eSENTIRE

DATA SHEET:

Emergency Incident Response

Digital Forensics and Cyber Investigations

Rapid Deployment

Incident responders and supporting technologies are quickly deployed providing critical insight that accelerates investigation and completion of the incident response lifecycle.

Unmatched Expertise

Highly credentialed responders partner with our global 24/7 SOC Cyber Analysts extending your IR support and expertise across hundreds of individuals with decades of experience in stopping attackers.

Proven Tools And Processes

Industry-leading digital forensics, remote access, investigation and response tools and techniques battle-tested against real world threats ensuring attackers are quickly contained and incidents resolved.

Comprehensive Recovery

End-to-end incident lifecycle support not only stops attackers but supports remediation and recovery that ensures root causes are fixed and the chance for recurrence is eliminated.

When a security incident occurs, how fast your organization can contain and recover is critical to limiting business disruption, reducing cost, and salvaging reputational damage. While traditional managed service providers, consulting firms and forensic agencies have risen to answer the call, these organizations often lack critical experience in discovering how attackers break through and the tactics they use to achieve their objectives.

The **eSentire Artemis Incident Response team** is here to rapidly respond to and remediate cyber attacks. With Incident Commander level expertise and industry-leading technologies for remote access and recovery, we work with you to handle emergency security incidents and digital forensics investigations. eSentire supports the incident response lifecycle end-to-end, prioritizing rapid deployment to stop the attack, containment & analysis, and incident resolution including reporting to relevant parties, and security strategy support to stop recurrences.

The eSentire Artemis Team difference

Power of 24/7 SOC Team

- Access to hundreds of team members
- 24/7 SOC Cyber Analysts and Elite Threat Hunters
- Expertise detecting, disrupting and responding to threats

