Integrity360

your security in mind

Managed Network Detection and Response

Service Description for G-Cloud 15

Table of Contents

1 Document Purpose

This document serves as the official service description for the Integrity360 Managed Network Detection and Response (NDR) service.

The aim is to describe, in simple terms, the service, the deliverables of the service and the associated benefits. This is described in a non-technical and vendor agnostic way. More detail can be provided when engaging with our team so that we can understand your specific requirements.

- Please visit: https://www.integrity360.com
- Phone: +44 20 3397 3414
- Email: info@integrity360.com

2 Introduction

2.1 What is NDR?

The term Network Detection and Response (NDR) was coined in 2019 by Gartner. NDR uses a combination of AI, machine learning and advanced analytics to detect anomalous or suspicious activity on enterprise networks.

A big part of the value proposition with NDR is the automation of detection and response capabilities which drastically reduce the associated manual effort, reducing SOC fatigue and alert overwhelm, while also supporting threat hunting, forensics and incident response use cases. NDR differs to traditional threat detection capabilities like EPP and IDPS in that these systems are typically signature based, i.e. known malicious malware signatures and indicators of compromise, whereas NDR detection is typically anomaly based, more sophisticated, using machine learning to identify normal patterns of activity and identifies deviations from this baseline as well as behaviours associated with threat actor methods and techniques. NDR extends the threat detection coverage of other core detection and response solutions such as Endpoint Detection and Response (EDR) and Identity Threat Detection and Response (NDR) to uncover undetected threats and suspicious traffic patterns in the network.

3 Scope of the Service

3.1 Service Overview

Utilising a NDR technological stack, Integrity360's SOC can detect security issues in real time and respond promptly to them. Our NDR managed service is part of a broader portfolio designed to provide a complete suite of managed security services, addressing the full lifecycle of necessary controls:

- **Threat exposure management** – Risk-based Identification and prioritisation of exposure to threats.
- **Threat prevention** – Detect and prevent unwanted and malicious activity.
- **Threat monitoring, detection and response** – Monitor, detect, and respond to threats in the customer's environment.

Our service approach:

1. **Architecture review** – Customer's architecture review and solution sizing: appliance type (hardware, virtual), sensors (virtual, local, cloud), etc.
2. **Deployment/Implementation** – Sensors will be strategically placed across customer's networks, including the Data Centre (DC), and Cloud, to capture and analyse network traffic. These sensors continuously collect network metadata and feed it into the detection engine.
3. **Deployment/Implementation** – Our MDR platform integrates and collects alerts and telemetry from the NDR solution.
4. **Monitoring and Response** – Our SOC Team will receive the alerts and will have complete visibility of the customer environment using the NDR platform.

Leveraging the *ingress* and *egress* network traffic monitoring, we can oversee some key use cases as follows:

- **Initial Intrusion** – NDR can reveal well-known exploits such as Log4J, Hafnium, Kaseya, as well as thousands of lesser-known exploits on a regular basis (unusual incoming RDP, application protocol to uncommon port, unusual file download, etc.).
- **Detects lateral movement between hosts and network segments** – As an attacker begins to increase their knowledge of the network, perform scans, and escalate their privileges - for instance by obtaining admin credentials, NDR correlates thousands of data points.
- **Data Exfiltration** – Whether smash and grab or a low and slow, NDR identifies subtle deviations in activity (anomalous SMB traffic, unusual external data transfer, etc.).
- **Data Encryption** (additional extension appended to SMB file, sustained MIME type conversion, possible ransom note, etc.).
- **Insider Threat** – NDR understanding of normal patterns of life allows it to stop threats on the inside (sustained SSL and HTTP increase, anomalous file download, multiple unusual file uploads, fast beaconing to DGA, etc.).
- **Credential stuffing** – On the network side, NDR can detect instances of credential stuffing through a number of unusual behaviours (Kerberos username brute force, etc.).

3.2 Service Tiers and Features

Integrity360's Managed Threat Detection and Response service portfolio combines and integrates industry leading Threat Detection & Response platforms with our unparalleled security expertise to proactively monitor and protect customers from threats.

We offer two tiers of services for our NDR managed services:

1. Managed Threat Detection (MTD)
2. Managed Detection and Response (MDR)

3.2.1 Managed Threat Detection (MTD)

The Managed Threat Detection (MTD) service tier includes all aspects of managing the platform, integration into Integrity360 SOC for alert ingestion, analysis and incident management, 24x7x365.

- NDR platform management and support
- Platform health monitoring
- Continuous detection tuning
- Alert triage and investigation
- Threat intel integration
- Alerting customers if a qualified incident has been detected

3.2.2 Managed Detection and Response (MDR)

Managed Detection and Response (MDR) is the highest-level of service within our portfolio and is supported across a wide configuration of underlying platforms (SIEM, EDR, NDR, XDR, ITDR, CDR). This level of service can be offered with the NDR platform alone or in conjunction with any of these other technologies.

The MDR service is a comprehensive detection and response service where Integrity360 can act to rapidly contain detected threats according to pre-defined response actions.
This service includes:

- All platform management and managed threat detection components
- Threat Detection, Response and Containment
- Elective rules of engagement per use case (evolves with service)
- Support for platform native response actions and playbooks

With a broader range of MDR services, response can be integrated into a wide variety of control points, including endpoint, network, and identity solutions. If it's a service exclusive to the NDR platform, then we only take action that is enabled on the platform itself.

