



COUNTERINTELLIGENCE & PERSONNEL RISK ENTERPRISE SECURITY SOLUTION

351X: THE SOLUTION

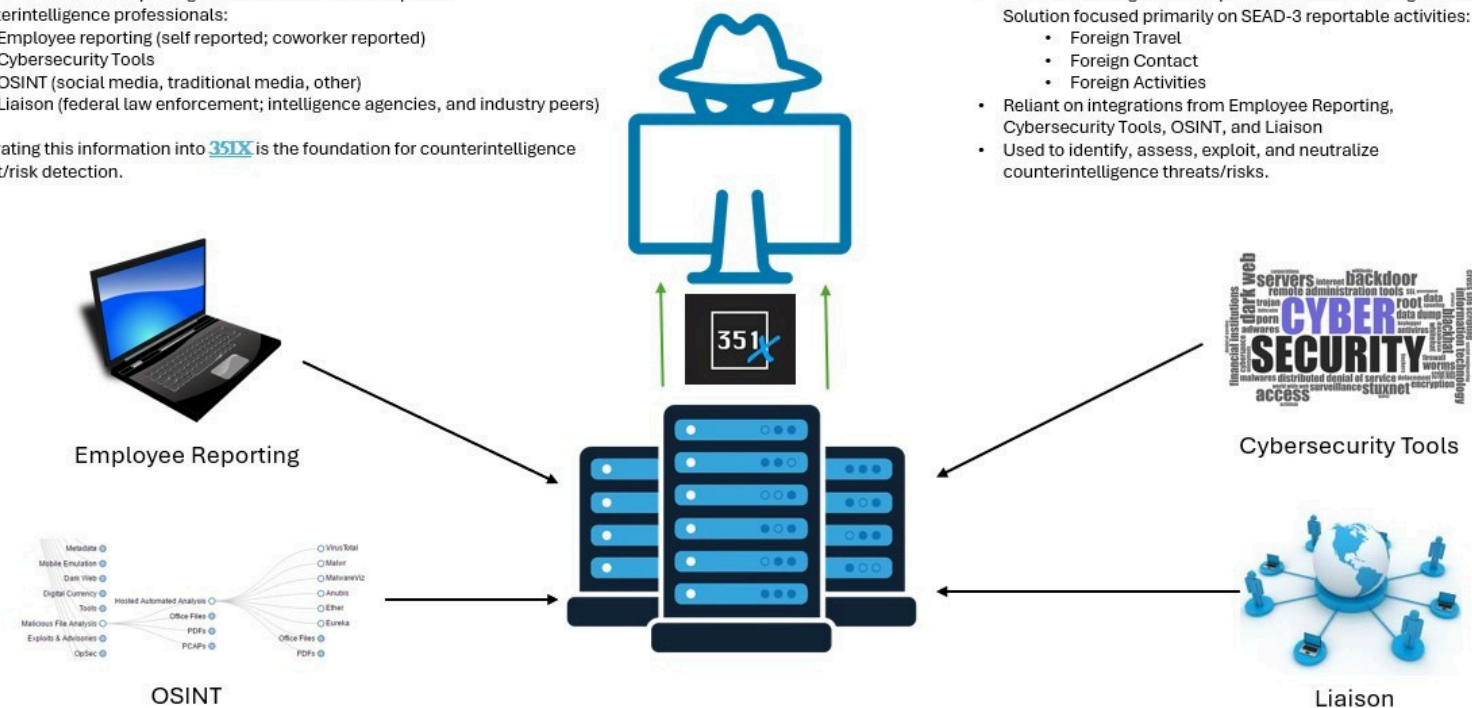
There are 4 essential reporting channels available to corporate counterintelligence professionals:

- Employee reporting (self reported; coworker reported)
- Cybersecurity Tools
- OSINT (social media, traditional media, other)
- Liaison (federal law enforcement; intelligence agencies, and industry peers)

Integrating this information into 351X is the foundation for counterintelligence threat/risk detection.

351X

- A Counterintelligence Compliance and Case Management Solution focused primarily on SEAD-3 reportable activities:
 - Foreign Travel
 - Foreign Contact
 - Foreign Activities
- Reliant on integrations from Employee Reporting, Cybersecurity Tools, OSINT, and Liaison
- Used to identify, assess, exploit, and neutralize counterintelligence threats/risks.



EMPLOYEE REPORTING

Comply with NISPOM and SEAD-3 requirements through employee self-reporting of Foreign Travel, Foreign Contact, and Counterintelligence Incidents.

CYBERSECURITY TOOLS

Integrate cybersecurity tools through APIs enabling faster and more efficient investigations:

OPEN SOURCE INTELLIGENCE

Incorporate open-source intelligence feeds for threat and risk identification, investigations, and mitigation.

LIAISON

User submission of external/internal liaison reports and integration with external public/private entities to enable CI analysis, investigations, and reporting.



Visit Our Website
www.ixnsolutions.com



Email
info@ixnsolutions.com