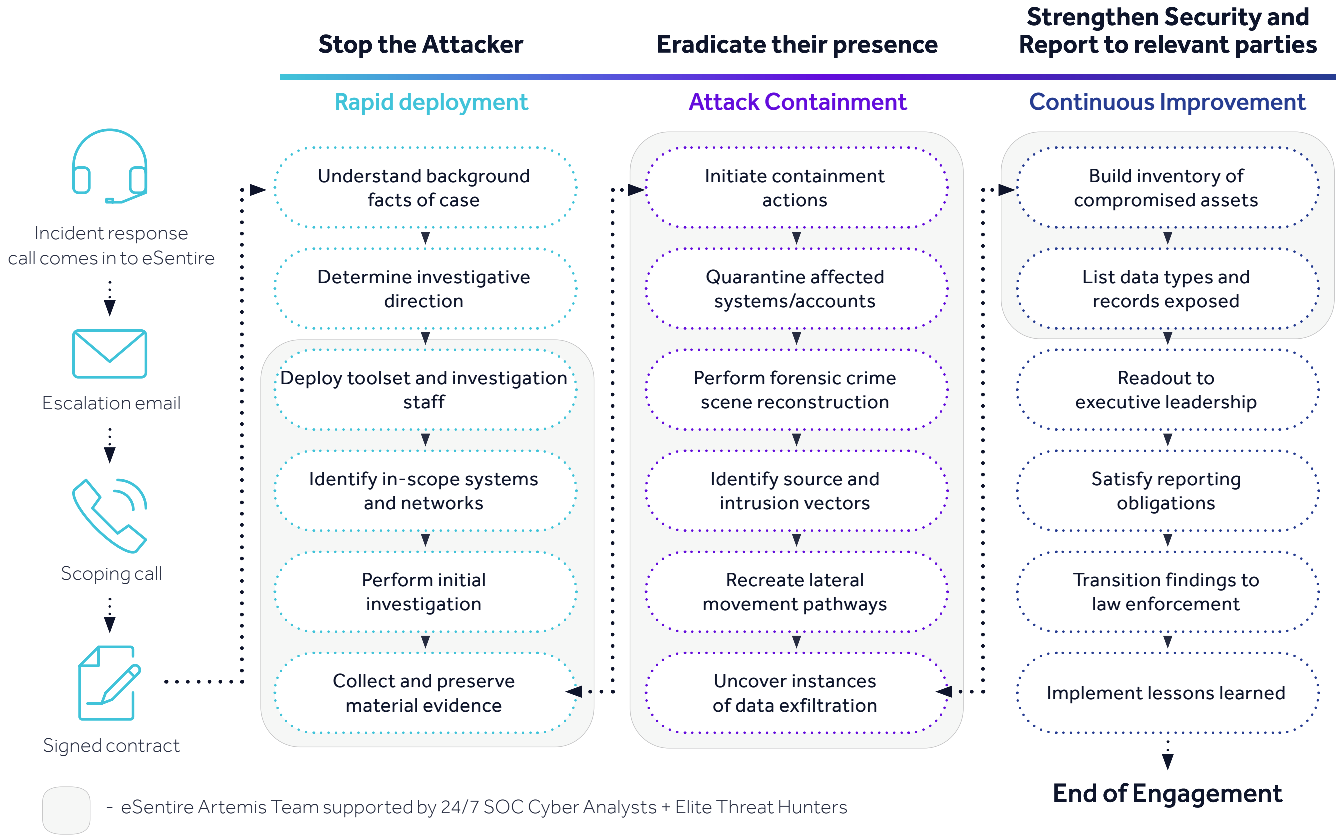
Delivers Results

- Attacks are quickly contained, incidents are resolved and recovery is supported eliminating the chance for recurrence
- Root cause analysis and threat eradication
- Systems clear for return to standard business operations

Flexible Delivery Model

- Available to address Emergency Incident Response
- Can be engaged on Retainer for Incident Response and Emergency Preparedness

How it works



Incident response call comes in to eSentire

Escalation email

Scoping call

Signed contract

Stop the Attacker — Rapid deployment

- Understand background facts of case
- Determine investigative direction
- Deploy toolset and investigation staff
- Identify in-scope systems and networks
- Perform initial investigation
- Collect and preserve material evidence

Eradicate their presence — Attack Containment

- Initiate containment actions
- Quarantine affected systems/accounts
- Perform forensic crime scene reconstruction
- Identify source and intrusion vectors
- Recreate lateral movement pathways
- Uncover instances of data exfiltration

Strengthen Security and Report to relevant parties — Continuous Improvement

- Build inventory of compromised assets
- List data types and records exposed
- Readout to executive leadership
- Satisfy reporting obligations
- Transition findings to law enforcement
- Implement lessons learned

End of Engagement

▢ - eSentire Artemis Team supported by 24/7 SOC Cyber Analysts + Elite Threat Hunters

Features

End-to-End Incident Management

Team of incident responsers and supporting technologies cover the full incident response lifecycle.

Rapid Deployment

Quickly mobilizes responders and investigative tool sets providing critical visibility across your affected networks and assets.

Elite Tool Sets

To illuminate where attackers are present. Supports root cause analysis.

Managed Containment

Locks down and isolates threat actors preventing further spread and business impact.

Digital Forensic Analysis

Reconstructs the incident determining root cause, affected systems and attacker pathways.

Asset Handling

Secure and robust processes for asset handling and chain of custody support.

Eradication

Identifies exploited vulnerabilities, remediates affected assets and deletes presence of all malware.

Confirmation

Gathers and stores incident details that meet legal and regulatory requirements.

Robust Reporting

Detailed findings and impacts of the cyber investigation chronicle all actions taken with lessons learned at the Executive and technical level.

Compliance Satisfaction

Meets regulatory requirements with centralized collection, retention and reporting.

Litigation Support

Expert and fact witness testimony, if needed, is available.

Crisis Communication

Assist with internal and external communications, including media releases, FAQs, and executive communications.

Make the case for eSentire Emergency Incident Response

- Account for risk across your network assets
- Expedites response for quicker return to normal
- Alleviates burden on limited personnel and skillsets
- Contains and eradicates attackers from environment
- Supports crisis management, escalation and notification
- Determines extent of compromised data and handling of evidence
- Ensures the threat is completely discovered and eradicated
- Delivers a complete understanding of the full scope of a compromise
- Determines root cause and closes gaps ensuring no recurrence
- Minimizes potential business impact
- Supports third party and regulatory requirements

> “There are times where any security leader, where any enterprise, needs to have an added layer of support…That’s the exclusive domain of the kind of approaches and toolsets that are used in Incident Response.”
>
> *-- Bryan Sartin, Chief Services Officer, eSentire*

> “With eSentire you're getting the visibility, you’re getting the detection and identification of potentially bad traffic and you’re getting response if anything is detected as malicious.”
>
> *-- Alex Bazay, CISO, Align Communications*

54% of attackers can complete an attack in under 15 hours[1]

$15K+ the cost incurred every day a breach goes uncontained[2]

87% of organizations report a shortage of skilled personnel in 2021[3]

60% of organizations lack a cybersecurity incident response plan[4]

[1,2] Ponemon 2019 Cost of a Breach Report, Verizon, [3] 2021 CyberEdge Group 2021 Cyberthreat Defense Report, [4] Ponemon: Cyber resilient organization report, 2020

Experiencing an incident? We're here to help.

Contact us at 1-866-579-2200

If you’re experiencing a security incident or breach contact us ☎ 1-866-579-2200

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1000+ organizations in 70+ countries from known and unknown cyber threats. Founded in 2001, the company’s mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts & Elite Threat Hunters, and industry-leading threat intelligence research from eSentire’s Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit **www.esentire.com** and follow **@eSentire**.