo la complessità delle applicazioni all'interno del nuovo livello di formattazione.

SSL (Secure Sockets Layer): SSL è un protocollo di sicurezza internet basato sulla crittografazione. È stato sviluppato per garantire privacy, autenticazione e l'integrità dei dati nelle comunicazioni internet. Solo i dispositivi dei client e dei server sicuri sono in grado di riconoscere i dati. SSL è utilizzato anche in abito di certificazioni, sicurezza dei protocolli SMTP e NNTP per nuovi gruppi. SSL è il predecessore del protocollo TLS

TLS (Transport Layer Security): TLS è un protocollo ampiamente adottato in ambito di sicurezza per facilitare la privacy e la sicurezza dei dati nelle comunicazioni internet. L'uso primario di TLS è la comunicazione crittografata tra le web application e i server, come i motori di ricerca. Il protocollo TLS può essere usato per la crittografazione di altre comunicazioni, quali mail, messaggi e VoIP (voice over IP).

SMB (Server Message Block): Il protocollo di Messaggio di Blocco del Server è un protocollo di comunicazione client-server, usato per la condivisione degli accessi a file, stampanti, porte seriali e altre risorse di rete. Può anche trasportare protocolli per l'intero processo di comunicazione. Il protocollo SMB si basa su protocolli di trasporto di basso livello.

DCERPC (Distributed Computing Environment / Remote Procedure Calls): La struttura del DCE Remote Procedure Call (RPC) è un protocollo di rete usato nei sistemi di distribuzione. La procedura di RPC è eseguita in differenti processi che dal processo di chiamata, ed è solitamente eseguito in un'altra macchina. La struttura del RPC rende più semplice la struttura dei sistemi distribuiti perché permette agli sviluppatori di concentrarsi sui fondamenti della costruzione delle applicazioni distribuite, invece di soffermarsi sui meccanismi della comunicazione.

SMTP (Simple Mail Transfer): SMTP è un protocollo a livello applicativo per la trasmissione di posta elettronica. Il client che vuole mandare una email, apre una connessione TCP verso il server SMTP e manda la mail attraverso la connessione. Il server SMTP è sempre impostato su listening mode. Dopo l'effettuata connessione TCP (porta 25 di solito) con il client, il server manda la mail istantaneamente.

FTP (File Transfer Protocol): FTP è un protocollo di rete largamente utilizzato per il trasferimento di file tra computer attraverso protocollo TCP/IP, come nel World Wide Web. Il protocollo FTP è considerato non sicuro perché permette il passaggio dei dati non crittografati.

SSH (Secure Shell): Il protocollo SSH è un metodo sicuro di accesso da remoto da un dispositivo ad un altro. I due dispositivi aprono una porta TCP (di solito 22) per aprire la connessione. Fornisce diverse opzioni per una autenticazione sicura e protegge le comunicazioni sicure e integra una forte crittografia. Il protocollo lavora a livello client-server, che implica una connessione stabilita attraverso il SSH del client connettendosi al SSH del server

DNS (Domain Name System): DNS è un protocollo standard che aiuta gli utenti di internet a trovare siti web usando indirizzi leggibili all'uomo. La funzione principale del protocollo DNS è di tradurre i nomi del dominio in indirizzi IP, che sono leggibili per i computer.

Modbus: Modbus è un protocollo di comunicazione dati usato con PLC (programmable logic controllers). Modbus è diventato un protocollo di comunicazione standard e adesso è comunemente utilizzato per connettere dispositivi aziendali.

CIP (Common Industrial Protocol): CIP è un protocollo indipendente dai media che usa un modello di comunicazione produttore-consumatore, ed è un protocollo strettamente orientato agli oggetti nei livelli superiori. CIP include una vasta libreria di oggetti per supportare le comunicazioni di rete per scopi generali, i servizi di rete come il trasferimento di file, e le tipiche funzioni di automazione come i dispositivi di input/output analogici e digitali, HMI, controllo del movimento e feedback di posizione.

DNP3 (Distributed Network Protocol): DNP3 è un insieme di protocolli di comunicazione utilizzati tra i componenti nei sistemi di automazione di processo. Il suo uso principale è nelle utility come le compagnie elettriche e dell'acqua. Gioca un ruolo cruciale nei sistemi SCADA, dove è usato dalle SCADA Master Stations (a.k.a. Control Centers), Remote Terminal Units (RTUs), e Intelligent Electronic Devices (IEDs).

NFS (Network File System): NFS è un protocollo di file system distribution che permette a un utente su un computer client di accedere ai file su una rete nello stesso modo in cui accederebbe a un file di archiviazione locale. Poiché è uno standard aperto, chiunque può implementare il protocollo.

