eSENTIRE

eSENTIRE THREAT RESPONSE UNIT

Advanced Threat Analytics

Threat Response Unit

Real-Time Threat Intelligence | Elite Security Researchers | Sophisticated Threat Hunting Tools | Rapid Threat Detection | Machine Learning Applications

Threat Intelligence | Tactical Threat Response | **Advanced Threat Analytics**

Research That Informs Machine Learning

Our research informs development efforts and identifies potential counter-threat use cases that could be accelerated by machine learning and data science.

5 Machine Learning Patents for Threat Detection and Data Transfer

We develop security force multipliers and proprietary machine learning applications that hunt and respond to elusive threats.

Threat Hunting is at The Core of Our Service

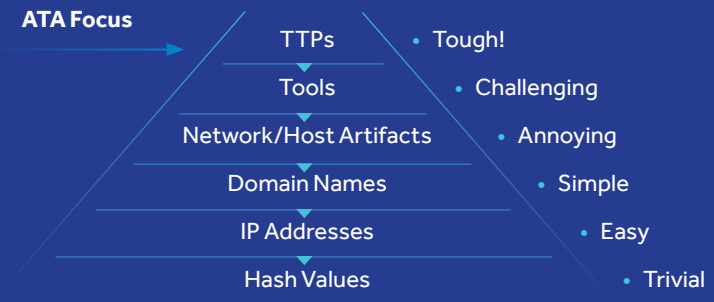
We are the Authority in Managed Detection and Response – we deliver Response, Remediation, and Results through proactive, hypothesis-driven threat hunting.

The Advanced Threat Analytics practice is our innovative threat research and development group. Our expert threat researchers concentrate on solving challenges posed by disparate data sets and expanding attack surfaces. Leveraging data science and machine learning expertise, the Advanced Threat Analytics team creates proprietary and proven models designed to identify threat actor tactics, techniques and procedures that traditional security tools miss. Our innovations, in combination with unique human expertise, accelerate investigations and threat hunts in our Security Operations Center (SOC). As is the case with all modern Threat Response Unit services, eSentire customers benefit from Advanced Threat Analytics expertise and outputs included in our core Managed Detection and Response (MDR) service.

Taking on the cybersecurity "Pyramid of Pain"

Traditional security technologies such as antivirus and firewalls deliver protection through basic security signals like hashes and IP addresses.

The true challenge of security today is identifying ever-changing adversary tactics, techniques and procedures (TTPs), which requires the combination of human expertise and advanced tools.



Notable ATA Innovations

BLUESTEEL
Machine learning-based detection of malicious Powershell activity at scale

MALKARA
Machine learning-based detection of unusual VPN connections at scale

READ ABOUT ATA INNOVATIONS IN ACTION:

→ Threat Dissection: Anatomy of a Powershell Attack

Our Difference	Innovative and high-impact threat hunting tools	Proven AI/ML expertise	Long-horizon counter threat research	Dedicated and focused team
Your Outcome	Detect threats that legacy technologies miss	Accelerate efficiencies and automation in your security posture	Prepare for emerging threats of tomorrow	Alleviate resource and staffing constraints

"I can say with a high degree of confidence that my team and the firm can sleep at night knowing that the eSentire team of security experts are working diligently to protect our environment and the firm's assets!"

– CTO, mid-sized law firm

We're here to help!

Get Started

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

eSENTIRE

eSentire, Inc. is the Authority in Managed Detection and Response, protecting the critical data and applications of 1500+ organizations in 80+ countries, representing 35 industries 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**.