Cybersecurity – Intuitus Managed Detection and Response (MDR) Service Guide

Version 2025.04.21

Contents

1. Introduction

This Service Guide describes the different cybersecurity services offered by "Intuitus" and resold by Intrado Safety Solutions Corp. ("Intrado"), which are performed for end customers (each, a "Customer"), each as detailed more fully herein (collectively "Services").

2. Services Overview

2.1. Managed Services

Intuitus Managed Services are operated out of a cyber Security Operations Center (SOC) that supports Customers 24/7/365. The Intuitus cyber SOC provides both security monitoring and is staffed by expert Cyber Defense Analysts and other cybersecurity experts.

What is MDR? Managed detection and response (MDR) providers deliver 24/7 threat monitoring, detection and lightweight response services to customers leveraging a combination of technologies deployed at the host and network layers, advanced analytics, threat intelligence, and human expertise in incident investigation and response. MDR providers undertake incident validation, and can offer remote response services, such as threat containment, and support in bringing a customer's environment back to some form of "known good." – www.gartner.com

2.1.1. Network and Endpoint Monitoring Services

- **Network MDR**
  Intuitus Network Managed Detection and Response (MDR) provides 24/7 Security Operations Center (SOC) services that identifies and thwarts malicious activity on your network. Cyber Defense Analysts are assigned to customers and are dedicated to studying and understanding your unique network environment. Analysts become a part of your team and worry about cyber threats so you can focus on your business objectives. Network MDR includes weekly and monthly cybersecurity reports and Incident Response First Aid.
- **Endpoint MDR Complete**

  Endpoint protection is a cornerstone of cybersecurity. Securing all your endpoint devices is an easy and inexpensive way to thwart ransomware and other malicious threats that try to infiltrate your systems. Intuitus Endpoint MDR Complete is a fully managed threat hunting, detection, and incident response service that provides a dedicated 24/7 security team to detect and neutralize the most sophisticated and complex threats. Includes full Incident Response support.

- **Endpoint MDR Complete with Network Detection and Response (NDR)**

  Endpoint MDR Complete with NDR combines the Endpoint MDR Complete protection for endpoint devices with monitoring, detection, and response of your network. NDR monitors and protects data traversing your network, providing full network visibility. NDR enables Cyber Defense Analysts to visualize the network and the traffic flow between the monitored network and the outside world. As well, it monitors traffic flow between devices on the internal network thereby detecting lateral movements of threats. Includes full Incident Response support.

2.1.2. Firewall Services

- **Firewall + Firewall Management**

  Intuitus provides next-generation firewalls and firewall management for those who desire to leave the burden of configuring, fine-tuning, and updating their frontline cybersecurity defense to the professionals. Intuitus configures and fine-tunes firewalls based on the principles of Confidentiality-Integrity-Availability to the unique needs of your organization. Next-generation firewalls provide encrypted data protection and verification. Intuitus utilizes Sophos next-generation firewalls.

2.1.3. Email Protection Services

- **Central Email Advanced**

  Central Email Advanced provides cloud email security and advanced threat protection. Stop spam, malware, ransomware, and malicious URLs. Block malware-free phishing and impersonation attempts. Protect sensitive data with email encryption and data loss prevention. Inbound SPF, DKIM and DMARC authenticate senders and block attacks. Central Email Advanced utilizes deep learning artificial intelligence to block zero-day threats in their tracks.

2.2. Cybersecurity Consulting Services

Intuitus Cybersecurity Consulting provides customers with the information they need to protect their networks. Intuitus consulting can assist in the development of a cohesive security posture that enables organizations to respond more effectively when intrusions occur in their networks. Intuitus offers a range of cyber consulting services. If you do not see the service you need, talk to us. We offer custom consulting as well.

Do I need a Cybersecurity Assessment or a Cybersecurity Framework?

Both utilize recognized guidelines to assess your organization's cyber posture. However, the Cybersecurity Assessment includes a technical assessment to reveal the impactful vulnerabilities in your network environment and quickly spot priority exposures with a high likelihood of attack and business impact. The Cybersecurity Framework does not include the technical assessment but does include a gap-analysis of your cybersecurity posture, a "roadmap" to resolve or mitigate shortfalls, Cybersecurity Policies, and an Incident Response Action Plan.

