eSENTIRE

MANUFACTURING SEGMENT

Manufacturing Cybersecurity Checklist

While manufacturers look at facilities and see the manifestation of industry 4.0, private and nation state threat actors see a vast attack surface littered with vulnerable systems and valuable data. Manufacturing organizations need cybersecurity expertise to proactively detect, disrupt and remediate cyber threats before they become business impacting events, or trigger procurement penalties.

Top Manufacturing Security Challenges

- A clear understanding of risk-based best practices
- Lack of visibility into IT and OT assets
- Technical capabilities to identify and contain threats that cross from IT into OT resources
- Zero-day threats, often associated with geo-political decisions, global wars or industrial disruptions
- Lack of internal resources and expertise
- Lack of alignment between IT and OT operations
- Failure to plan for cyber incidents
- Compliance to regulatory requirements and supply chain SLAs

A Comprehensive Approach to Manufacturing Protection

Whether your organization is a national or regional entity, threat actors are going to capitalize on vulnerable systems and human nature. Ultimately, the difference between organizational protection and potential disruption will come down to the speed at which you can identify and contain an attack.

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

eSentire offers a comprehensive suite of cybersecurity services to ensure your cyber resiliency aligns with the CMMC requirements and the NAM Cybersecurity Framework.

Our services include:

Managed Risk Services

Strategic services including Security Assessments, Managed Phishing and Security Awareness Training to identify gaps, build defensive strategies, operationalize risk mitigation and continuously advance your security program. Our Managed Vulnerability Service continuously assesses and accurately identifies vulnerabilities across your organization's traditional and dynamic IT assets including mobile devices, IoT and virtual machines with a cloud-based scanning cadence. We prioritize and remediate the vulnerabilities in your business-critical assets, whether on-premises or in the cloud.

Managed Detection and Response Services

Our team doesn't drown you in alerts, we go beyond other MDR providers to drive results. We support your cyber program with a combination of cutting-edge machine learning XDR technology, human expertise and security operations leadership to mitigate your business risk, enable security at scale and drive your cyber program forward. eSentire MDR provides improved detection, 24/7 Threat Hunting, deep investigation, end-to-end coverage and complete response. We stop threats before they disrupt your business.

Digital Forensics and Incident Response Services

Battle-tested Incident Commander level expertise driving incident response, remediation, recovery, and root cause analysis to determine the extent of impact and produce evidence that could bear scrutiny in a court of law. Emergency IR services and Incident Response retainer offering available.

How our services map to the NAM Cybersecurity Framework

		eSentire MDR	eSentire Managed Risk Services	eSentire Incident Response
Part 1: Governance				
1.0	**Cybersecurity Leadership**			
A	Chief information security officer (CISO/CSO)		• Virtual CISO • Threat Advisories • Executive Briefing	
B	Cybersecurity governance committee (CSG)		• Virtual CISO • Threat Advisories • Executive Briefing • Security Policy Guidance • Security Program Maturity Assessment	

		eSentire MDR	eSentire Managed Risk Services	eSentire Incident Response
Part 1: Governance cont...				
C	Documented cybersecurity roles and responsibilities		• Security Program Maturity Assessment • Security Architecture Review	
D	Documented cybersecurity risk profile and registry		• Security Program Maturity Assessment • Security Policy Guidance • Threat Advisories	
E	Documented cybersecurity program		• Virtual CISO • Security Policy Guidance • Security Program Maturity Assessment	
F	Documented business continuity plan (BCP)		• Virtual CISO • Security Policy Guidance • Security Program Maturity Assessment	
G	Documented incident response (IR) plan			• Security Incident Response Planning
2.0	**Classifcation and Inventory of Assets**			
A	Personal data/identifiable info (PD/PII)		• Managed Vulnerability Service	
B	Financial data, accounts and transaction information		• Managed Vulnerability Service	
C	Client account and transaction records		• Managed Vulnerability Service	
D	Confidential health or employee records		• Managed Vulnerability Service	
E	Identify sensitive intellectual property		• Managed Vulnerability Service	
3.0	**Map Regulatory Requirements**			
A	Federal regulations (HIPAA, GLBA)		• Security Policy Guidance • Security Program • Security Architecture Review • Maturity Assessment • Managed Vulnerability Service	

