The fourth industrial revolution (IR 4.0) connects factory floors and supply chain elements through industrial IoT (IIoT) and execution systems tied to enterprise resource management and critical business intelligence services. Manufacturing sees IR 4.0 as the future, while sophisticated threat actors view it as an expanded attack surface littered with vulnerable systems and valuable data—all belonging to companies with much to lose.

Business and IT leaders alike are responsible for developing security programs that can detect and contain threats, in a new landscape where ransomware gangs and state-sponsored actors have identified supply chains and manufacturing business processes as preferred targets. Managing cyber risk is a business imperative for manufacturing organizations to enjoy the benefits of Industry 4.0 without falling victim to debilitating, expensive and public cyberattacks.

Manufacturing organizations need cybersecurity expertise to proactively detect, disrupt and remediate cyber threats before they become business impacting events, or trigger procurement penalties. We have demonstrated success working with manufacturing firms and their supply chain partners. Through our experience, we’ve developed a leading framework for firms to address the most common concerns and risks security leaders face:

- The risk of ransomware-based attacks designed to create massive operational disruption, disable manufacturing automation systems, and impact assembly line management applications leading to financial losses
- Avoiding supply chain or procurement penalties, or client loss as the results of a massive cyberattack
- Lack of confidence in the security acumen of smaller supply chain partners
- Security coverage during acquisitions of small manufacturing operations
- The risk of stolen intellectual property, patent information, manufacturing process information or other critical IP that profits counterfeit producers, and erodes your enterprise value and market share.

We help manufacturing organizations:

1. Monitor their environments 24/7
2. Disrupt known and unknown threats
3. Stop breaches before they impact business operations
4. Protect Proprietary and supply-chain information
5. Avoid supply chain penalties
6. Mitigate Supply Chain Risk
Preventing Operational Disruption

Managing cyber risk requires cooperation between the Operational Technology and Information Technology groups that have traditionally functioned as separate entities. It requires the ability to monitor both the shop floor and front office to rapidly detect suspicious activity, investigate in minutes and take measures to contain threats before they become business disrupting.

eSentire Managed Detection and Response (MDR) services balance cutting-edge machine learning XDR technology, human security expertise and security operations leadership to mitigate your business risk, enable security at scale and drive your cyber program forward. Our 24/7 Security Operations Center Cyber Analysts and Elite Threat Hunters have discovered and defended numerous instances of ransomware gangs attempting to establish a foothold in one of our protected manufacturing environments. Sample support included:

- Detecting malicious administrative activity early in the attack cycle to disrupt threats before they can land and island hop from IT systems to OT controllers and management services
- Identifying and disrupting malware active on mobile devices before threats can move to core network operations
- Blocking active attempts to deploy credential collection tools, malware payloaders and even multiple ransomware attacks

Protecting Proprietary and Supply Chain Information

Manufacturers work in partnership with upstream vendors and downstream clients. Coordinated production requires the sharing of proprietary knowledge including intellectual property, manufacturing processes, tolerance and standards, and other business intelligence. Stolen information can cripple production, reduce enterprise value or even break relationships.

Our 24/7 MDR services detect intrusions and stop attacks before data is exfiltrated. Our Threat Response Unit (TRU) actively scours the dark web looking for stolen client data. Our services are designed to catch intrusions in the early stage before they can establish a foothold and steal valuable manufacturing data, providing trust and confidentiality that is so imperative in this line of business.

Avoiding Supply Chain Penalties

Operational disruptions can have a massive effect on downstream suppliers and trigger contractual procurement penalties could result in significant financial losses for manufacturers participating in complex supply chains. eSentire Managed Detection and Response (MDR) services hunt threats and suspicious activity to investigate in minutes and contain these attacks before they become business disrupting. Our security experts have protected firms from sophisticated criminal campaigns and target state-sponsored espionage attacks.

Mitigating Supply Chain Risk

We identify core services, such as manufacturing execution systems (MES), ICS/SCADA controllers, and other OT systems, and prioritize these services for monitoring.

Our services detected and blocked the malicious web shell scripts associated with the 2021 Microsoft Exchange vulnerabilities, worked with clients to secure their SolarWinds Orion issues, and discovered multiple remote administrator tool vulnerabilities. Our Risk Management services provide assessments of risk, recommend minimum security measures, and ways to offset risk.
About Managed Detection and Response (MDR)

At eSentire, our comprehensive approach to MDR helps organizations test, mature, measure, and protect their environments from a multitude of risk factors. Our MDR services rapidly identify and contain threats that bypass traditional security controls. Ingesting signals from your on-premises, cloud and hybrid environments, we combine endpoint, network, log, vulnerability, and cloud data to identify known and elusive threats. Averaging 15 minutes from identification to containment, we ensure attackers don’t have the time to achieve their objectives.

<table>
<thead>
<tr>
<th>Key Industry Challenges</th>
<th>How eSentire MDR Services Help</th>
</tr>
</thead>
</table>
| Protecting Proprietary Information | • Our 24/7 Security Operations teams actively hunt for threats across your environment. We detect intrusions and contain attacks before they can exfiltrate data  
• eSentire Threat Response Unit (TRU) actively searches the dark web looking for stolen data  
• Active threat hunting catches intrusions before valuable manufacturing data is stolen |
| Victim to Ransomware             | • 24/7 eSentire Security Operations team discovers intrusion, preventing pervasive deployment of malware and ransomware  
  • We support multi-signal coverage ensuring visibility across endpoint, network, log, cloud, and other data sources for deep investigation and response capabilities  
  • We offer endpoint protection to prevent your defenses from being disabled |
| Operational Disruption           | • Threat hunting and investigation of suspicious activity  
  • Contains threats before they deploy malware in critical systems that lead to massive outages |
| Supply Chain Penalties and Risk  | • eSentire Managed Risk Service experts support in security assessments, testing and make strategic recommendations to offset risk |
| Compliance                       | • Our SOC leverages hardened run books which include plays to manage issues and reporting for PII, PCI, HIPAA, GDPR, CCPA and state level regulations |

eSentire is capable of supporting your firm with end-to-end comprehensive cybersecurity services. Our expertise includes:

Managed Risk Services
Strategic services including Vulnerability Management, Managed Phishing and Security Awareness Training to identify gaps, build defensive strategies, operationalize risk mitigation and continuously advance your security program.

Managed Detection and Response Services
We deliver complete and robust Response. By combining cutting-edge machine learning XDR, human security expertise and security operations leadership, we hunt and disrupt known & unknown threats before they impact your business.

Digital Forensics and Incident Response Services
Battle-tested Incident Commander level expertise driving incident response, remediation, recovery, and root cause analysis. Emergency Preparedness and Emergency Response services as well as industry-leading 4-hour Threat Suppression SLA with eSentire IR Retainer available.
The service and deployment that eSentire offers is second to none. I sleep better at night knowing our business is protected with eSentire services.

- Jason Ruoff
  IT Architect, Lam Technology

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

1 https://www.industryweek.com/technology/cybersecurity-factory-floor