2.2.1. Governance

- **Cybersecurity Policies**

  Organizations should adopt Cybersecurity Policies that comprise of industry standard best practices. Intuitus can tailor Cybersecurity Policies to the unique needs of your organization. Policies may include Acceptable Use, Password, Data Protection, Remote Access, and more. (Cyber) Security Policies are often a requirement for industry compliance or certifications necessary for government contracts.

- **Cybersecurity Assessment**

  Cybersecurity threats exploit the increased complexity and connectivity of infrastructure systems, placing businesses security, economic health, and safety at risk. Cyber threats can drive up costs and affect revenue. They can harm an organization's ability to innovate. Intuitus Cybersecurity Assessments analyze People, Processes, and Technology so organizations can comprehensively mitigate vulnerabilities.

  An Intuitus Cybersecurity Assessment includes a Vulnerability Assessment or an Internal Penetration Test to assess technical vulnerabilities. Intuitus then leverages the NIST Cybersecurity Framework or other desired assessment guidelines (e.g., ISO 27001 SCF, NENA NG-SEC

Checklist, SPRS score, etc.) to assess People and Processes. These recognized guidelines provide standardization as well as aid in meeting regulatory compliance requirements.

- **Cybersecurity Framework**

  Don't know what you need to do to have good cyber hygiene? Do you need an assessment of your organization's cybersecurity and a plan to mitigate security gaps? You need a Cybersecurity Framework. A Cybersecurity Framework will assess your organization's current cybersecurity posture and will outline a plan to get to a Target Profile. The Target Profile may be of your own designation, or it might be from an existing assessment guideline (e.g., NIST CSF, ISO 27001 SCF, NENA NG-SEC Checklist, SPRS score, etc.). A Cybersecurity Framework includes Cybersecurity Policies and an Incident Response Action Plan. A Cybersecurity Framework often satisfies multiple compliance requirements

2.2.2. Risk

- **External Penetration Testing**

  The "Pen" Test is designed to expose security vulnerabilities by emulating the latest tactics, techniques, and procedures in real time with real, simulated attacks. The Pen Test has a singular goal of compromising the organization and obtaining sensitive data or access to systems. Vulnerabilities that were used throughout the attack are delivered in a chronological timeline of events which lead to compromise and/or sensitive information disclosure.

  The External Pen Test replicates what a threat actor could do if attacking from the outside of your network and tests the perimeter defenses of the network. This test simulates a threat actor which has no prior knowledge of the internal network or the components within.

- **Internal Penetration Testing**

  Like the External Pen Test, the Internal Pen Test is designed to expose security vulnerabilities. However, an Internal Pen Test exposes misconfigurations, internal threats, and threats from active adversaries inside an organization's network.

- **Penetration Testing – Annual Subscription**

  An Annual Subscription allows for up to 12 Internal Pen Tests per year. The pen tests can be either internal or external. A subscription is a great option if an organization is dynamic and is constantly under change. Examples are if the organization is developing and testing new software, rolling out new applications, or modifying their network and desires to check for security vulnerabilities along the way. A subscription is a great value if your organization plans on conducting four or more Pen Tests per year.

- **Vulnerability Assessment – One-Time**

  Intuitus Vulnerability Assessments combined the capability of Tenable Vulnerability Management—the world's #1 vulnerability management solution—with Intuitus expertise to ensure the process is easy and understandable. Vulnerability assessments allow customers to gain full visibility to reveal the impactful vulnerabilities in your environment, quickly spot priority exposures with a high likelihood of attack and business impact, then take rapid and decisive action to close critical exposures and execute remediations. Includes one Vulnerability Assessment Report Review with a cybersecurity expert.

- **Vulnerability Assessment – Annual Subscription**

  Intuitus Vulnerability Assessments combined the capability of Tenable Vulnerability Management—the world's #1 vulnerability management solution—with Intuitus expertise to ensure the process is easy and understandable. Vulnerability Assessments allow customers to gain full visibility to reveal the impactful vulnerabilities in your environment, quickly spot priority exposures with a high likelihood of attack and business impact, then take rapid and decisive action to close critical exposures and execute remediations.

