CERT Insider Risk Overview

MARCH 27, 2023

Randy Trzeciak
Dan Costa

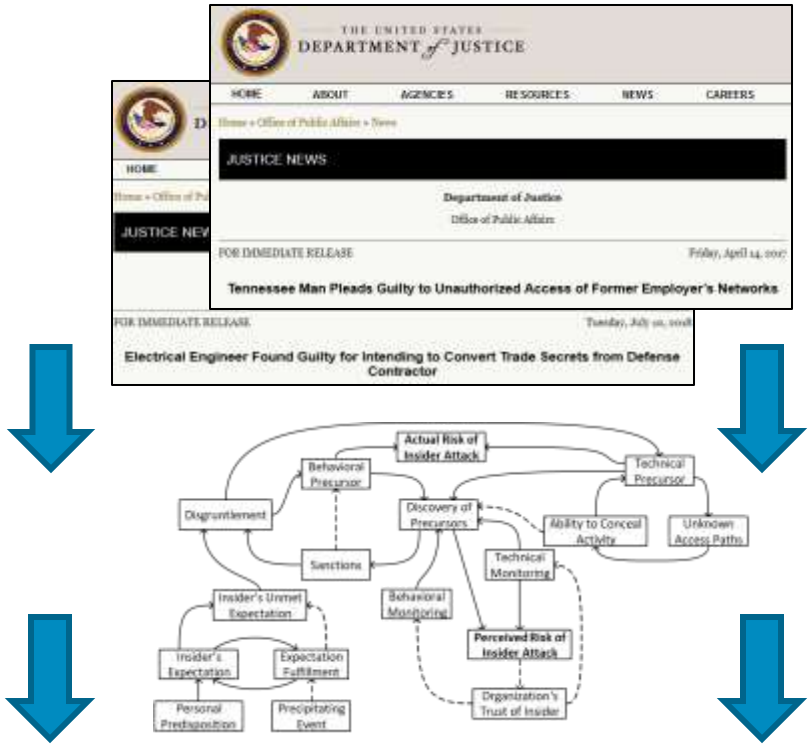
Carnegie Mellon University
Software Engineering Institute

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM23-0275

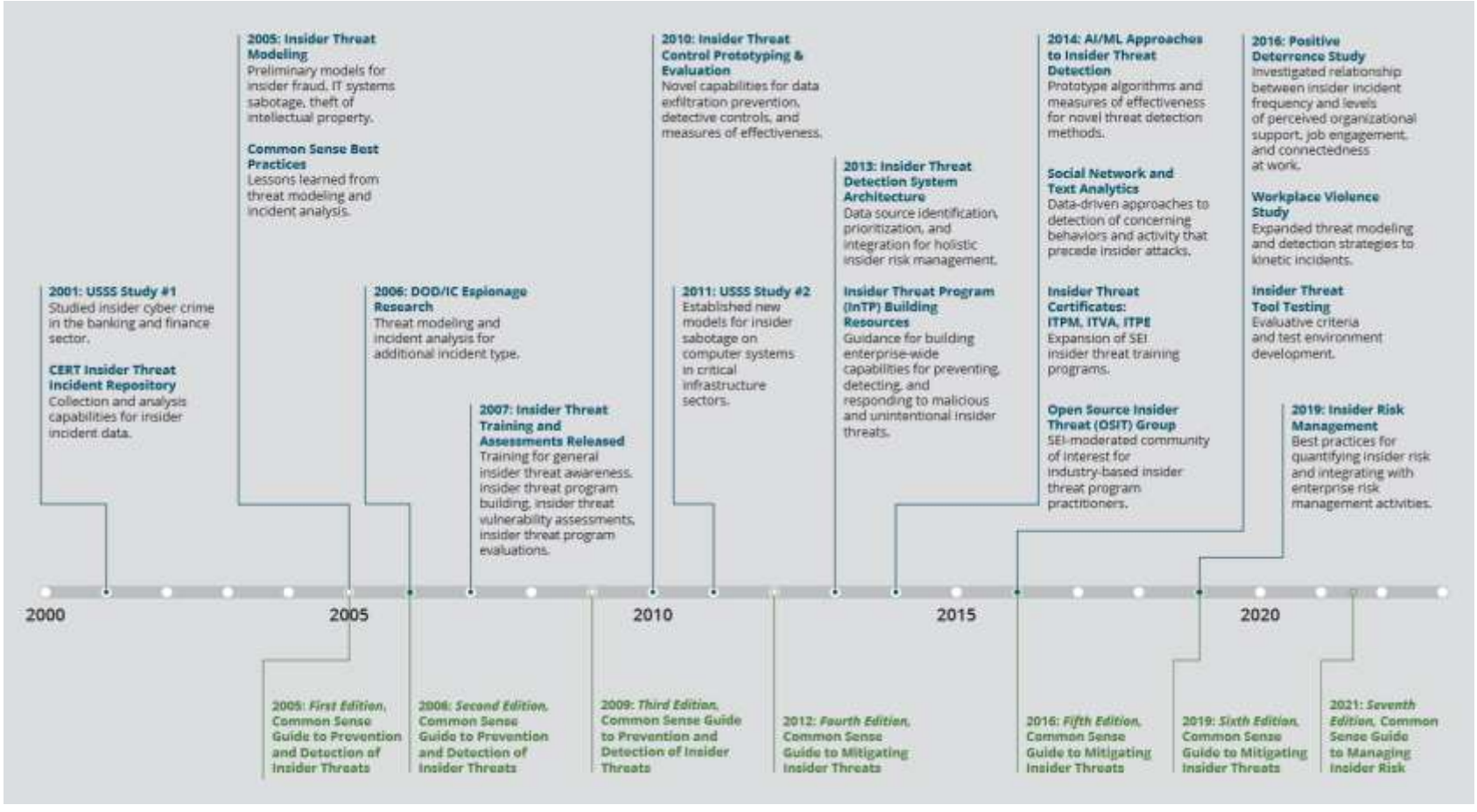
Insider Risk Research at CERT




```
Splunk Query Name: Last 30 Days - Possible Theft of IP
Terms: 'host=HECTOR [search host="zeus.corp.merit.lab" Message="A user account was  disabled. *" |
eval Account_Name=mvindex(Account_Name, -1) | fields Account_Name | strcat Account_Name
"@corp.merit.lab" sender_address | fields - Account_Name] total_bytes > 50000 AND
recipient_address!="*corp.merit.lab" startdaysago=30 | fields client_ip, sender_address,
recipient_address, message_subject, total_bytes'
```

