Six Essential Requirements for Network Detection and Response (NDR)

To effectively detect and quickly respond to threats that can lead to a major incident, organizations need an innovative solution that goes beyond the capabilities of legacy network security tools. Network detection and response (NDR) is that solution.

NDR taps into the inherent power of network traffic and is fast becoming an essential security monitoring tool for enterprises because of its ability to uncover serious and imminent risks from network activity, generate evidentiary logs, and facilitate rapid incident response.

There are six essential characteristics of an effective NDR system that should be considered by organizations as they evaluate network-based threat detection and response solutions.

STAMUS NETWORKS

Sophisticated detection

Automated detection from multiple techniques

- Explicit rules
- Machine learning
- Behavioral analytics
- Stateful logic
- 3rd party threat intel
- Statistical anomalies

- No single tech can detect all threats
- Immediate detection results on day 1
- Uncover hidden threats
- Evidence for investigation & hunt

Transparent, explainable results with evidence

- Asset-oriented insights into network activity
- Timeline of threats & activity on assets
- All related events, including flows, protocol transactions, packets, and extracted files

- Total view of attack & impacted assets
- Clearly communicate results response
- No mysterious "black box" detections

High-fidelity response triggers

- High-confidence alerts for critical threats
- Confidently trigger automated response
- Virtually eliminate false positives

- Rapid response to fast-moving attacks
- Confidence encourages investigations
- Differentiate between context and critical security events

Guided threat hunting

- Analytics for proactive threat hunting
- Built-in or customizable filters
- Query metadata from event logs, flows, transactions

- Automated detection will miss threats
- Inexperienced analysts need guidance
- Security teams can focus on most critical items first

Openness and extensibility

- NDR only part of the solution
- Integrations with SOAR, SIEM, XDR, and IR
- Leverage 3rd party & custom threat intelligence

- NDR does not address all security needs
- Straightforward integrations are required
- Optimize for organization-specific needs
- Access to the best of breed tech

Complete data sovereignty

- Deploy central analytics system in private cloud, on premise, or in completely air-gapped environment
- No SaaS analytics required

- Control where sensitive data lives
- No shipping probe logs to 3rd party
- Keep all data in-country

SN-ER-NDR6-112023-1

5 Avenue Ingres
75016 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

contact@stamus-networks.com
www.stamus-networks.com

STAMUS NETWORKS