NetWorks
GROUP

WWW.NETWORKSGROUP.COM

MANAGED DETECTION & RESPONSE

Strengthen Your Security

Service Overview

NetWorks Group Managed Detection & Response service provides a comprehensive service to collect, analyze, and store log data from endpoints, network infrastructure, servers, and applications to detect and respond to security threats. The service leverages NetWorks Group's proprietary threat detection & response platform to determine important security events and then correlate, validate, investigate and alert on potential incidents.

Log Aggregation

Logs are securely collected in a manner that works best for the architecture of the target environment, either via an on-site collector or NetWorks Group's log collector in the cloud and are securely tunneled to the NetWorks Group's threat detection and response platform.

Threat Hunting

Our threat detection and response platform leverages big data tools to apply threat intelligence and advanced security analytics to the collected log data. Our security analysts actively hunt through these logs to identify indicators of compromise and validate if a security incident has occurred within the environment.

24x7x365 Response

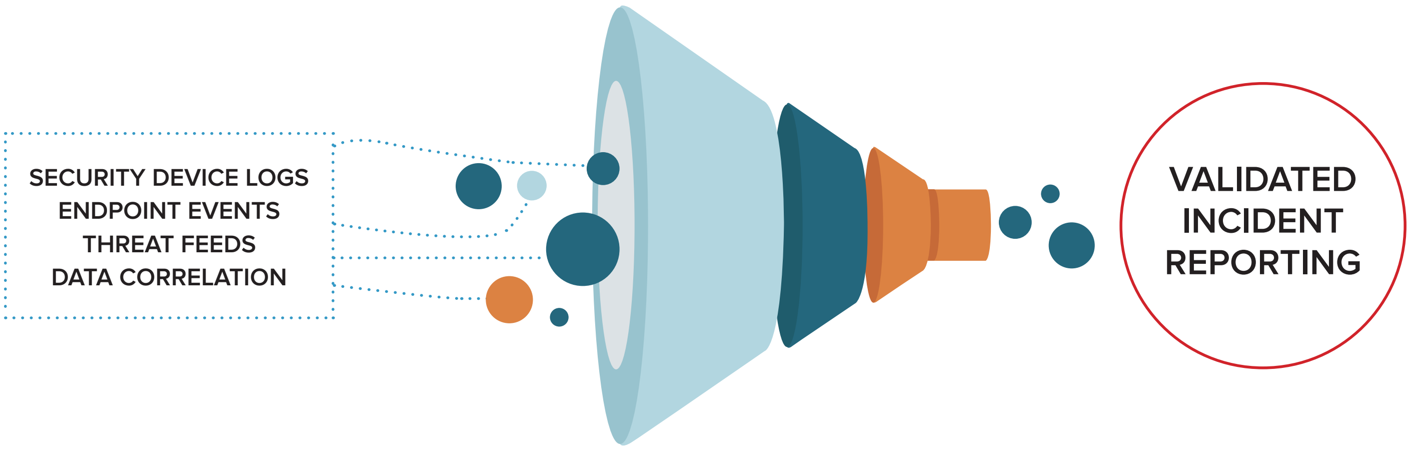
Using automated alerting, threat feeds, and tools, any security events that need immediate attention are escalated to senior security analysts 24x7x365. If the initial investigation demonstrates the need for immediate action, the events are escalated to a security incident and appropriate customer team members are notified with recommendations for resolution.

