Executive Overview

•Headquarters: Waterloo, Ontario -Canada
•Founded in 2001
•600+ Employees
•2 Security Operations Centers (Cork, Ireland and Waterloo, Ontario -Canada)
•Over 1,600 customers

Product & Service Offerings

BREACH PREVENTION
Managed Detection & Response
•Network
•Endpoint
•Cloud
•Log

BREACH SERVICES
Digital Forensics & Incident Response
•On-Demand 24/7 Incident Response
•Emergency Incident Response

PRE-BREACH SERVICES
Managed Risk Programs
•Managed Vulnerability Service
•Managed Phishing and Security Awareness Training
•Penetration Testing
•Virtual CISO Services

Sales Engineer Take On Best Fit

One of the largest 'pure play' security providers in the market focused on breach prevention, detection & remediation. Full DFIR services can be purchased standalone/after a breach. Offer MDR services. Offerings around Crowdstrike & Microsoft Security and can bring SumoLogic as a SIEM service. Best consulting vCISO practices in the portfolio with some size and length of service minimums. Offer 24/7 SOC services include proactive Threat Hunters and their patented Atlas XDR platform which has a 15-minute mean time to contain (an incident). Finally they offer an agent called CYFIR that allows for some of the fastest investigation and response services on the market. They will work with smaller customers, but their ideal cusstomer is 100-500 with no IT team or 500-2,500 as an extension of their cyber team. They have identified niche opportunities with customers over 2,500 employees usually around their IR services.

-Rick Mischka, Cybersecurity FSE

Key Features & Differentiators

•Full Threat Visibility & Investigation eSentire's multi-signal approach ingests high-fidelity data sources from the endpoint, network, log, cloud, insider threat, assets, and vulnerability data, enabling complete attack surface visibility.
•24/7 Threat Hunting & Disruption eSentire's SOC analysts and elite threat hunters rapidly investigate, contain, and close down threats when an automated response isn't possible.
•Atlas XDR Platform Patented AI and Machine Learningusinghigh fidelity detection and automated real-time threat disruption powered by unique intelligence from across our global customer community identifies and disrupts new and emerging threats.
•Rapid, Robust Response SOCanalysts and threat hunters disrupt, isolate, and stop advanced threats with a 15-minute mean time to contain.
•Original Threat Intelligence eSentire's Threat Response Unit (TRU) delivers original research, curates threat intelligence, and builds new detection models to stay ahead of attackers.

Top Industries Served

- Manufacturing
- Financial Services
- Information Technology
- Law

Ideal Customer Profile

- Has no team & needs one: Needs an extension of the team
    - Looking for a complete cyber solution, looking to hire "the team" as a Service
    - Manager or Director of IT
    - Influencers: Manager, Engineer, Architect
    - Less than 500 employees
    - •1-2 people in security
    - •"One man show"
- Needs an extension of the team: Hiring threat hunting and response expertise to expand capabilities, augment 24/7 SOC as a Service
    - VP or CISO, IT, Cyber
    - Influencers: Manager, Engineer, Architect
    - 500 -2,500 employees
    - •Understaffed
    - •Requires off-hours support
    - •Lacks threat hunting/response
- Has a team needs –Niche Expertise: Outsource capabilities to focus their team on higher priority initiatives, may be secondary SOC, driven by compliance requirements
    - CISO, CIO, CRO, CEO
    - Influencers: Manager, Engineer, Architect, Director, CFO
    - 2,500-10,000+ employees
    - •Right-Sized
    - •Looking for compliment or back up to support technical expertise

Qualifying & Technical Questions

Qualifying Questions

1. Do you have a dedicated security team?
2. Do you have a team and a security policy and incident response plan in place?
3. How does your security process scale for larger, heavily regulated clients?
4. Where do you feel the existing program is falling short?
5. What have you done to ensure you are meeting industry regulations?
6. How do you think a breach can impact your organization?
7. If you were breached, how would this impact your brand reputation?
8. How long would it take you to diagnose a breach?
9. How are you currently monitoring your network?
10. Are you sure threats are not bypassing your controls?
11. How do you assess the security risks of partners, supply chain, and prospective acquisitions?
12. How do you address security due diligence questionnaires from potential clients?

Technical Questions

NETWORK

1. Total number of locations?
2. Total number of Knowledge Users?
3. What is the make/model of core switches?
4. Is the internet direct or backhauled? Speed?

ENDPOINT

1. Total Number of Workstations, Laptops, Servers?
2. Are you running Windows OS, Mac OS, Linux (RHEL / CentOS) specific versions?

LOG

1. Currently do you have a SEIM?
2. Do you have compliance requirements? If so, which ones?
3. Are compliance requirements driving your decision to have a SEIM?
4. For audit purposes do you have a data retention timeframe? If so, how long?

CLOUD

1. Are you using IaaS or SaaS?
2. What cloud service provider are you using? IE. AWS, Azure, Google, private
3. If known, how many total workloads do you have?