ISPM FIELD NOTES

for Energy & Utility Companies

Along with the perennial risk from ransomware and other malware attacks, power companies and other public and private utilities face mounting risk from nation-state threats targeting critical infrastructure (CI). Modernization efforts — like expanding IT networks to include legacy and operational technology (OT) systems, cloud services, machine identities, and third-party vendors and suppliers — create omplexity and dangerous visibility and security gaps.

Identity Security Posture Management (ISPM) helps providers maintain control and compliance to protect uptime, public safety, govnerment funding, and business continuity. Identity and access management (IAM) and security leaders can use this 12-point ISPM Field Notes Guide to assess their identity security journey and the next steps to take in ruggedizing defenses and threats to their workforce, customers, and extended supply chain.

ISPM Field Notes for Energy & Utility Companies

A critical imperative . . .

Research from the TrustWave SpiderLabs[1] team found that 80+% of ransomware attacks against energy and utility companies use phishing as the initial attack vector. In 2024, threat actors continued to use proven security tactics to compromise credentials and identities:

- 67% of credential access techniques used brute force tactics (TrustWave)
- The majority of attacks on CI targeted identity infrastructure like Active Directory
- Many attacks abuse privileged identities—including undersecured machine identities— through service account compromise or lateral movement[2]

60/day

the number of susceptible points in North American electrical networks is rapidly increasing

North American Electric Reliability Corporation (NERC)

The core of the energy crisis: Identity

Risk from both human and non-human identities — IoT devices, robotics, automation systems — continues to grow. The most concerning trends include:

- **Infostealer malware** that captures credentials from undersecured user devices and other
- **Incomplete MFA coverage** across OT infrastructures including VPNs and SCADA that leaves credentials notably vulnerable
- **The integration of AI tools** introducing visibility gaps and new cyber risk

#1

The energy sector was the #1 targeted OT vertical in 2024

Dragos 2024 OT Cybersecurity Year in Review

100+

number of coordinated phishing and malware campaigns targeting energy and water infrastructure in 2024 as tracked by U.S. DOE

52%

of energy and utility companies reported a data breach in the past year

Thales Data Threat Report 2025

ISPM restores the power

Identity Security Posture Management (ISPM) takes a proactive cybersecurity approach. Like critical infrastructure itself, ISPM runs 24/7 to continuously monitor, assess, and improve the way companies manages digital identities (human and machine). A way of life vs. a one-time upgrade, ISPM delivers a real-time, unified view of every identity, privilege, and potential risk across every application, device, system, and supply chain connection at every location.

The 12-point Field Notes Guide to ISPM exposes gaps — like undersecured remote facilities, over-privileged accounts, orphaned users, and misconfigured access — so you can prioritize IAM investments to stop attacks from disrupting essential services or putting your service area at risk.

ISPM keeps utilities up and running by:

- Illuminating visibility and coverage gaps before attackers exploit them
- Streamlining federal, state, and industry compliance and audit readiness
- Capturing and generating data and insights to improve digitalization, convergence, and automation
- Enabling proactive, resilient 24/7 security

1 https://www.trustwave.com/en-us/company/newsroom/news/trustwave-unveils-2025-cybersecurity-threat-report-for-energy-and-utilities-sector-highlights-surge-in-ransomware-attacks/?utm_source=chatgpt.com

2 CyberArk 2024 Threat Report

12-Point ISPM Field Guide for Energy and Utility Companies

1. **Build and maintain up-to-date user and asset inventories**
   - Do you regularly—or automatically—update databases of users, devices, and service accounts across IT, OT, and IoT systems?
   - Are you regularly reviewing for dormant or orphaned accounts?
   - Do you have automated processes for removing access when employees or vendors leave?

2. **Implement and enforce least-priviledge access principles**
   - Do you have a way to continuously review and right-size access rights to prevent "privilege creep"?
   - Do you regularly identity and adjust over-privileged accounts?
   - Are access rights reconciled across both legacy and modern platforms?
   - Can you quickly identify and address unauthorized privilege escalation or shadow admin accounts?

3. **Implement 24/7 threat monitoring**
   - Are ICS, SCADA and other privileged accounts protected with strong controls and continuous monitoring?
   - Can you quickly identify and address anomalous behavior? Lateral movement?
   - Are you actively monitoring for identity-related misconfigurations?

4. **Implement strong, phishing-resistant authentication**
   - Is multi-factor authentication (MFA) enabled and required for all privileged and remote access users, including contractors and third parties?
   - Does MFA feature strong, AAL3-compliant techniques like verified push, passwordless, and biometics?

5. **Accelerate response**
   - Can you quantify and reduce the average time it takes your team to detect and respond to security threats?

6. **Strengthen supply chain and third-party identity controls**
   - Is third-party and supply chain access governed and monitored?
   - 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?

7. **Improve compliance and audit workflows**
   - Are your identity security practices aligned with industry regulations like NERC CIP and NIS2?
   - Can you easily produce audit trails during access and compliance reviews?

8. **Improve analytics – Aggregate, visualize, and analyze identity data to improve your security practice**
   - 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?

9. Automate risk assessment and alerting

- 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
- Does your monitoring solution(s) detect:
  - ☐ Failed MFA attempts
  - ☐ Excessive privileges
  - ☐ Orphaned or shared accounts
  - ☐ Service accounts

10. Apply threat intelligence and automation to prioritize risk

- Can you prioritize based on attack chains and business context?
- Which have the potential to disrupt operations or compromise sensitive data?

11. Automate onboarding and offboarding of users

- Do you have a way to automatically disable access for orphaned accounts?

Guage your progress
Assign a risk posture score to measure your identity security progress advance your IAM and Zero Trust journeys.

12. 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?

BONUS TIP: 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 passwordless authentication flexible to support biometrics, hardware tokens, and other user-preferred methods?

Simeio | Get access right now™

info@simeio.com | www.simeio.com