  An annual subscription allows for multiple assessments throughout the year that provide valuable feedback on the security of evolving networks or to meet compliance requirements. Includes one Vulnerability Assessment Report Review with a cybersecurity expert. Additional Report Reviews are an excellent option if customers desire ongoing analysis and feedback after each Vulnerability Assessment.

  Do I need a Vulnerability Assessment or a Penetration Test?

  A Vulnerability Assessment identifies and classifies potential weaknesses in an organization's IT infrastructure. The outcome is a high-level overview of potential vulnerabilities, their severity, and recommended remediation actions.

  A Penetration Test simulates real-world cyberattacks to uncover vulnerabilities that could be exploited by malicious actors. The outcome is a detailed report on vulnerabilities, their exploitability, and the potential impact of successful attacks.

- **Incident Response Action Plan (IRAP)**

  It is not if a cybersecurity incident will happen, but *when* it will happen. Companies need to be prepared by knowing what to do in advance. If a security incident is detected, the IRAP provides the vehicle to respond and mitigate it.

  Intuitus will produce a written IRAP that is tailored to the customer and gives clear step-by-step instructions on what to do next in the event of a cyber incident. Instructions include tasks by name or by position and playbooks to respond to the most common cyber incidents.

- **Incident Response (IR) Consulting**

  Many organizations do not have the on-hand expertise or experience to mitigate the damage caused by a cyber incident. Intuitus IR Consulting puts an IR specialist on your team to assist your personnel in going through the steps necessary to stop further damage and provide guidance on how to get your organization back to "normal."

2.2.3. Compliance

- **Compliance Consulting**

  Cybersecurity consultants will evaluate your organization to ensure the proper policies, procedures, and technology are in place to protect any organization's most important asset—information. Depending on the industry sector, whether it is finance, health, energy, communications, or other, there are unique rules that must be followed to protect that information. Our cybersecurity consultants are familiar with those rules and can help ensure compliance.

  Intuitus can provide:

  CMMC 2.0 Level 1 Certification

  CMMC 2.0 Level 2 Audit Prep

  NENA Security Audit (NG-SEC / STA-040.2)

  SIG Lite Audit Prep

  SOC 2 Type II Audit Prep and Certification

  SPRS Score

  Other (Contact us to see if we can help)

- **Cloud Security Management**

  Easily identify cloud resource vulnerabilities, ensure compliance, and respond to threats faster. Do you need an AI-powered security and compliance platform for public cloud environments that offers a real-time inventory of servers, storage, and network elements, helps manage resources, monitors security, and helps meet compliance standards? Cloud Security Management offers a range of features to help organizations manage their cloud security and compliance effectively:

  Multi-Cloud Visibility: Get a single view of security posture across AWS, Azure, Google Cloud, Kubernetes, and Infrastructure-as-Code environments. It offers asset and network traffic visibility, continually analyzing for security risks, over-privileged access, and spend anomalies.

  Security and Cost Optimization: Fix security gaps fast, optimize cloud costs, and stay compliant by automating compliance assessments and producing audit-ready reports instantly.

  Secure DevOps: Get security and compliance checks at any stage of the development pipeline to scan container images and Infrastructure-as-Code templates to block vulnerabilities pre-deployment.

  AI-Powered Security Automation: Automate security and compliance checks, providing a real-time inventory of servers, storage, and network elements in the cloud.

  Compliance Monitoring: Continuously monitor compliance and get reports for standards such as SOC2, HIPAA, and GDPR.

2.2.4. Cybersecurity Training

- **Cybersecurity Tabletop Exercises (TTX)**

  A TTX provides training so that each participant knows exactly what to do in the event of a cyber incident. A TTX consists of simulating known and emerging threats against critical assets and processes in a real-world context where conclusions are documented without disruption to actual assets. These facilitated simulations equip participants with the knowledge to identify and respond effectively to real and potential cyber threats and associated risks.

  The TTX is made up of progressively complex scenarios, such as a phishing attempt that leads to a ransomware attack. Each scenario is scripted to be as close to reality as possible, leading to identification of security gaps and vulnerabilities to be addressed. The scenarios are carefully planned to achieve identified goals and learning objectives.

