SERVICE OVERVIEW

nuspire

Managed Detection & Response

Detect attacks immediately, with real-time threat detection and 24x7x365 monitoring by expert cybersecurity analysts.

Accelerate Cyber Threat Detection, Response and Remediation Across Your Entire Network and Security Infrastructure

DETECT AND RESPOND TO ATTACKS IN REAL-TIME

Isolate Threats and Minimize Impact

Nuspire's dedicated team of threat analysts monitor, triage and respond to security incidents 24x7x365. Our analysts examine a variety of threat intelligence feeds to perform advanced analytics and investigate indicators of compromise (IOCs). The team then references clients' custom runbooks to inform detection and response actions.

DIFFERENTIATE REAL THREATS FROM THE NOISE

Reduce Alert Fatigue

Our cybersecurity experts distill billions of logs into a handful of actionable events. Receive fast and accurate response to security incidents as our team correlates security events with Nuspire's proprietary threat intelligence to reduce false positives — all while leveraging your existing tech stack.

AUGMENT YOUR TEAM WITH 24/7 EXPERTISE

Add Expertise without Adding Headcount

Our passionate cybersecurity experts engage as an extension of your security team — holding themselves accountable for your success. Nuspire supports clients with three 24x7x365 security operations centers (SOCs), providing rapid response times to minimize impact and expedite recovery. We log endpoint activity and retain client logs for a rolling 400 days — at no additional cost.

SERVICE COMPONENTS

- Smart Start custom client onboarding experience
- Log collection and retention for 400 days
- Ongoing tuning of security rules
- Threat detection and alerting based on a customized runbook
- Threat intelligence incorporated into SIEM
- Active remediation and guidance for detected threats
- Threat hunting for active threat scenarios
- Real-time security information and recommendations
- Flexibility to choose between self-service or guided security reviews to improve security posture
- Client portal access to interact with SOC, dashboards and reports

SERVICE BENEFITS

- Accelerate cyber threat detection and response to minutes, not days
- Receive real-time incident validation
- Remediate threats effectively
- Leverage skills not available in-house
- Gain 24x7x365 expert support

Managed Detection & Response | Use Cases

RANSOMWARE

1. Critical systems in the ransomware attack path provide early indicators of compromise.
2. Upon early detection, a Nuspire SOC analyst refers to the client's custom runbook to understand the environment, industry and special instructions.
3. If determined to be a false positive, we re-evaluate the detection criteria. If determined to be a threat, our SOC analyst will move to the investigation phase.
4. The SOC analyst provides detailed tracking of all actions taken and communicates the situation with the client.
5. The SOC analyst then executes relevant playbook, identifies which hosts are infected and checks for lateral movement.
6. Nuspire (or the Asset Authority) contains the threat and initiates recover. The team blacklists IPs, domains and/or URLs associated with the anomalous traffic.
7. The SOC analyst identifies gaps in security controls and makes recommendations to proactively prevent future attacks and reduce risk.

PHISHING

1. Client submits a ticket indicating they fell victim to a phishing scam.
2. Our SOC analyst reviews logs for unusual logins. They validate the threat, research its origin and determine how many people are affected.
3. The SOC analyst notifies the client after validation.
4. Nuspire (or the Asset Authority) blacklists any IPs, domains or URLs associated with the phish or its C&C communication.
5. Nuspire (or the Asset Authority) purges reported phishing messages from inboxes, identifies and contains potential compromised accounts, and changes passwords
6. Nuspire identifies gaps in security and makes recommendations to prevent future phishing attempts.

DETECTION OF UNAUTHORIZED ACCESS

1. Nuspire SIEM triggers security alert indicating suspicious network traffic. Our SOC analyst determines the scope of the attack using the log received. They then profile the source of suspicious traffic to determine scope.
2. The SOC analyst notifies the client of unauthorized activity.
3. Nuspire (or the Asset Authority) will contain potentially compromised accounts and change passwords to those accounts.
4. Nuspire (or the Asset Authority) reviews user access rules and implements principle of least privilege.
5. Nuspire's SOC identifies gaps in security controls and makes recommendations to prevent future attacks.

nuspire

Nuspire is a leading managed security services provider (MSSP) that is revolutionizing the cybersecurity experience by taking an optimistic and people first approach. Our deep bench of cybersecurity experts, world-class threat intelligence and 24x7 security operations centers (SOCs) detect, respond and remediate advanced cyber threats. We offer comprehensive services that combine award-winning threat detection with superior response capabilities to provide end-to-end protection across the gateway, network and endpoint ecosystem. Our client base spans thousands of enterprises of all sizes, across multiple industries, and achieves the greatest risk reduction per cyber-dollar spent. At Nuspire, we are laser focused on delivering an extraordinary cybersecurity experience that exceeds client expectations.

For more information, visit nuspire.com and follow @Nuspire

nuspire.com
LinkedIn @Nuspire
Twitter @NuspireNetworks