

SANGFOR ATHENA NDR

Piattaforma Intelligente di Network Detection & Response

Sangfor Athena Network Detection and Response è una piattaforma NDR all'avanguardia che eleva il framework di cybersecurity delle aziende. Sfrutta l'intelligenza artificiale (AI) e l'apprendimento automatico (ML) per fornire informazioni sulle minacce in tempo reale e sofisticate analisi di sicurezza, consentendo di individuare e mitigare rapidamente le minacce informatiche. Questa piattaforma scopre attivamente le minacce nascoste, risponde agli attacchi in corso e scopre le vulnerabilità per rafforzare le difese informatiche di un'organizzazione.

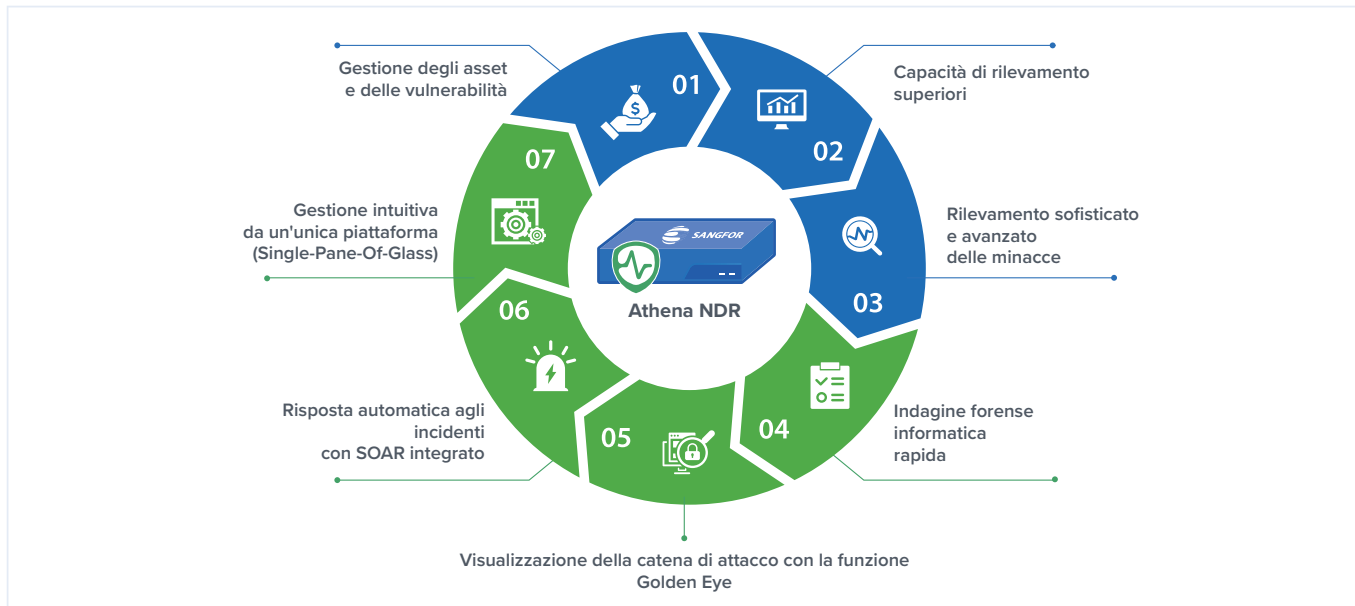
Il monitoraggio in tempo reale, l'analisi approfondita e gli avvisi tempestivi di Athena NDR garantiscono una rapida identificazione delle anomalie del tracciato di rete, consentendo strategie di cybersecurity proattive anziché reattive. È rafforzato da un modulo SOAR integrato che automatizza la risposta alle minacce e offre playbook personalizzati per una gestione degli incidenti su misura.

Con Sangfor Athena NDR, le aziende passano da osservatori passivi a difensori attivi contro le minacce informatiche in continua evoluzione, con la possibilità di fornire la massima protezione ai propri asset digitali.





CARATTERISTICHE CHIAVE



Vantaggi principali di Athena NDR

1 **Visibilità completa della rete e protezione contro gli exploit**

Athena NDR raccoglie e analizza i tracciati dell'intera rete, compresi i modelli di tracciati nord-sud ed est-ovest, i dati dei log e le informazioni sugli endpoint, per offrire una visibilità senza pari della rete. Sfrutta l'intelligenza artificiale e i modelli di apprendimento automatico appositamente creati per identificare le anomalie e le minacce avanzate con velocità e precisione. Ciò consente alle organizzazioni di mantenere una posizione proattiva e di essere all'avanguardia nel panorama in continua evoluzione degli attacchi informatici.

2 **Riduzione di MTTI e MTTR con il Threat Hunting integrato**

Athena NDR riduce in modo significativo il tempo medio di identificazione (Mean Time to Identify - MTTI) e il tempo medio di risposta (Mean Time to Respond - MTTR). Monitora attivamente le attività di rete per rilevare le anomalie e correlarle con gli indicatori di minaccia noti, come gli Indicatori di compromissione (IOC) e gli Indicatori comportamentali di compromissione (BIOC). Definendo una solida linea di base del comportamento normale, la piattaforma identifica rapidamente le anomalie e dà priorità alle minacce reali, riducendo al minimo i falsi positivi. I team di sicurezza hanno la possibilità di concentrarsi sugli incidenti più critici e di rispondere in modo efficace, semplificando il processo complessivo di gestione delle minacce.

3 **Risposta rapida agli incidenti grazie al SOAR integrato**

Il modulo SOAR integrato di Athena NDR automatizza le risposte alle minacce verificate per aumentare l'efficienza delle operazioni di sicurezza. Con il modulo SOAR, la piattaforma si coordina con il firewall e l'EDR per eseguire azioni di risposta automatica come l'isolamento dei sistemi compromessi e il blocco degli IP dannosi. Questo non solo alleggerisce il carico di lavoro manuale dei team di sicurezza, ma accelera anche la risposta alle minacce, riducendo al minimo l'impatto degli attacchi informatici sull'organizzazione.

4 **Operatività ottimizzata e risparmio di costi**

Athena NDR è progettato per integrarsi perfettamente con un'ampia gamma di tool di sicurezza, tra cui firewall, soluzioni di sicurezza degli endpoint e sistemi SIEM (Security Information and Event Management). Supporta la perfetta integrazione con strumenti di sicurezza di terze parti di fornitori rinomati come Sophos, Bitdefender, Trend Micro e altri. Con Athena NDR, le organizzazioni possono raggiungere una solida strategia di cybersecurity senza gravare eccessivamente sui loro bilanci e senza interrompere i loro sistemi attuali.