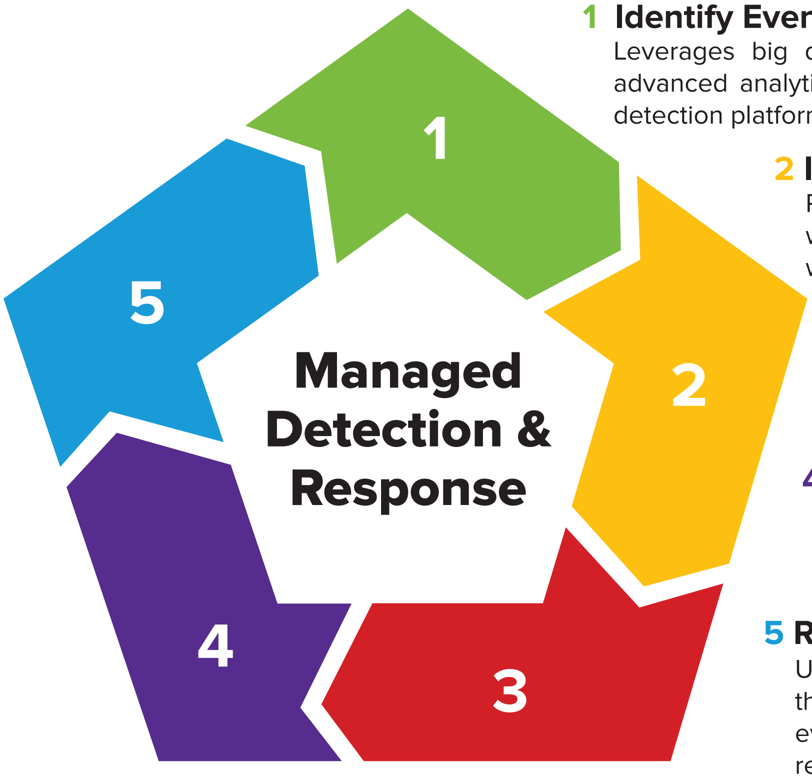
Features

- 24x7x365 monitoring and visibility into threats
- Quick breach notification
- Leverage known threat details to identify ongoing incidents
- Customer Portal for visibility into identified incidents
- Flexible alerting
- Supports common log types

Benefits

- Supports compliance efforts
- Fast and frictionless startup compared to SIEM tools
- Correlates multiple devices and log types to provide high-level view to investigators
- Context around how threats relate to the environment
- Faster identification of potentially infected devices
- Prioritize events based on threat and risk profile
- Ability to focus staff on validated incidents & threats





1 Identify Events

Leverages big data tools to apply threat intelligence and advanced analytics to data combined with proprietary threat detection platform to determine potential security events.

2 Investigation & Research

Potential adverse events are researched in concert with related data to determine is an incident occurred within the environment.

3 Prioritize & Define Incident

The threat detection platform determines the prioritization and categorization of the incident, allowing for an organized remediation plan.

4 Recommendations

Analysts provide clear recommendations on what happened, how it happened, and how to react to as well as remediate the issue.

5 Remediate & Track

Utilizing the Customer Portal, customers can track the progress and status of all events and discuss events with MDR Security Analysts, allowing for easy remediation and auditing of past events.

Key Differentiators of NetWorks Group MDR

NetWorks Group helps organizations detect and respond to advanced cybersecurity threats through a powerful combination of our proprietary threat detection platform, expertise and security tools. Our unique approach to security not only helps you stay ahead of cyber criminals but also helps you reduce cost and increase efficiency.

Our service adapts to new threats based on a consistent feedback mechanism built into the platform and offers actionable intelligence once a security threat is detected. The ability to actively hunt through logs to identify indicators of compromise has helped us achieve one of the fastest time to detect and lowest false positive rates in the industry.

Unlike other options for detecting security events, NetWorks Group's MDR service provides context to your security events. A team of expert resources become an extension of your team, immediately driving access to Senior Security Analysts and Engineers who understand the environment and the threats that pose the most risk.

In addition to a better security posture, insight into real-time events, and a 24x7x365 always-on experienced security staff, PCI compliance is attainable with ease. Identifying and researching adverse events, creating and prioritizing security events, as well as researching remediation can be a time-sink, NetWorks Group MDR takes a complicated but necessary security need and makes it simple.

NetWorks
GROUP

NetWorks Group is a Managed Detection & Response (MDR) and Ethical Hacking Service provider. Founded in 1997, we have over 20 years of experience delivering security services aligned with your infrastructure and compliance needs. Our team is comprised of some of the most experienced, well-rounded, and security-conscious people in the industry.

Learn More (888) 798-1012 | sales@networksgroup.com

100 S. Main St, Suite 200, Ann Arbor, MI 48104

networksgroup.com

@networksgroup