NUCLEON
AHEAD OF CYBER THREATS

Nucleon XDR
Extended Detection and Response

MODERN THREATS NEED MODERN SECURITY SYSTEMS

In today's hyperconnected world, cyber threats move across endpoints, servers, networks, and cloud applications with alarming speed. Security teams face fragmented visibility, alert fatigue, and delayed responses. Nucleon XDR unifies detection and response across multiple data sources into a single platform. By leveraging Sigma-based detection rules and powerful correlation logic, it identifies suspicious activity, connects related events, and enables faster, more effective responses.

Why choose Nucleon XDR?

Breaks the silos – consolidates endpoint, network, and cloud signals into one platform for unified visibility.

Smarter detection – correlation rules link multiple events across sources to uncover complex, multi-stage attacks.

Noise reduction – fewer false positives by focusing only on alerts generated by real attack patterns.

Faster investigations – clear traceability from raw events → detection rules → alerts → response.

Flexible integration – easy configuration of diverse data sources (endpoints, servers, apps, network devices).

Analyst empowerment – intuitive dashboards with event details, alert insights, and contextualized response options.

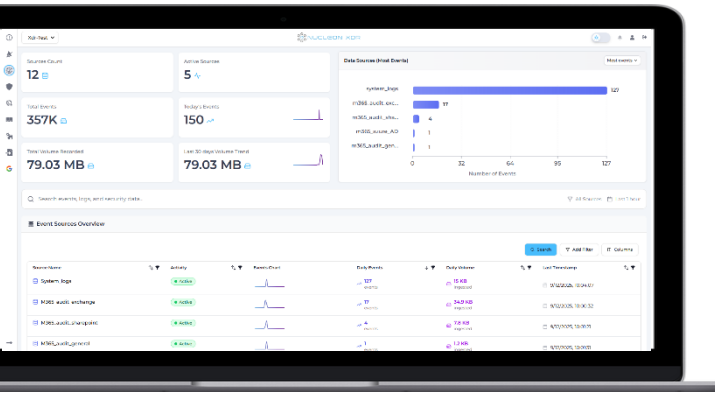
01 DATA SOURCES
Connect endpoints, network devices, cloud/SaaS and 3rd-party tools; configure format templates once

02 INGESTION
Events are parsed, indexed and tagged by Sigma detection rules

03 CORRELATION
Link one/many tagged events across sources/time via four rule types (single-query, temporal, event-count, static-match)

