ISPM FIELD NOTES

for Manufacturing

The manufacturing industry gets targeted by more cyberattacks than any other sector. Attacks continue to grow in volume and sophistication as attackers exploit human error, supply chain weaknesses, and gaps in observability. That makes Identity Security Posture Management (ISPM) essential to protecting uptime, intellectual property (IP), and compliance.

Use this 12-point ISPM Field Notes Guide to self-assess your current identity security practice, expertise, and the urgency with which you should act to strengthen defenses and extend trust and visibility across your entire ecosystems.

Simeio | Get access right now™

ISPM Field Notes for Manufacturing

A strategic imperative . . .

Verizon[1] confirmed 1,607 breaches impacting manufacturing companies in 2024 — almost twice as many as the year before and more than any other sector:

- Espionage-driven attacks accounted for 20% of breaches
- Third-party risk escalated with partners and supply chains involved in 30% of breaches
- Credential abuse remained the leading initial attack vector, involved in 22–32% of incidents[2]

33+%

Stolen credentials played a role in manufacturing breaches

The core of the identity crisis: Access

The human element remains cybersecurity's weakest link with 60% of breaches involving phishing or social engineering.[3] The growth of non-human identities — IoT devices, robotics, automation systems — only compounds the problem with under-secured, sometimes over-privileged machines.

60%
of manufacturing breaches start with intrusion – malware, hacking, vulnerabilities

66%
Malware is present in manufacturing breaches

37%
Ransomware attacks increased in now playing a role @ 45% of breaches

A way of life vs. a one-time upgrade

Identity Security Posture Management (ISPM) is proactive cybersecurity that continuously monitors, assesses, and improves the way your organization manages digital identities (human and machine) across every system, application, and supply chain connection. Unlike traditional identity and access management (IAM) that focuses on authentication and permissions, ISPM delivers a real-time, unified view of every identity, privilege, and risk across your entire business.

Use the following guide to automatically detect gaps — like over-privileged accounts, orphaned users, and misconfigured access — to stop attacks from halting production, stealing IP, and destroying trust within your ecosystem. An essential business enabler – versus another tool or routine upgrade — ISPM keeps production lines running:

- Find and close identity gaps before attackers exploit them
- Streamline compliance and audit readiness
- Capture and generate the right data, insights, and automation
- Move from reactive firefighting to proactive, resilient security

12-Point ISPM Field Guide for Manufacturing

Enterprises all need to give the right people the right access. For some, it makes sense to engage a managed identity and access management provider to build, scale, consolidate, or fix their identity programs when:

1. **Integrate Identity Providers (IdPs), cloud platforms, SaaS apps, and on-premises systems.**
   - Do you have a way to ensure integrations are kept up to date automatically?
   - Do integrations cover on-premises legacy and custom systems?

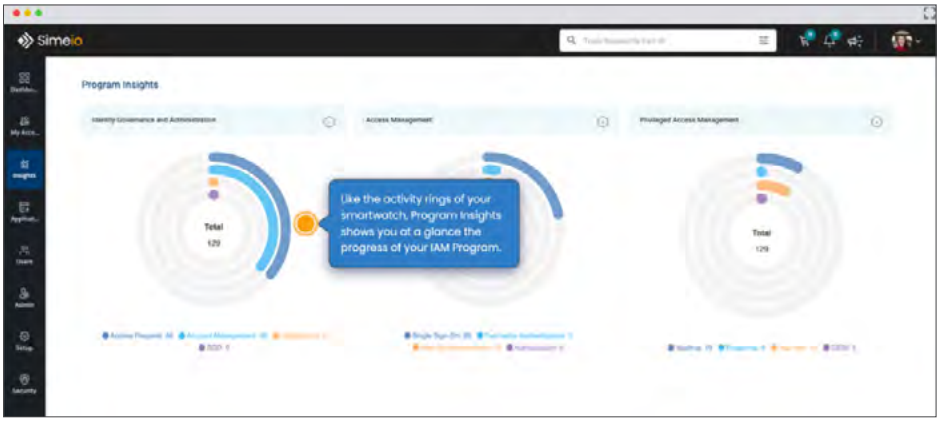
2. **Aggregate and visualize identity data**
   - Can you see everything in one portal or dashboard?
   - Does your dashboard provide real-time visibility?
   - Does it automatically visualize relationships, permissions, and risk exposure?

3. **Automate risk assessment**
   - Do you monitor for anomalies and unusual access patterns 24/7?
   - Does your identity security system automatically identify:
     - ☐ MFA enrollment
     - ☐ Policy violations
     - ☐ Cloud and SaaS apps
     - ☐ Orphaned accounts
     - ☐ Identification of potential insider threats
     - ☐ On-premises and legacy systems

4. **Automate detection and alerting of risk**
   - Do you have visibility to both managed and third-party identities? Both in the cloud and on-prem?
   - Do you continually scan for vulnerabilities and misconfigurations?
   - Does your monitoring solution(s) detect:
     - ☐ Failed MFA attempts
     - ☐ Excessive privileges
     - ☐ Orphaned or shared accounts
     - ☐ Service accounts

5. **Prioritize issues**
   - Can you prioritize based on attack chains and business context?
   - Which have the potential to disrupt production, compromise sensitive data, or enable lateral movement throughout your IT and OT environments?

6. **Implement identity security posture scoring**
   - Can you generate and regularly update a reliable identity security posture score?
   - Are you able to chart and document progress and demonstrate value to stakeholders?



What's in a number?
Assign a risk posture score to identity security to chart progress and demonstrate the value of strategic investments in IAM — multifactor authentication (MFA), single sign-on (SSO), and privilege access management (PAM).

7. **Automate compliance and audit readiness**
   - Does your solution help streamline collection of audit trail evidence?
   - Does it simplify reporting and policy enforcement to meet evolving regulations:
     - ☐ NIST Cybersecurity Framework (CSF)
     - ☐ NIST SP 800-171
     - ☐ NERC CIP (for energy-related manufacturing)
     - ☐ HIPAA
     - ☐ ISO/IEC 27001
     - ☐ ISA/IEC 62443
     - ☐ GDPR

8. **Implement and enforce least-priviledge access principles**
   - Do you have a way to continuously review and right-size access rights to prevent "privilege creep"?

9. **Strengthen supply chain and third-party identity controls**
   - Have you implemented 'just-in-time' access controls and automated offboarding for third-party users?
   - Do you maintain visibility into all supplier and partner identities accessing your systems?

10. **Automate onboarding and offboarding of users**
    - Do you have a way to automatically disable access for orphaned accounts?

11. **Integrate ISPM tools with IT workflows, ticketing and messaging platforms**
    - Are IT ticketing and messaging platforms integrated to streamline incident response and remediation workflows?Do you have a process for escalating critical identity threats through your messaging workflows?
    - Can you ensure all relevant stakeholders stay informed about identity threats and risk resolution?
    - Are ITDR tools integrated seamlessly with existing IT workflows?

12. **Eliminate passwords – the weakest link in security — everywhere you can**
    - Can you ensure seamless integration of passwordless authentication with your existing manufacturing systems and processes?
    - Is passwordess authentication flexible to support biometrics, hardware tokens, and other user-preferred methods?

Simeio | Get access right now™

info@simeio.com | www.simeio.com