




eSentire Response and Remediation

The World’s Most Complete Response Capability























eSentire’s Multi-Signal Managed Detection and Response (MDR) services balance high fidelity automated blocks with rapid human-led threat investigations to disrupt, isolate, and stop threats on your behalf across your full attack surface with a Mean Time to Contain of less than 15 minutes. We detect in seconds and contain in minutes, so your business is never disrupted.

When it comes to response, it’s how we do it that makes all the difference.

 <p>RESPONSE SPEED</p>	 <p>RESPONSE EXPERTISE</p>	 <p>RESPONSE COVERAGE</p>
<p>When your business operations and reputation are under attack, every minute matters. We hunt and stop cyber threats faster than anyone else.</p>	<p>Your MDR provider should take real ownership of protecting your business, not just drown your team in alerts.</p>	<p>Get continuous protection across your entire attack surface so you can sleep easy knowing that whenever and wherever a new cyber threat is detected, we’ll always respond to protect you.</p>

Multi-Signal Complete Response

As part of our All-in-One MDR service we ingest signal sources that drive data correlation, cyber threat analysis and kill switch response capabilities. When combined we deliver full attack surface visibility, deep investigation, threat detection, and complete response.

		TECHNOLOGY PARTNERS	DETECTION	INVESTIGATION	RESPONSE
 ENDPOINT	Guard endpoints by isolating and remediating threats to prevent lateral spread.	eSENTIRE    	✓	✓	✓
 NETWORK	Defend brute force attacks, active intrusions, and unauthorized scans.	eSENTIRE	✓	✓	✓
 LOG	Investigation and threat detection across multi-cloud or hybrid environments.	sumo logic 	✓	✓	✓
 EMAIL	Remediate phishing attempts including retroactive purges of malicious emails and files.		✓	✓	✓
 CLOUD	Remediate cloud misconfigurations, vulnerabilities, and policy violations.	  sumo logic   	✓	✓	✓
 IDENTITY	Investigate and respond to compromised identities and insider threats.	  	✓	✓	✓
 VULNERABILITY	Routine scanning of all internal and external assets plus expert advice.		✓	✓	

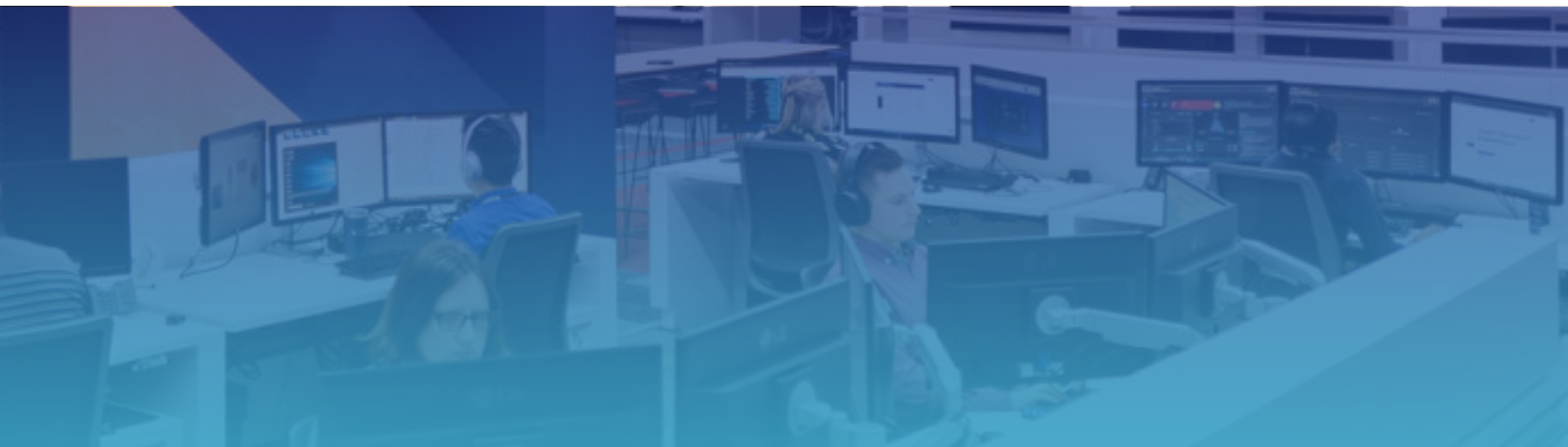


Our XDR Platform and Human Threat Hunters Provide Response + Remediation You Can Trust

The eSentire XDR Platform makes the outcomes driven by eSentire MDR possible. Patented machine learning and proprietary threat content from our Threat Response Unit (TRU) eliminate noise, enabling real-time detection & response, and automatically blocking millions of threats per day. The Atlas XDR Platform also makes our Predictive Threat Defense Network possible by pushing new threat detection and containment content to every eSentire customer.

Our XDR platform can answer questions like:

- Which of these pieces of information are relevant?
- Which of these events are related?
- Which activities are obviously, clearly and demonstrably malicious?
- When is it appropriate to initiate an automated response workflow?
- What requires further analysis and human attention?
- How many IT assets do I have, where are they, and how has that number changed over time?
- How does my external risk compare to my industry peers?



When there are very high-confidence answers to all of these questions, eSentire threat response can be fully automated. This entirely removes human effort from the process.

In cases where there is ambiguity and requires human intuition, the Atlas Security Operations Platform gives our 24/7 SOC Cyber Analysts and Elite Threat Hunters in-depth information that makes their jobs easier. It also allows them to be more creative, have more confidence in their effectiveness, and stop more threats.