NTP (Network Time Protocol): NTP è un protocollo creato per sincronizzare gli orologi dei computer su una rete tra sistemi informatici attraverso lo scambio di pacchetti, con tempi di latenza variabili ed inaffidabili.

DHCP (Dynamic Host Configuration Protocol): DHCP è un protocollo di rete per la gestione, è usato per automatizzare i processi di configurazione degli IP dei dispositivi di rete. Un Server DHCP dinamico assegna gli indirizzi IP e altri parametri di configurazione di rete ad ogni dispositivo di rete, permettendo così la comunicazione con altri IP connessi alla rete.

TFTP (Trivial File Transfer Protocol): è un semplice Protocollo di Trasferimento File che permette al client di ricevere un file o di mandare un file da o a un host remoto, utilizzando il protocollo UDP. Uno dei suoi usi principali è nelle prime fasi di avvio dei nodi da una rete locale. TFTP è stato usato per questa applicazione perché è molto semplice da implementare.

KRB/KRB5 (Kerberos): Il protocollo di autenticazione Kerberos ha un servizio di autenticazione RPC_C_AUTHN_GSS_KERBEROS. Il protocollo Kerberos definisce come i client devono interagire con un servizio di autenticazione di rete ed è stato standardizzato da Internet Engineering Task Force (IETF). Kerberos 5, realizza un'autenticazione sicura basata su un singolo accesso.

IKEv2 (Internet Key Exchange version 2): IKEv2 è un protocollo di crittografia VPN che gestisce le azioni di richiesta e risposta. Si assicura che il traffico sia sicuro stabilendo e gestendo l'attributo SA (Security Association) all'interno di una suite di autenticazione - di solito IPSec poiché IKEv2 è fondamentalmente basato su di esso e costruito in esso.

SIP (Session Initiation Protocol): SIP è usato per segnalare e controllare sessioni di comunicazione interattive. È usato per segnalare e controllare sessioni di comunicazione multimediali in applicazioni di telefonia Internet per chiamate vocali e video, in sistemi telefonici IP privati, nella messaggistica istantanea su reti Internet Protocol (IP) e nelle chiamate di telefonia mobile su LTE in tempo reale.
SNMP (Simple Network Management Protocol): è un protocollo a livello applicativo definito dal Internet Architecture Board (IAB) in RFC 1157 per lo scambio di informazioni di gestione tra dispositivi di rete. Fa parte della suite di protocolli TCP/IP. SNMP è utilizzato per il monitoraggio e la gestione della comunicazione di rete.

RDP (Remote Desktop Protocol): è un protocollo sicuro di comunicazione di rete sviluppato da Microsoft. RDP è costruito per la gestione da remoto, accesso remoto a desktop virtuali, applicazioni e al terminal di RDP server. Per usare la connessione RDP, l'amministratore di rete RDP si connette al software client RDP e i singoli utenti potranno usare il software RDP server.

RFB (Remote Framebuffer): RFB è un semplice protocollo aperto per l'accesso remoto alle interfacce grafiche. Funziona a livello di framebuffer ed è applicabile a tutti i sistemi a finestre e applicazioni, compresi Microsoft Windows, Mac OS e X Window System.

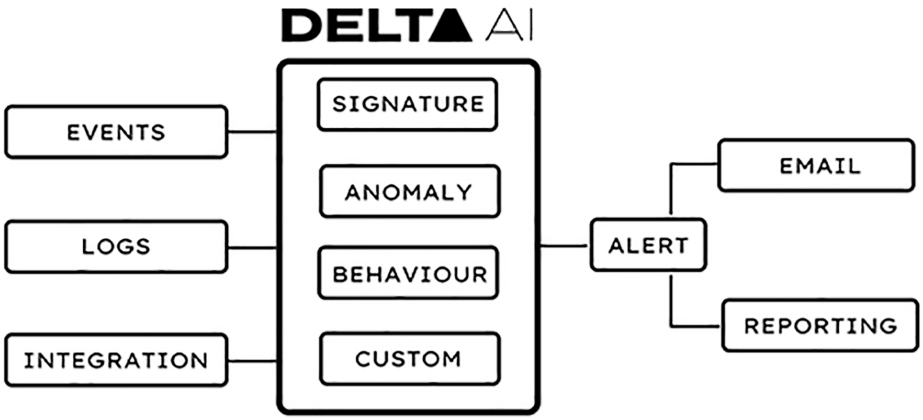
MQTT (Message Queuing Telemetry Transport): È un protocollo di messaggistica leggero per l'uso in casi in cui i client abbia bisogno di una piccola impronta di codice e sono collegati a reti inaffidabili o a reti con risorse di larghezza di banda limitate. È usato principalmente per la comunicazione machine-to-machine (M2M) o per connessioni di tipo Internet of Things.

