DITMAC

AUGUST 2025

NITAM NOTES

CYBERSECURITY

MISSION PARTNERS

Information technology (IT) networks provide an avenue for detecting concerning behavior in the workplace and are at a nexus of insider threat mitigation planning. Cybersecurity professionals as InT practitioners provide the technical and analytic perspective, of a person's behavior in this cyberspace, that brings forth and addresses unique InT risk indicators. Armed with both technical and analytic skillsets, Cybersecurity can detect and triage anomalous user (human) and technical activity, contributing to the holistic analysis of insider threat and information threat management planning

BARRIERS & CHALLENGES

- Translating systems behavior (e.g., UAM triggers, reported statements on social media, security violations) into meaningful InT activity for analysis
- Privacy/information security laws and user monitoring limitations
- Data access sharing policies between disparate databases and data owners
- Continuously evolving threat landscape; new vulnerabilities, methods, behaviors
- Coordination of cybersecurity, physical security, and insider threat timelines and planning for threat mitigation

CYBERSECURITY CONTRIBUTIONS

- Expertise and insight to synthesize analysis of technological indicators and anomalous activity to identity patterns on the "critical pathway" to a malicious act, providing opportunities for early threat mitigation
- Incident handling to triage cyber related incidents such as privileged abuse, data loss/exfiltration, phishing, malware, and system vulnerability exploitation
- Context-based analysis, beyond raw data monitoring, to identify incident 5W, and enable informed decision-making
- Ethical data incorporation from observed network activity, personal Internet based services (e.g. social media, email), and reported risks to add critical context about an individual's motivations, stressors, and intentions

PARTNERSHIP IMPACTS

- ***Cyber Partnership:*** Including cybersecurity professionals as mission partners and members of InT working groups enables Multidisciplinary Team (MDT) information sharing required to identify behavioral indicators, concerning online activity, and improve UAM detection.
- ***Coordinated Efforts:*** By early engagement with cybersecurity professionals through the MDT, security actions required for information security can be integrated as part of a holistic risk management plan protecting information and personnel assets
- ***Unifying Reporting Pathways:*** DoD policy requires all authorized users to "immediately" report data spills and "potential threats and vulnerabilities" through cybersecurity, meaning incidents may be directly reported through information security that informs insider threat analysis
- ***Developing Best Practices:*** Cybersecurity contributes relevant threat-based intelligence and risk informed data to establish UAM and behavioral analytic best practices, threat/risk-based profiles, efficient resource allocation, and effective InT program sustainment

KEY CONTRIBUTIONS

DETER

- Utilize behavioral principles to create a security culture that encourages compliance and discourages risky behaviors
- Create comprehensive training programs that educate users about common cyber threats (e.g., phishing, malware, social engineering), secure practices, and acceptable use.

DETECT

- Implement advanced security monitoring tools to identify unusual user behavior and system activity
- Identify cyber-driven threat indicators that improve detection and provide systems activity alerts
- Concerning online behavior analysis of Publicly Accessible Information (PAI)
- Streamline reporting; empower users to become an active part of the detection process.

MITIGATE

- Implement strict logical and physical access control to prevent further damage or compromise.
- Utilize countermeasures that reduce threat landscape and improve security posture.
- Hold accountable those who have created risk or loss through unauthorized cyber activity