Managed Detection & Response (MDR)

Ingalls MDR is an industry leading network and endpoint security solution designed for advanced detection, threat hunting, and response guidance. We do this by utilizing very latest in cloud and data analytics technology to analyze, in real-time, all connections coming to and from your network. Ingalls MDR is designed to:

- Detect threats before they become breaches
- Monitor, identify, and notify any suspicious network behavior
- Perform threat detection and identify activity with known malicious hosts
- Establish a baseline of network traffic and investigate any deviations
- Monitor and discover all egress and ingress network flow data
- Leverage continuous up to date threat intelligence with event data
- Perform continuous notification and curation of alerts into reporting
- Provide actionable information through ticketing and monthly reporting

Ingalls' Managed Detection and Response (MDR) service combines the very latest in Cloud and Data Analytics technology with Cybersecurity's leading Incident Response team to Identify and Defend against potential incidents on your network.

Service Components

Client Portal

Ingalls Client Portal provides a comprehensive dashboard to provide at-a-glance summaries of security events over time, location, and severity. This allows our Clients to instantly gain a frame of reference for the security events that are being collected and analyzed.

Ingalls Client Portal also enables direct messaging between our Clients and their dedicated analysts.

INGALLS
INFORMATION SECURITY

Alert Monitoring and Analysis

Ingalls leverages a suite of detective tools, evaluates the output of these tools, and classifies security alerts based on a combination of custom, predefined alert rules, anomalous activity detection, machine learning, and curated threat intelligence to enhance security event detection, discover malicious automation, detect vulnerability exploits, and track attacker activity and/or data exfiltration.

Security Alert Response and Reporting

Ingalls will perform traffic/and or event correlation to determine which data and alerting constitutes an actionable security alert. Once such an alert has been identified, Ingalls will communicate this event alert to the Client via email, telephone, or SMS text messaging, depending on severity, time sensitivity, and other factors that may be present during the event timeframe.

Ingalls MDR Clients can expect to receive investigated and curated alert reports for the following:

- Malicious/Anomalous Network and Endpoint Activity
- Malicious/Anomalous Windows Domain Activity
- Policy Violations
- Network Reconnaissance and Vulnerability Probing

Ingalls analysts assigned to Clients will hold sync meetings with our Clients' IT Support Points of Contact on a weekly or less frequent basis (as determined by Client request). These meetings allow our analysts and our Clients to stay in touch and on track.

Vulnerability Assessments

Ingalls will perform vulnerability assessments from its network sensor device at regular intervals. Current vulnerability data will be pulled daily from national databases to evaluate the security of devices on the Client's network. Ingalls sensor devices contain over 50,000 individual tests to validate security controls and identify vulnerabilities.

Each month, a comprehensive vulnerability report will be generated. Vulnerabilities will be ranked according to their CVSS score and potential impact. These reports can be used as reference guides to install patches and configure computer hosts to resolve any discovered security vulnerabilities.

MDR Technology Components

The following technology components form the Ingalls MDR solution:

MDR	Description
Email Defense	Ingalls provides an advanced email spam and phishing filter for Clients as well as an Email Phishing Helpdesk, where our Clients' users can forward suspicious emails for review by Ingalls SOC analysts. Emails that are identified as phishing attacks are used a threat intelligence to search Client logs located in the Ingalls LCASS system, in order to identify the scope and severity of phishing attacks. Phishing emails that are determined to have led to account compromise are reported to our Clients and we offer the ability to purge email accounts of attacker access upon approval by our Clients.
Advanced Endpoint Security Technology	Ingalls uses Cylance PROTECT® as its preferred solution for endpoint prevention of malware, especially ransomware and other automated threats. Cylance PROTECT® is deployed and Client endpoint prevention alerting is integrated into the Ingalls' Analytics Platform. Cylance PROTECT® uses intuitive software that prevents, rather than reactively detects, viruses and malware. Cylance PROTECT® uses a host of advanced capabilities such as artificial intelligence, algorithmic science, predicative analysis and machine learning against known and unknown threats.
Active Directory Detection and Deception	Javelin is an advanced detection and deception tool for Microsoft Active Directory environments. Javelin provides the ability to deceive attackers who gain unauthorized access to Active Directory accounts and produces alerts and forensic packages designed to allow SOCs to identify unauthorized activity and respond, while presenting attackers with information about the Active Directory environment that delays their ability to create impact.
Network and Host-Based Intrusion Detection	Ingalls MDR includes an Intrusion Detection System module that evaluates ingress/egress (e.g. LAN to Internet and vice versa) network traffic for known threats and suspicious activity using signature-based and heuristic threat detection engines. Ingalls MDR also includes a Host-based Intrusion Detection System that operates as an agent on each workstation and server (Windows, Mac, Linux) in our Clients' environments. The HIDS solution allows for alerting based on third-party and internally-developed rulesets which are updated regularly. IDS signatures are constantly updated using the latest in threat intelligence derived from third parties as well as Ingalls own Incident Response investigations.