		eSentire MDR	eSentire Managed Risk Services	eSentire Incident Response
Part 1: Governance cont...				
B	Privacy regulations (GDPR, CCPA)		• Security Policy Guidance • Security Program • Security Architecture Review • Maturity Assessment • Managed Vulnerability Service	
C	Map of jurisdictions in which firms/ clients operate		• Security Policy Guidance • Security Program • Security Architecture Review • Maturity Assessment • Managed Vulnerability Service	
D	Map of federal statutes		• Security Policy Guidance • Security Program • Security Architecture Review • Maturity Assessment • Managed Vulnerability Service	
E	Map of state statutes		• Security Policy Guidance • Security Program • Security Architecture Review • Maturity Assessment • Managed Vulnerability Service	
4.0	**Cyber Insurance**			
A	Documented policy and carrier		• Security Policy Guidance • Security Program Maturity Assessment	
B	Documented minimum security standards		• Security Policy Guidance • Security Program Maturity Assessment	
C	Documented notification of claim procedures		• Security Policy Guidance • Security Program Maturity Assessment	

		eSentire MDR	eSentire Managed Risk Services	eSentire Incident Response
Part 2: Risk Assessment				
5.0	**Risk Profile**			
A	Document industry associated risks		• Managed Vulnerability Service • Security Program Maturity Assessment	
B	Evaluate likelihood and consequences		• Managed Vulnerability Service • Security Program Maturity Assessment	
C	Create a risk registry		• Managed Vulnerability Service • Security Program Maturity Assessment	
D	Monitor risk mitigation activities and performance		• Managed Vulnerability Service • Security Program Maturity Assessment	
6.0	**Annual Risk Assessment**			
A	Document known threat actors and persistent threats		• Managed Vulnerability Service • Security Program Maturity Assessment	
B	Document technology base vulnerabilities		• Managed Vulnerability Service • Security Program Maturity Assessment	
C	Document business model vulnerabilities		• Managed Vulnerability Service • Security Program Maturity Assessment	
D	Document regulatory obligations and penalties		• Managed Vulnerability Service • Security Program Maturity Assessment	
E	Document client obligations and penalties		• Managed Vulnerability Service • Security Program Maturity Assessment	
F	Document supply chain obligations and penalties		• Vendor Risk Management Program • Managed Vulnerability Service	

		eSentire MDR	eSentire Managed Risk Services	eSentire Incident Response
Part 2: Risk Assessment cont...				
7.0	**Annual Penetration Test**			
A	Conduct annual penetration test		• External/Internal Penetration Testing	
B	Document identified vulnerabilities and recommendations		• External/Internal Penetration Testing	
C	Document identified compliance violations		• Managed Vulnerability Service • Security Program Maturity Assessment	
8.0	**Periodic Ad Hoc Assessment**			
A	Review security controls given material change		• Managed Vulnerability Service • Security Program Maturity Assessment	
B	Document risks associated with material change		• Managed Vulnerability Service • Security Program Maturity Assessment	
C	Document required changes to policies and insurance		• Managed Vulnerability Service • Security Program Maturity Assessment • Security Policy Guidance	
Part 3: Security Program				
9.0	**Asset Inventory and Device Management**			
A	Documented operating systems, versions and mapping		• Managed Vulnerability Service	
B	Mapped network mapping, file structure and segments		• Managed Vulnerability Service	
C	Documented security controls and infrastructure		• Managed Vulnerability Service	
D	Documented endpoints (MAC address, OS)		• Managed Vulnerability Service	

		eSentire MDR	eSentire Managed Risk Services	eSentire Incident Response
Part 3: Security Program cont...				
E	Mapped cloud-based services and data		• Managed Vulnerability Service	
F	List of users, groups and privileges		• Managed Vulnerability Service	
C	Documented security controls and infrastructure		• Managed Vulnerability Service	
10	**Access Control to Sensitive Data and Systems**			
A	Documented and controlled user credential standards		• Managed Vulnerability Service • Security Program Maturity Assessment • Security Policy Guidance	
B	Documented and controlled user privilege standards		• Managed Vulnerability Service • Security Program Maturity Assessment • Security Policy Guidance	
C	Multi-factor authentication		• Managed Vulnerability Service • Security Program Maturity Assessment • Security Policy Guidance	
11	**Data Encryption and Retention**			
A	Controls and standards to encrypt storage devices		• Managed Vulnerability Service • Security Program Maturity Assessment • Security Policy Guidance	
B	Controls and standards to encrypt cloud devices		• Managed Vulnerability Service • Security Program Maturity Assessment • Security Policy Guidance	