04 ALERTS
Alerts are displayed when each correlation rule is triggered

05 RESPONSE
Trigger source-aware actions (e.g., isolate endpoint, block IP) manually or automatically

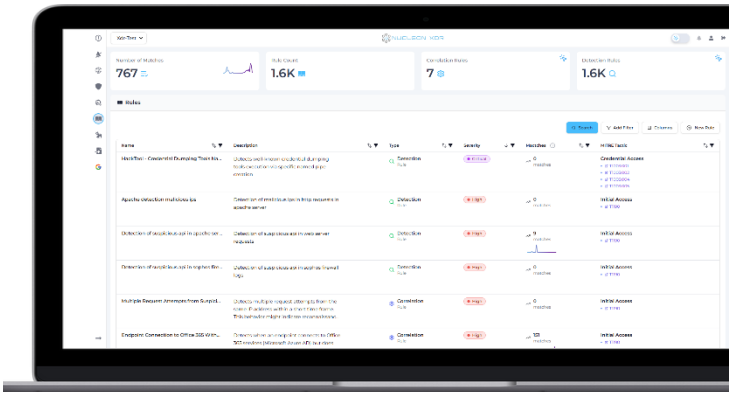


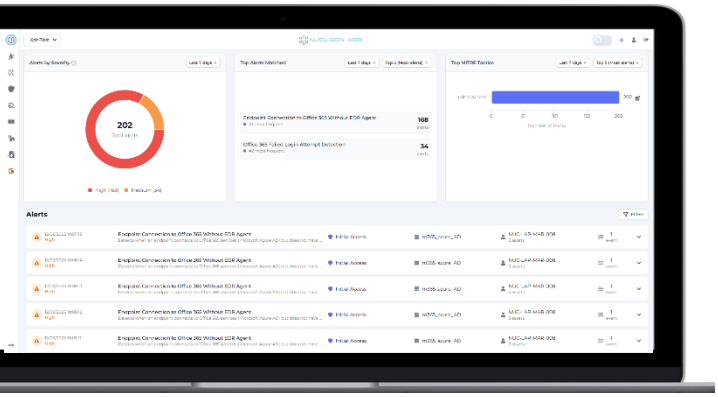
Complete Visibility at a Glance

Nucleon XDR centralizes telemetry from all connected data sources endpoints, servers, firewalls, cloud, and applications into a single analyst-friendly dashboard. Events flow in real time, giving teams a clear overview of activity, source health, and potential anomalies.

Events with Detection Rules

As events are ingested, they are automatically parsed, normalized, and evaluated against Sigma-based detection rules. Each event is tagged with relevant logic — highlighting suspicious behaviours or known attack techniques. This transforms raw logs into structured insights, reducing noise.





Business Contextual Protection

Analysts can easily create and edit correlation rules that reflect their unique environment. By defining logic across multiple events, time windows, or sources, Nucleon XDR adapts to business-specific attack scenarios. This flexibility ensures that detection is not just generic but context-aware.

Real World Use Cases

M365 brute-force

Detects and correlates failed login attempts to stop account takeovers

Unmanaged host login

Flags rogue or unmanaged devices logging in outside secured perimeters

XDR

Web attack across layers

Correlates firewall and server logs to expose hidden intrusion attempts

One-click response catalog

Executes preconfigured, source-aware response actions instantly

4.7 ★★★★★ Gartner Peer Insights™

Microsoft Virus Initiative

ABUSE.ch

ROYAUME DU MAROC
ADMINISTRATION DE LA DEFENSE NATIONALE
DIRECTION GENERALE DE LA SECURITE DES SYSTEMES D'INFORMATION

HAFS
Distributeur à valeur ajoutée

VOTRE PARTENAIRE TECHNOLOGIQUE
POUR DES INFRASTRUCTURES IT SÉCURISÉES ET PERFORMANTES

EXPERTISE
Des solutions adaptées à chaque environnement

CONFIANCE
Un partenaire fiable à vos côtés

PERFORMANCE
Des infrastructures sécurisées et évolutives

SUPPORT
Un accompagnement technique de qualité

HAFS
Distributeur à valeur ajoutée

Des solutions IT innovantes pour un monde connecté et sécurisé

WIRELESS RADIO
Connectivité sans fil haute performance

RÉSEAUX & SÉCURITÉ IT
Des réseaux fiables et sécurisés

VIRTUALISATION CLOUD
Des solutions Cloud flexibles et évolutives

CYBERSECURITY
Protéger vos données et vos systèmes

VIDÉO PROTECTION
Solutions de vidéosurveillance intelligentes

HCI STOCKAGE SAUVEGARDE
Stockage, sauvegarde et haute disponibilité

SOLUTIONS IT | CYBERSÉCURITÉ | CLOUD | INFRASTRUCTURE RÉSEAU | STOCKAGE | PROTECTION



Département Commercial

HAFS
Distributeur à valeur ajoutée

Vous accompagne

HAFS NETWORKS WCA
+225 07 89 82 56 49 / +225 07 59 05 85 82
sales-ci@hafs-networks.com

HAFS NETWORKS FRANCE
+33 (0)7 49 92 62 57 / +33(0)9 73 89 20 39
sales@hafs-networks.com

Distributeur à Valeur Ajoutée de Solutions de Cybersécurité | Réseaux | Wi-Fi | HCI/Sauvegarde

Hillstone NETWORKS | Synology | SANGFOR | SECPOINT | Axidian | NEOWAVE | HORNETSECURITY FORMERLY vade | CyberShield

RUCKUS NETWORKS | Ruijie Reyee | RAY | Wiflyx | SEARCHINFORM | MOBOTIX | EXTRAVIS | HAFS MediVision