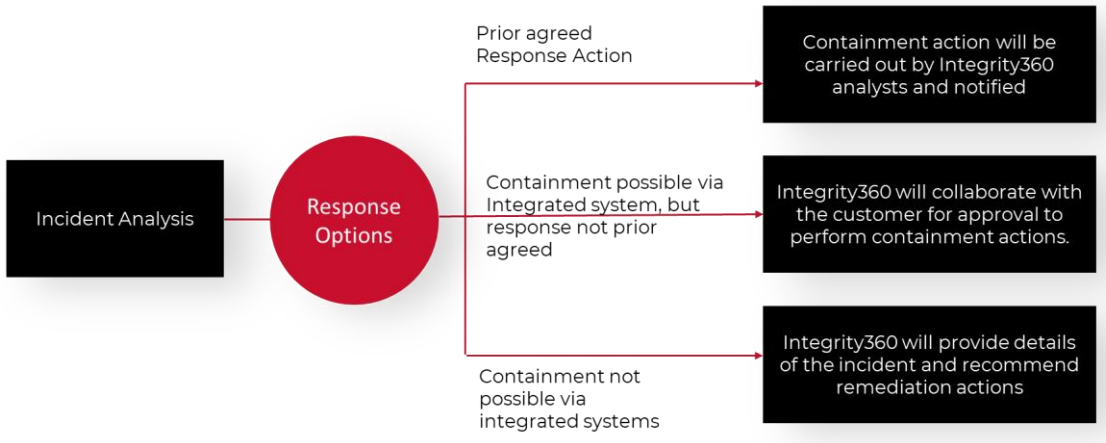
4 Security Incident Management

This section describes the lifecycle of incidents and how they are handled through the stages of Triage, Investigation, Response and Reporting. The Incident Lifecycle is underpinned by the Integrity360 Aegis platform which combines related alerts into a single case for effective handling during the incident lifecycle.

Alert Triage
Alerts will be checked by the security analysts team and triaged. The principle followed is to look at the alerts and quickly analyse the traffic that goes around these alerts and make sure the traffic matches what we expect from a security threat. The goal is to remove false positive alerts at the earliest stage. Once they have been triaged and categorised (using our categorisation matrix), an incident notification is sent to the client team if moving to investigation stage. The case then may be assigned to the specialised analyst for further investigation.

Incident Analysis
Integrity360 will carry out security incident analysis on incidents. The incident ticket will be assigned to the security analyst for investigation, based on priority and in line with the SLA.
Verified security incidents will be notified to the client automatically upon creation through the agreed communication method, purely as a notification that one or more alerts have been received by the Integrity360 SOC that are deemed to be an incident and is actively being investigated. This information will be updated once the investigation is completed and, depending on the ability for Integrity360 to respond on behalf of the client, will either include response actions carried out or recommendations and actionable intelligence for the client.
Where, following analysis & investigation, it is deemed a response is required, it will enter the security incident response stage. Incidents deemed as false positives will be marked and closed.

Incident Response
Integrity360 will respond to investigated incidents to contain and mitigate the acute threat presented. Threat will be responded to in one of three ways:



Agreed Rules of Engagement drives response option

Exception: Response actions executed within the MDR service are limited to the scope of pre-agreed response integrations, and only where the action has been pre-approved as part of the Response Rules of Engagement.

5 Integrity360 Client Portal

The Integrity360 Client Portal is a secure, user-friendly platform designed to give clients real-time visibility and control over their service. It streamlines communication, reporting, and incident tracking, enhancing collaboration between clients and the Integrity360 service teams.

Key Features include:

- **Dashboard Overview**
  - Access to Threat Detection & Response metrics
  - Visibility of open security incidents, escalated alerts, and service summaries
  - Interactive graphs showing ticket trends and top assets
- **Ticket Management**
  - Log, view, and update Incident, Service Request, and Change Request tickets
  - Quick filters for open tickets, escalated alerts, and awaiting client action
  - Export ticket data for internal reporting (CSV format)
- **Reports**
  - Monthly MDR reports with analyst commentary and service summaries
  - SLA reports showing performance against service targets
  - Threat Hunting and Threat Intelligence reports available for download
- **Detections Library**
  - View latest threat detection content deployed by Integrity360
  - Search and browse detection rules by category or name
- **CVE Dashboard**
  - Access to Common Vulnerabilities and Exposures (CVEs) database
  - Filter by severity and view last 30 days' statistics
- **Documents Repository**
  - Centralised access to service reviews, reports, and shared documentation
- **User Management**
  - Role-based access control with read-only or read-write permissions
  - Easy onboarding of additional users via Service Management Team
- **Support Access**
  - Direct contact details for Integrity360 Service Desk and Service Management Team
  - Action Required banner for tickets needing client input

The portal is updated and improved regularly, with latest release notes being shared with the client.

6 Next Steps

Work with us to ensure that your business maintains a proactive security stance in a field where new threats emerge daily. Contact an Integrity360 advisor today to learn more about our services.

www.integrity360.com