		eSentire MDR	eSentire Managed Risk Services	eSentire Incident Response
Part 3: Security Program cont...				
C	Virtual private network (VPN) controls		• Managed Vulnerability Service • Security Program Maturity Assessment • Security Policy Guidance	
D	Documented data retention standards		• Managed Vulnerability Service • Security Program Maturity Assessment • Security Policy Guidance	
E	Documented data destruction standards		• Managed Vulnerability Service • Security Program Maturity Assessment • Security Policy Guidance	
12	**ICS and Industrial Controls**			
A	Discovery and control of workstations and devices		• Managed Vulnerability Service • Security Program Maturity Assessment • Security Policy Guidance	
B	Discovery of L2 devices (PLCs and controllers)		• Managed Vulnerability Service • Security Program Maturity Assessment • Security Policy Guidance	
C	Mapped industrial controls and intersections with IT		• Managed Vulnerability Service • Security Program Maturity Assessment • Security Policy Guidance	
D	Documented controls to update and maintain ICS systems		• Managed Vulnerability Service • Security Program Maturity Assessment • Security Policy Guidance	

		eSentire MDR	eSentire Managed Risk Services	eSentire Incident Response
Part 3: Security Program cont...				
13	**Mobile Devices**			
A	Documented data retention standards	• MDR for Endpoint	• Managed Vulnerability Service • Security Program Maturity Assessment • Security Policy Guidance	
B	Documented data destruction standards	• 24/7 SOC as a Service • MDR for Endpoint	• Managed Vulnerability Service • Security Program Maturity Assessment • Security Policy Guidance	
C	Documented data destruction standards	• 24/7 SOC as a Service • MDR for Endpoint	• Managed Vulnerability Service • Security Program Maturity Assessment • Security Policy Guidance	
14	**Back-up and Recovery**			
A	Documented back-up and recovery services		• Managed Vulnerability Service • Security Program Maturity Assessment • Security Policy Guidance	
B	Documented testing procedures		• Managed Vulnerability Service • Security Program Maturity Assessment • Security Policy Guidance	
15	**Application Testing and Maintenance**			
A	Documented controls to test new applications		• Managed Vulnerability Service • Security Program Maturity Assessment • Security Policy Guidance	
B	Documented controls to update applications		• Managed Vulnerability Service • Security Program Maturity Assessment • Security Policy Guidance	

		eSentire MDR	eSentire Managed Risk Services	eSentire Incident Response
Part 3: Security Program cont...				
C	Documented controls to verify application status		• Managed Vulnerability Service • Security Program Maturity Assessment • Security Policy Guidance	
16	**Continuous Monitoring for Unauthorized Access**			
A	Security monitoring and logging	• 24/7 SOC as a Service • Multi-signal MDR • Signals include network, endpoint, log, cloud, insider threat, vulnerability scans	• Managed Vulnerability Service • Security Program Maturity Assessment • Security Policy Guidance	
B	Proactive threat hunting	• 24/7 SOC as a Service including 24/7 Threat Hunting • Rapid human-led investigations • Multi-signal MDR • Signals include network, endpoint, log, cloud, insider threat, vulnerability scans		
17	**People and Training**			
A	Documented annual security awareness training		• Phishing and Security Awareness Training • External/Internal Penetration Test • Threat Advisories • Executive Briefing support	
B	Documented phishing testing		• Phishing and Security Awareness Training	
C	Documented red-team/blue-team exercises		• Red Team Exercises	
Part 4: Supply Chain Risk Management				
A	Documented supply chain risk management policy		• Vendor Risk Management Program • Security Programs Maturity Assessment • Security Policy Review	

		eSentire MDR	eSentire Managed Risk Services	eSentire Incident Response
Part 4: Supply Chain Risk Management cont...				
B	Documented procedures to evaluate vendors		• Vendor Risk Management Program • Security Programs Maturity Assessment • Security Policy Review	
C	Documented minimum security standards for vendors		• Vendor Risk Management Program • Security Policy Review • Vulnerability Management Program	
D	Documented security event notification for vendors		• Vendor Risk Management Program • Security Policy Review • Security Incident Response Planning	
E	Documented warranties, requirements and liability clauses		• Vendor Risk Management Program • Security Programs Maturity Assessment • Security Policy Review	
Part 5: Incident Response				
A	Documented and tested incident response plan			• Security Incident Response Planning
B	Documented team roles and responsibilities			• Security Incident Response Planning
C	Documented procedures for the collection of forensics			• Security Incident Response Planning
D	Documented reporting mechanisms and procedures			• Security Incident Response Planning
E	Documented notification procedures			• Security Incident Response Planning
F	Documented review and lessons learned procedures			• Security Incident Response Planning

If you're experiencing a security incident or breach contact us  **1-866-579-2200 or +44 (0)8000 443242**

eSENTIRE

eSentire, Inc., is The Authority in **Managed Detection and Response** Services, 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, human expertise, 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 and 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 Digital Forensic and Incident Response services. For more information, **visit www.esentire.com** and follow **@eSentire**.