2.2.5. Other Consulting Services

- **Onsite Services**

  Often, customers require cybersecurity consulting for a unique situation or unique to their industry. Intuitus can help. Intuitus offers a range of cybersecurity expertise that is not specifically listed. Contact us with your problem and Intuitus can help solve it.

  Intuitus also offers onsite services when a customer requires cybersecurity experts to be at the Customer's location to: a) assist with a security incident response or cyber incident, b) provide cybersecurity consulting services, or c) provide data forensic analysis support. Sometimes it is invaluable to have an expert onsite to help.

Onsite teams might be used:

- When there is a unique cybersecurity situation
- For sensitive security reasons
- During Incident Response
- When determined that the problem cannot be resolved remotely (i.e. via phone, secure messaging, remote desktop, etc.)
- When the customer does not have the technical expertise onsite to action critical cybersecurity-related items (e.g. Installations, modifications, troubleshooting, etc.)

3. Implementation Cooperation

Appendix A attached to this Service Guide describes a standard implementation timeframe for the Services, including Customer and Intrado responsibilities and key milestones (as herein attached, or as otherwise agreed by the parties, the "Implementation Schedule"). Each party will timely fulfill its obligations per the Implementation Schedule, and will make available all resources necessary to meet the Implementation Schedule, including, as applicable: personnel, facilities, circuits, APIs, network information, third party coordination, and timely approvals (each, an "Implementation Dependency"). Unless otherwise agreed, Implementation Dependencies will be completed within five business days after request.

Either party may notify the other if it has not timely completed an Implementation Dependency, and the party at fault will remedy the deficiency within ten business days. If Customer does not so remedy an outstanding Implementation Dependency following notice, then Intrado may commence charging for any minimum recurring fees due under the Order for the Services.

For third party dependencies outside of Customer's control, Customer will promptly communicate any expected delay, and any remedies stated above will not apply.

Any modified or expanded Implementation Schedule agreed on by the parties will replace the attached Appendix A, and the above terms will continue to apply.

4. Customer Obligations

4.1. Cooperation with Intrado and Intuitus

Customer will cooperate and assist Intrado and Intuitus as reasonably necessary regarding installation and maintenance of the Intuitus Services, including but not limited to (a) the review and acceptance of the Order and any schedules or other documentation applicable to the Order; (b) if Customer elects additional services, the review and acceptance of the Order and any other documentation applicable to the Order; (c) the prompt communication of any questions or issues potentially affecting or pertaining to performance of the Intuitus Services to Intrado; and (d) prompt response to Intrado queries and requests on issues and matters pertaining to the Intuitus Services and other matters arising under this Service Guide.

4.2. Data and Information

Customer will make available in a timely manner at no charge to Intrado and Intuitus all technical data, computer facilities, programs, files, documentation, test data, sample output, or other information and resources reasonably required by Intrado or Intuitus for the implementation and provisioning of the Intuitus Services. Customer will be responsible for ensuring the correctness, accuracy, and completeness of all data, materials, and information supplied by Customer.

4.3. Equipment

Customer will provide access to equipment, network connectivity, personnel and Customer expertise and institutional knowledge required by Intrado or Intuitus for the implementation and provisioning of the Intuitus Services.

4.4. Intuitus Appliance

Intuitus Appliances are the physical hardware that allows cyber threats to be detected. Intuitus Appliances include: Secure Utility Server (SUS), Forensic Data Collector (FDC), and OneBox. Customer acknowledges that any Intuitus Appliance located at Customer's facilities is the property of Intuitus. Customer will provide and maintain a secure environment at its facilities for the Intuitus Appliance(s), including safeguards to prevent unauthorized physical access and ensure protection against fire and other disasters. Customer will ensure that the Intuitus Appliance(s) have reliable power, reliable connectivity to the network(s) to be monitored, and reliable connectivity to the Internet, and will notify Intrado reasonably in advance of any planned outages affecting power or connectivity of the Intuitus Appliance(s). Customer will permit Intuitus as the delivery agent, to inspect the Intuitus Appliance(s) during ordinary business hours upon reasonable prior notice.

Appliance(s) must be returned to Intuitus within 14 days of the end of service term. End of service may be the end of the service term, end of a trial or pilot period, or other reason for termination. Appliance(s) can be mailed to Intuitus offices.