03 Threat Detection

DeltaThreat basa il proprio motore di identificazione di minacce su tre diversi metodi:

1. Signature-based Detection
2. Behavior-Analysis and Machine Learning Detection
3. Threat Intelligence Engine

Nell'ambito della Cyber Security esistono diversi metodi di prevenzione contro attacchi informatici, molti di essi però aiutano gli utenti a proteggersi solo contro una piccola percentuale di attacchi. DeltaThreat per creare la soluzione ideale, ha basato la propria scelta sui migliori metodi di difesa, che offrono le migliori prestazioni con il minor effort e risorse possibili, offrendo al contempo un livello di sicurezza più elevato e stabile delle tradizionali soluzioni.



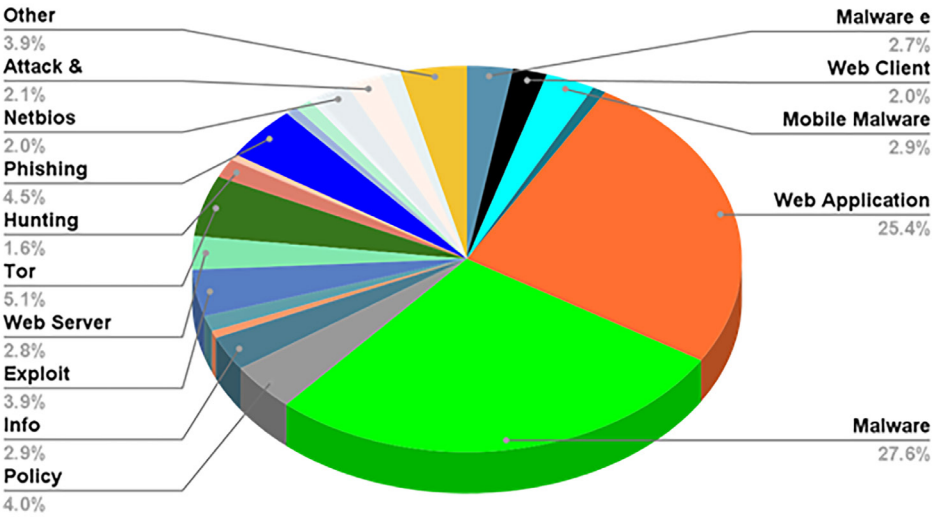
Signature-Based Detection

Il motore di Signature è basato sulle firme di malware e pattern di attacco studiati in passato. Attualmente sono state implementate oltre ventiduemila firme, ovvero possibili scenari di attacco.

Signature-Based Detection è un metodo per rilevare e identificare le intrusioni abbinando modelli o firme digitali già identificate in passato, attraverso la verifica degli attributi specifici delle connessioni, come file di log ed eventi. DeltaThreat AI verifica la timeline degli eventi con le firme digitali imple-

mentate direttamente all'interno dell'appliance, per permettere l'identificazione di diverse tipologie di intrusione, attacco e minaccia. Questo metodo aiuta DeltaThreat NDR a identificare azioni malevole in tempo reale e con alta precisione.

Questa metodologia permette di identificare le prime avvisaglie di operazioni che potrebbero comportare la completa compromissione dei sistemi informatici. Uno dei vantaggi di questo motore di identificazione è il basso tasso di falsi positivi e l'alta precisione nell'identificazione di attori malevoli. Come mostrato nel grafico sottostante DeltaThreat pone maggiore attenzione alle minacce Malware e alle Web Application, ritenuti i più frequenti vettori e schemi di attacco.
Lo svantaggio di questa metodologia di rilevazione è l'assenza di individuazione di attacchi di tipo zero-day, ma questa lacuna è compensata dai motori User Behavior e Machine Learning.



Machine Learning Detection

Il motore di Artificial Intelligence, tramite l'implementazione di algoritmi complessi e algoritmi statistici, identifica le anomalie comportamentali. L'implementazione del motore di AI permette un'analisi dinamica grazie alle sue capacità di integrazione a qualsiasi infrastruttura di rete.

Basare la propria analisi unicamente sulla Signature-based detection permette solo di proteggere gli attacchi conosciuti, ma ogni giorno si calcola che oltre 390.000 nuove varianti di malware siano scoperte ogni giorno.