MDR	Description
Forensics	Ingalls combines Cylance OPTICS, forensic endpoint agents, and its host-based intrusion detection system to collect forensic data across the enterprise and maximize your organization's speed to resolution when handling a computer security incident, an insider threat investigation, or other digital forensic investigation issue. Our toolset offers unparalleled speed in identifying, isolating, remediating, and removing hostile threats in today's complex information technology environments.
Log Collection, Aggregation, Storage and Search	Ingalls Log Collection, Aggregation, Storage, and Search offers the ability to forward logs from Client systems (e.g. network firewalls, other devices, servers, and applications) as well as cloud-based services (e.g. Office365, Google Business) to a central repository where it is stored to maintain compliance with regulation, reviewed for anomalies that require SOC analyst attention, and searched during any investigation performed by the SOC.
Data Analytics Platform	Our Data Analytics Platform uses cloud technology to provide scalable data warehousing, indexing, and search capabilities. Each Client is provided with a self-contained environment that can be configured to support any data retention requirement. Advanced Machine Learning algorithms are harnessed to evaluate all collected data and present analysts with a structured view of outlier and anomalous data that allows for advanced security operations such as Entity and User Behavior Analytics and health and reporting checking for any data source.

Security Operations Center (SOC)

Ingalls monitors our Clients' environment from our Security Operations Center (SOC). Ingalls employees are qualified and experienced cyber security analysts with real-world data breach response experience. Ingalls' Security SOC analysts review all security events through a "single pane of glass." Events and alerts are flagged for priority review, and analysts process analysis using the Analyst workflow management system. Analysts process multiple alerts as a single event, and view information from multiple sources simultaneously. Any data source provided to the Data Analytics Platform can be leveraged to provide analysts with situational awareness that exceeds what is possible using traditional SEIMs.

Hardware and Software

Ingalls provides sensor(s) for monitoring network traffic. These may be either physical or virtual appliances depending upon our Client's environment and/or specific needs. The sensor is capable of receiving, parsing, and indexing logs, monitoring network traffic, performing DNS queries, etc. The sensor communicates with Ingalls' cloud-based, analysis environment via a secure, persistent virtual private network over UDP port 500 or other means as necessary.

Deliverables

The following MDR reports will be delivered to Ingalls' MDR Clients:

MDR	Description
Security Event Report	A ticket report will be emailed to the Client POC that contains information about any alert deemed a Security Event. The report will contain the date and time that the event occurred, the classification, system(s) involved, and specific recommendation and additional data related to the event.
Vulnerability Assessment Report	A periodic report detailing the results of vulnerability assessment scans performed by Ingalls using the security sensor host(s) installed in your environment. These reports can be used to identify necessary patching and configuration management activities to reduce your overall risk to compromise by malware or hackers.
Monthly Activity Report	A periodic report detailing monitoring activity, including number of events processed, Security Events reported, closed, and pending resolution.
System Outage Report	A report will be sent to the Client POC in the event of system outage and followed-up by a notice of restoration of service.

Incident Response and Breach Remediation

Even with the best controls in place, a security incident can still happen. Whether your incident is the result of a hacker, malware, or a negligent employee, Ingalls Information Security is prepared to respond quickly to security incidents. All Ingalls MDR Clients receive 4 hours of Incident Response support.

Our certified security and forensic experts can help you contain the situation and determine your next steps.

- Analyze security incidents, event correlation, and stop data exfiltration
- Provide complete visibility through forensic examination and analysis
- Begin remediation and speed up recovery time
- Integrity and preservation of forensic evidence and presentation of “a chain of custody”
- Provide executive reporting and expert court representation
- Resume business operations quickly
- Incident Response guidance and planning

Request a Demo

Ingalls Information Security is a specialized, cyber defense company with a mission to prevent and respond to data security breaches. Our consultants, analysts, and engineers are certified and experienced professionals with diverse backgrounds ranging from military and defense intelligence, network security, and information technology, giving us domain dominance and a leading edge in cyber defense.

Contact us at **contact@iinfosec.com** or call **888.860.0452.**

INGALLS
INFORMATION SECURITY

Cyber Innovation Center (CIC)
6300 Texas Street, Ste. 240, Bossier City, LA 71111

WWW.IINFOSEC.COM
(888) 860-0452 TOLL FREE