N4 Threat Detect Services

Technical Description

Public

Node4 Limited

25/04/2016

INTRODUCTION

N4Threat Detect is a Threat Intelligence managed service. By monitoring network traffic, server traffic, scanning for internal and external vulnerabilities as well as performing web application penetration testing, N4Threat Detect provides a reactive service alerting the client to potential threats and system attacks.

Information discovered by the service will be critical to the security integrity of the client. It is important that the information from the service is escalated to the appropriate areas within the client's organisation that mitigating actions can be taken by the clients IT department.

If we assume that eventually, a breach will take place it is critical to detect and respond as soon as possible. How can this detect and response window be reduced to stop the outflow of client information, stop the spreading of infection and limit the damage done?

Implementing N4Threat Detect will;

- identify possible weaknesses in network and host assets before the breach
- identify persistent attacks to block the threat
- detect malicious activity in order to identify the target
- detect data breaches and prevent data loss
- manage compliance and reporting goals

N4Threat Detect will be your Security Operations Centre (SOC), utilising the Kill Chain Taxonomy to highlight the most important threats facing your network and the anomalies which should be investigated. The N4Threat Detect SOC team will see the types of threats directed against your network, when known bad actors have triggered an alarm and escalate level 4 & 5 alarms to your internal IT team for investigation.

The Kill Chain Taxonomy breaks out threats into five categories, allowing you to understand the intent of the attacks and how they're interacting with your network and assets:

- Level 5 - System Compromise – Behaviour indicating a compromised system.
- Level 4 - Exploitation & Installation – Behaviour indicating a successful exploit of a vulnerability or backdoor/RAT being installed on a system.
- Level 3 - Delivery & Attack – Behaviour indicating an attempted delivery of an exploit.
- Level 2 - Reconnaissance & Probing – Behaviour indicating an actor attempt to discover information about your network.
- Level 1 - Environmental Awareness – Behaviour indicating policy violations, vulnerable software, or suspicious communications.

N4Threat Detect will also provide vulnerability scanning of internal and external facing assets. Identifying vulnerable software and applications within your attacker who will also be looking for them.

Additionally, web application penetration testing can be performed to identify weaknesses in your web application code. Utilising the Open Web Application Security Project (OWASP) framework, the top 10 known web application attacks are run against your application in a controlled manner in order highlight weaknesses and information leakages.

Intrusion Detection and Alerting Nids: Detecting Attacks to your Network

Utilising Network Intrusion Detection Systems (NIDS), N4Threat Detect provides real-time analysis of network traffic entering and exiting your network. Threats targeting your vulnerable systems are detected with signature-based anomaly detection and

protocol analysis technologies. By scanning the network traffic for known signatures, N4Threat Detect identifies the latest attacks, malware infections, system compromise techniques, policy violations, and other exposures. Examples of such attacks are;

- System Compromise – Behaviour indicating a compromised system.
- Exploitation & Installation – Behaviour indicating a successful exploit of a vulnerability or backdoor/RAT being installed on a system.
- Delivery & Attack – Behaviour indicating an attempted delivery of an exploit.
- Reconnaissance & Probing – Behaviour indicating a bad actor attempting to discover information about your network.
- Environmental Awareness – Behaviour indicating policy violations, vulnerable software, or suspicious communications.

The N4Threat Detect NIDS does not require agents installed on systems to identify the threats, therefore not impacting the performance of any hosted applications. Multiple sensors can be deployed through your network to correlate disparate events from multiple devices. The N4Threat Detect SOC team monitor the NIDS in order to detect activity early in the kill-chain, and possibly prevent an attack.

Hids: Detecting Attacks to your Services

By utilising Host Intrusion Detection System (HIDS), N4Threat Detect will analyse system behaviour and configuration status to track user access and activity. Detect potential security exposures such as system compromise, modification of critical configuration files (e.g. registry settings, /etc/passwd), common rootkits, and rogue processes.

With host intrusion detection, you gain granular visibility into the systems and services you're running so you can easily detect:

- System compromises
- Privilege escalations
- Unwanted applications
- Modification of critical configuration files (e.g. registry settings/etc/password)
- Malware
- Rootkits
- Rogue processes
- Critical services that have been stopped
- User access to systems and applications

Vulnerability Scanning

Vulnerability management is the "cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities. Once vulnerabilities have been identified, remediation is required. Since thousands of vulnerabilities are discovered each year, and seemingly never-ending security updates and patches required, remediation needs to be prioritised. Since newly-found vulnerabilities are constantly surfacing, and the IT infrastructure is typically changing over time, consistent diligence is required for effective vulnerability management.

Vulnerability Management from the Inside

Utilising internal agent technologies, vulnerability assessments of internal network systems are conducted each month to expose potential attack vectors before they become targets. Remediation plans drawn up to mitigate the vulnerability.

Vulnerability Management from the Outside

External vulnerability scanning specifically examines an organisation's security profile from the perspective of an outsider or someone who does not have access to

systems and networks behind the organisation's external security perimeter. Conducted monthly, potential attack vectors are exposed before they become targets with remediation plans drawn up to mitigate the vulnerability.

Web Application Penetration Testing

In addition to vulnerability scanning, Node4 recommend quarterly penetration testing of the primary business application.
The goals of a penetration test are;

- Determine feasibility of a particular set of attack vectors
- Identify high-risk vulnerabilities from a combination of lower-risk vulnerabilities exploited in a particular sequence
- Identify vulnerabilities that may be
- difficult or impossible to detect with automated network or application vulnerability scanning software
- Assess the magnitude of potential business and operational impacts of successful attacks
- Test the ability of network defenders to detect and respond to attacks
- Provide evidence to support increased investments in security personnel and technology
- Communicate remediation plans where applicable.

Utilising the Open Web Application Security Project (OWASP) framework, the top 10 known web application attacks are run against your application in a controlled manner in order highlight weaknesses and information leakages. The OWASP top 10 is as follows;

- Injection (often found in SQL, LDAP, Xpath, or NoSQL queries; OS commands; XML parsers etc)
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Components with Known Vulnerabilities
- Invalidated Redirects and Forwards

Web application pen testing is a manual process performed over a number of days and utilises Open Source tools. Dialogue is maintained with the client throughout the process as there is potential to cause downtime if the tests are performed on the live website.

Service Levels

Essential, Enhanced and Elite

The N4Threat Detect service is presented in 3 levels giving you the choice of services suitable for your security posture.

	Essential	Enhanced	Elite
Network Threat Alerts	YES	YES	YES
Host Threat Alerts	No	YES	YES
Custom Threat Alerts	No	No	YES
Vulnerability Scanning	No	YES	YES
Security Advisor	1 hour pcm	3 hours pcm	5 hours pcm

Reports	5	10	15
Web Pen Testing	No	No	YES
Live Dashboard	YES	YES	YES

Scheduled Reports

The N4Threat Detect service also offers scheduled reports of a customers' Service

Profile to an email address. These reports can be based on;

- Alarm Report
  - Top Attacked Hosts
  - Top Attacking Hosts
  - Top Alarms
  - Top Alarms by Risks
  - Top Destination Ports
- Assets
  - Alarms
  - Security Events
  - Vulnerabilities
  - Inventory
- Availability
  - Trends
  - Performance
- Logons
  - Firewall
  - Failed
  - FTP
  - Database
- Compliance
  - PCI DSS 3.1 Report
  - HIPAA
  - FISMA
  - ISO27001
  - SOX

Please contact Node4 for any questions relating to this document or enquiries regarding N4Threat Detect services; please email sales@node4.co.uk or call 0845 1232222.