Our standard response procedures include:

- Preventing infected endpoints from spreading to other machines
- Isolating ransomware, data exfiltration and hands-on keyboard attackers
- Quarantining malicious files and terminating processes
- Stopping/removing service and registry keys
- Preventing compromised email accounts from forwarding compromised communications
- Reporting, investigating, and remediating phishing attempts
- Purging emails retroactively organization-wide
- Suspending accounts and user access to stop compromised users from corrupting data or applications
- Correcting critical misconfigurations across your multi-cloud environments
- Preventing any devices on the network from communicating with known bad actors
- Tactically disrupting network connections involved in investigations or incidents

What you can expect with eSentire Response

Standard Investigation Notifications Highlighting:

- 1 What we found
- 2 Where we found it
- 3 The response actions we've taken to isolate host on your behalf
- 4 Confirmation that IOCs from the malware download have been added to our XDR platform to prevent this occurring to another customer
- 5 Recommendations to support your cyber resilience

1 **What Happened**

The eSentire SOC has detected that INITECH.W10.03 (10[.1199][16][103] has been compromised.

Timestamp	2024-07-22T 13:14:16 UTC
Threat Type	Intrusion
Severity	Critical
Intrusion Vector	Phishing

Description of Activity

A security incident has been detected, involving a compromised host, specifically the Initech-w10.03 host. The user "ssmith", opened a file named "Invoices Outstanding (005).one" from OneNote which contained a malicious embedded macro.

Upon execution, the macro downloaded a malicious payload and executed various PowerShell commands, which are suspected to be related to Oakboat ransomware. The adversary employed evasive tactics to evade detection, including manipulating file attributes, names, and locations.

These tactics aim to deceive security tools and users, allowing the adversary to perform malicious activities without being detected and providing defense evasion capabilities. It is essential to take immediate action to limit the exposure of the ransomware and prevent it from moving laterally and causing further damage.

2 **Where Did it Happen**

INITECH.W10.03 (10[.1199][16][103]		CUSTOMER ASSET	TARGET
IP Address	10[.1199][16][103]		
Hostname	INITECH.W10.03		
Domain	INITEC		
OS Name	Windows		

ssmith [initech_suesmith@esentire].com		CUSTOMER ASSET
Username	ssmith	
Email	initech_suesmith@esentire[.]com	
Full Name	Sue Smith	
Domain	INITEC	

3 **Actions Taken**

We have placed a host isolation against **INITECH.W10.03**

We have submitted an AMP nomination for 34[.237][1129][186].

4 **Recommendations**

- If a forensic investigation is required physically isolate the following systems from the network and do not power them off to preserve volatile forensic data:
 - **INITECH.W10.03 (10[.1199][16][103]**
- If a forensic investigation is not required re-image the following systems:
 - **INITECH.W10.03 (10[.1199][16][103]**

Full details of this threat case can be found in the eSentire Insight Portal

5 Please acknowledge receipt of this alert. The eSentire SOC will be reaching out as per your escalation policy, if acknowledgement is not resolved.

The Response Spectrum

So how far does your MDR service provider go in terms of threat response and remediation?



Included Response and Remediation Actions:

eSentire vs. The Other Guys	Service	Support	eSentire	Other MDR and MSSPs
Multi-Signal Visibility (Network, Endpoint, Log, Cloud, Identity and Vulnerability)	MDR	Detection	✓	Limited
Best-of-Bread Integration Partners	MDR	Detection	✓	Varies
Rapid Human-Led Investigations	MDR	Detection	✓	✓
Containment in 15 Minutes	MDR	Response	✓	✗
Automated Response Driven by XDR Platform	MDR	Response	✓	✓
Endpoint Threat Containment	MDR	Response	✓	✓
Quarantine Files	MDR	Response	✓	✗
Hash Blocking	MDR	Response	✓	✗
Account and Access Suspension	MDR	Response	✓	✗
Network Isolation	MDR	Response	✓	✗
Blocking Compromised Email Accounts	MDR	Response	✓	✗
Unlimited Threat Hunting and Incident Handling	MDR	Response	✓	Limited
Terminate Malicious Processes	MDR	Remediation	✓	✗
Facilitated Retroactive Email Purges	MDR	Remediation	✓	✗
System Reboot	MDR	Remediation	✓	✗
Removal of Registry Keys/Values	MDR	Remediation	✓	✗
Threat Eradication	MDR	Remediation	✓	✗
Root Cause Analysis	MDR + DFIR		✓	Limited
Digital Forensics Analysis	DFIR		✓	Limited
Crime Scene Reconstruction	DFIR		✓	Limited
E-Discovery	DFIR		✓	Limited



eSENTIRE

Ready to get started?

Submit your information and an eSentire representative will be in touch to help you build a more resilient security operation today.

[CONTACT US](#)

IF YOU'RE EXPERIENCING A SECURITY INCIDENT OR BREACH CONTACT US  1-866-579-2200

eSENTIRE

eSentire, Inc., the Authority in Managed Detection and Response (MDR), protects the critical data and applications of 2000+ organizations in 80+ countries, across 35 industries from known and unknown cyber threats by providing Exposure Management, Managed Detection and Response and Incident Response services designed to build an organization's cyber resilience & prevent business disruption. Founded in 2001, eSentire protects the world's most targeted organizations with 65% of its global base recognized as critical infrastructure, vital to economic health and stability. By combining open XDR platform technology, 24/7 threat hunting, and proven security operations leadership, eSentire's award-winning MDR services and team of experts help organizations anticipate, withstand and recover from cyberattacks. For more information, visit www.esentire.com and follow [@eSentire](https://twitter.com/eSentire).