Conducting data collection, modeling, analysis, and outreach to develop socio-technical solutions that verifiably reduce the impact and likelihood of misuse of authorized access to organizations' critical assets

History of Insider Risk Research at the SEI



https://resources.sei.cmu.edu/asset_files/WhitePaper/2022_019_001_886876.pdf

USG Mission Impact

Carnegie Mellon University Software Engineering Institute

Developed widely-used models and potential risk indicators for common insider incident types

Influenced relevant policy, (National Insider Threat Policy, DoD Insider Threat Policy) standards, (National Insider Threat Task Force Minimum Standards, NIST 800-53 Rev. 4 Insider Threat Controls) and component-specific procedures

Informed efficient acquisition activities for multiple components, including the development of scalable testing and evaluation capabilities

Advanced the state of the art in applying multidimensional anomaly detection to insider risk mitigation, reducing false positive rates of detection analytics and increasing analyst efficiency

Transitioned research findings through over 150 publications and a training suite that prepares DoD insider threat analysts, program managers, and vulnerability assessors

Current Portfolio Overview

Carnegie Mellon University Software Engineering Institute

Insider Threat Program Evaluation, Vulnerability Assessment, and Program Building	Multi-dimensional anomaly detection for insider risk mitigation	Architecture analysis and acquisition strategy for scalable, cost-effective, cross-domain detection and prevention capabilities
Improved technical detection capabilities through experimentally-derived knowledge of the most effective combinations of AI/ML approaches, data sets, and risk indicators	Reduced time to evaluate the efficacy, scalability, and cost of insider risk management controls through cloud-based modeling and simulation capabilities	Timely, risk-based measures of personnel trustworthiness through novel data collection capabilities and evidence-based refinements to existing processes

Leading and Advancing the Research

Carnegie Mellon University Software Engineering Institute

Study, prototype, and transition methods capable of identifying and mitigating novel sources of insider risk in highly autonomous environments.

- Develop an evidence-based extension of the critical path to insider risk that models incident progression involving autonomous agents
- Enhance insider risk management framework with controls that verifiably reduce insider risk for human/machine teams

Study, make, and transition insider risk management techniques designed to optimize return on security investment, reduce complexity, and reduce time to deployment.

- Extend insider threat modeling, simulation, test, and evaluation capabilities to include organizational factors for insider risk
- Demonstrate return on risk investment for positive deterrence-based controls as an enhancement to traditional insider risk management controls
- Develop technical detection capabilities for insider susceptibility to mis, dis, and mal-information influence campaigns

Contact Information

Randy Trzeciak
Deputy Director, Cyber Risk and Resilience

Telephone: +1 412.268.7040
Email: rft@sei.cmu.edu

Dan Costa
Technical Manager, Enterprise Threat and Vulnerability Management
Telephone: +1 412.268.8006
Email: dlcosta@sei.cmu.edu