4.5. Customer Security Program

Customer acknowledges that it will provide the following controls, tools and processes to directly support the Intuitus Services, and that failure to do so may impact Intuitus's ability to perform the Services effectively:

- A written governance, risk and compliance (GRC) policy or policies, approved by a Senior Officer or equivalent, setting forth Customer's policies and procedures for the protection of its information systems and nonpublic information stored on those information systems (aka "Cybersecurity Policy");
- A written Incident Response Action Plan that is exercised and/or practiced with key scenario driven evaluations (i.e., tabletop exercises) on at least an annual basis;
- Designate two or more employees, executives, or agents who will respond to any security alerts and take recommended actions to mitigate harm to Customer's network; and,
- Although not required, it is recommended that each Customer conducts a periodic risk and vulnerability assessment to address changes to information systems, nonpublic information, and/or business operations. The risk and vulnerability assessment should allow for revision of controls to respond to technological developments and evolving threats.

4.6. Customer Incident Response and Remediation

Customer will be responsible for determining and undertaking or arranging for the undertaking of any action(s) in response to a security alert or report from Intrado, unless Intrado has expressly agreed to do so as an additional service under an Order.

4.7. Customer Contacts

Customer will appoint in writing a primary and alternate technical-level employee or agent to act as the primary contact person for all technical communication between the Customer and Intuitus related to the Services. Customer will also designate a managerial-level contact person. These contact persons will be responsible for monitoring the status of the Services, respond to any security alerts, take recommended actions to mitigate harm to Customer's network, receive cybersecurity reports, and will confer with Intuitus as needed.

4.8. Network Change Notification

Customer will immediately inform Intuitus and Intrado of any physical change to the Customer network.

4.9. Other Customer Obligations

Customer will be solely responsible for ensuring that it is not subject to contractual obligations materially affecting the implementation or use of the Intuitus Services.

5. Support

Customer may contact the Intuitus SOC at:

- Help Desk Number: (253) 343-0004
- Email Support: cybersupport@intuituscyber.com
- Hours: 24x7

6. Services Limitations

The following Services limitations and disclaimers apply:

- Services provide information to Customer to enable Customer to better assess security threats and take appropriate action. Services do not actively protect Customer's network or information from intrusion or cyberattack.
- Intuitus is the sole provider of Services; Intrado is acting as a reseller only.
- Customer may contact Intrado or Intuitus for support for any issues with Services.
- For Intuitus MDR, Customer must:
  - Maintain Internet connectivity to enable remote monitoring; and
  - Open ports and/or allow Intuitus to install necessary equipment that enables Intuitus MDR to inspect IP traffic passing through Customer's network.
- Customer agrees to review with Intuitus the Customer's architecture, including any and all changes to the architecture that may affect performance of the Services.
- A 6-week period is required to baseline network traffic, during which time the system is under full operational monitoring.

Appendix A

Implementation Schedule

Milestone	Duration	Deliverable	Owner
Initiation Phase	**34 days**		
Order placed & received.	10 days	Source security hardware.	Intrado
Site information provided. (Can be provided concurrently)	3 days	Gather site specific information about location and network addressing.	Customer, if it is Third Party CPE. Intrado, if it is Viper.
Pre-configure and test device.	10 days	Build and test security equipment.	Intrado
Hardware shipping/arrival.	10 days	Intrado ships the device; Customer provides contact information; Customer receives device.	Intrado/Customer
Rack equipment.	0.25 day	Connect power and network cabling.	Intrado/Customer
Network configuration.	0.25 day	Configure network switch for internet connectivity; Configure port mirroring on a separate switch.	Intrado/Customer
Production Phase	**32 days**		
Validation and Complete Installation.	2 days	Ensure data is being collected; Monitoring begins; Service Start Date. Network Connectivity confirmed. Service begins.	Intrado
Baseline Reporting Period	30 days	30-day Baseline reporting period begins. Limited reporting period. Only medium and critical alerts reported. Concurrent with Validation.	Intrado

- This schedule reflects a standard deployment of 36 days following Order Effective Date. Additional steps or requirements may be needed for non-standard deployments or unique circumstances.
- All references to “days” are to business days.