Grazie all'analisi costante del traffico DeltaThreat è in grado di comprendere le attività dei dispositivi, ad essi associati, presenti all'interno della propria rete, aumentando la precisione nell'identificare i comportamenti e andamenti delle richieste in uscita e in entrata. La presenza di anomalie nel traffico di rete di un dispositivo permette di individuare la possibile presenza di un malware o di un attacco di un end-point, che fingendosi "sicuro", cerca elementi vulnerabili da compromettere.
Alla base di questo motore si pone la raccolta dati, strutture comportamentali e algoritmi da diversi punti dell'intera infrastruttura. Attraverso l'analisi di questi dati Delta NDR è in grado di classificare il comportamento usuale dei dispositivi e creare un algoritmo di statistica per assegnare il livello di probabilità delle azioni dei device.
Attraverso questo motore DeltaThreat riesce a garantire uno strato di protezione aggiuntiva, permettendo di individuare Insider Threat e dispositivi infetti, proteggendo l'azienda, anche, da eventuali attacchi provenienti dall'interno.

Threat Intelligence

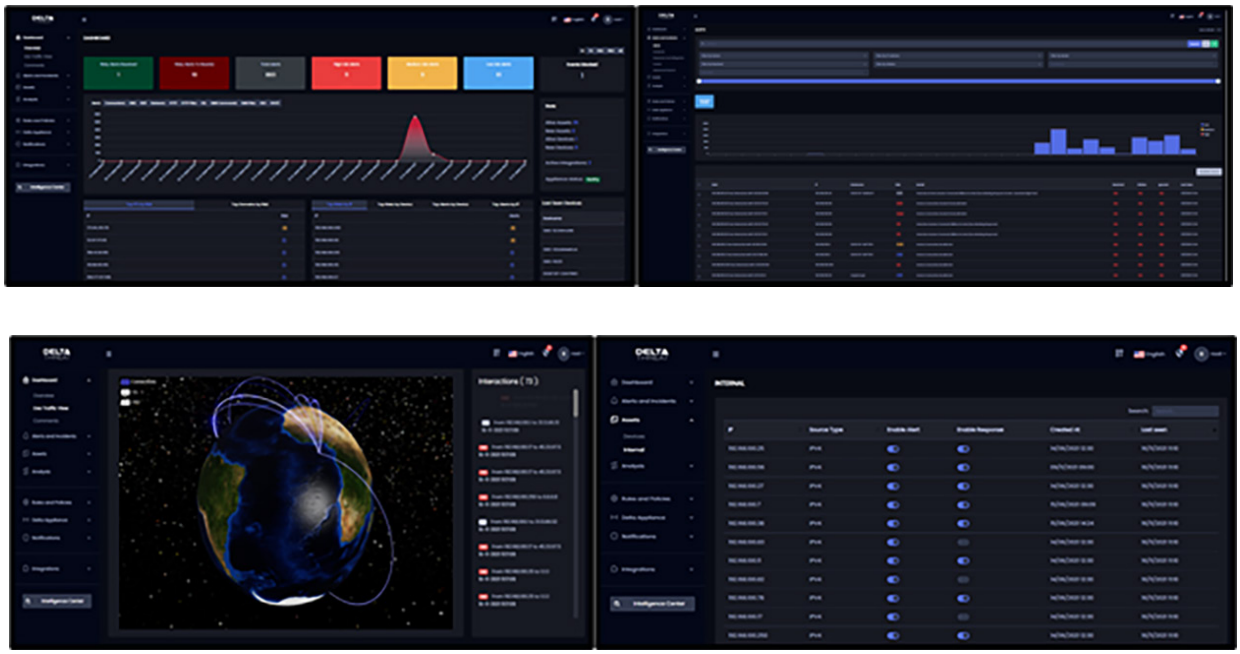
Identificare le nuove minacce emergenti è un compito essenziale nel mondo della cybersecurity, perchè basta una connessione malevola non identificata per compromettere un dispositivo, e successivamente l'intera rete. Per prevenire questo genere di attacchi, DeltaThreat ha implementato nella propria soluzione di NDR lo strumento di Cyber Threat Intelligence, un motore che permette di analizzare grandi quantità di dati riguardo le minacce esistenti ed emergenti, per identificare le possibili minacce correnti.
Il nostro motore di Threat Intelligence attualmente analizza tutti i dati che riceviamo da oltre 30 feed diversi, provenienti dal web, dark web e Deep web, per aumentare il livello di accuratezza nell'identificare le minacce ed aumentare il livello di sicurezza.
L'implementazione di questo motore permette non solo di identificare le minacce nascoste ma anche di rivelare i motivi e la metodologia dell'attaccante, offrendo al team di sicurezza il tempo e le conoscenze necessarie per scegliere la risposta migliore contro la minaccia corrente.

04 Threat Response

Il motore di Response ha la funzione di bloccare le minacce correnti permettendo di proteggere i dispositivi all'interno dell'azienda. Implementare una soluzione di NDR permette di dare supporto allo staff IT, offrendo il tempo necessario per intervenire in caso di minaccia rilevata. Il seguente servizio sarà attivato unicamente su richiesta del cliente.

05 Platform

L'appliance DeltaThreat NDR ha integrato una piattaforma che permette la visualizzazione di tutte le connessioni, dispositivi e ip identificati e di analizzare tutti gli alert, con relativo score e status, generati.



La Platform di DeltaThreat NDR è stata strutturata per essere utilizzata con diversi livelli di competenza, in base alle necessità e utilizzo:

Role	Usage
CTO / CISO	• Incident Response and Forensics • Threat Monitoring • Threat Response • Traffic Log Monitor • Network Traffic Monitoring • Executive Reports
IT Managers	
CERT Teams	
SOC	
NOC	
Network and System Engineers	

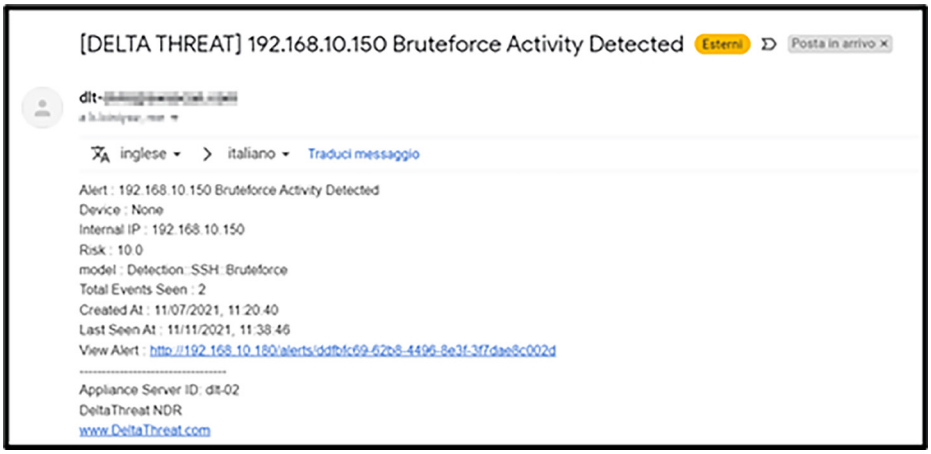
Notificazione via Email

La configurazione SMTP su DeltaThreat NDR permette l'invio delle segnalazioni agli utenti desiderati. Le mail inviate conterranno come oggetto una singola segnalazione generata, in base allo score settato come soglia minima.

Tra le configurazioni per l'invio delle mail, gli utenti hanno la possibilità di attivare le seguenti modalità di notifica (per singolo utente)

Modalita	Descrizione	Use - Case
Alert Creato*	L'utente riceverà solo le segnalazioni identificate per la prima volta	SOC
Alert Aggiornato*	L'utente riceverà ogni segnalazione generata, a partire dalla segnalazione creata fino alle successive identificazioni	CERT Teams
Report Settimanale	L'utente riceverà un report dettagliato ogni settimana *(Beta)*	Executive
Report Mensile	L'utente riceverà un report dettagliato ogni mese *(Beta)*	Executive

DeltaThreat invia solo le segnalazioni con score pari o superiore alla soglia minima impostata nella sezione "SMTP Configuration"



06 Documentazione

DeltaThreat fornisce ai propri clienti la seguente documentazione su richiesta o in data di acquisto dell'appliance DeltaThreat NDR:

- **Documento di Installazione dell'appliance DeltaThreat:** il seguente documento mostra il procedimento per effettuare l'installazione dell'appliance DeltaThreat all'interno della propria infrastruttura

- **Documento Getting Started - Easy:** documento che offre un'introduzione generale alla piattaforma DeltaThreat

- **Documento Getting Started - Advance:** documento che mostra e spiega ogni sezione della dashboard di DeltaThreat

07 In Allegato

- **Platform:** documento che elenca e descrive ogni sezione della piattaforma

- **Scheda Servizi:** documento completo che elenca e descrive nel dettaglio tutti i servizi inclusi ed opzionali proposti da DeltaThreat