SEI Bulletin

CERT Symposium to Explore Insider Risk Management

September 2, 2020 — The Software Engineering Institute's (SEI) CERT National Insider Threat Center (NITC) will hold its seventh annual symposium over two virtual sessions on September 10 and 24. This year's event for members of the Department of Defense, U.S. and international governments, and public-sector insider threat programs will focus on the latest challenges and best practices in insider risk management from the SEI's researchers and insider threat program practitioners in both government and industry.

The NITC Symposium 2020 supports National Insider Threat Awareness Month this September. For the second year running, the National Counterintelligence and Security Center, National Insider Threat Task Force (NITTF), Office of the Undersecretary of Defense for Intelligence and Security, Department of Homeland Security (DHS), and Defense Counterintelligence and Security Agency (DCSA) are partnering with insider threat community stakeholders to emphasize the importance of safeguarding the nation from insider threats.

Read more »

Insider Threat Resources from the SEI

[Common Sense Guide to Mitigating Insider Threats, Sixth Edition](#) – Report
Recommendations for mitigating insider threat based on the CERT Division's continued research and analysis of more than 1,500 insider threat cases.

[The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)](#) – Book
Best practices for managing the security and survivability of people, information, technology, and facilities.

[Insider Threats During Pandemic Conditions](#) – Collection
Resources from the CERT National Insider Threat Center on the unique set of insider threat risks and strategies during pandemic conditions.

[Insider Threats: Your Questions. Our Answers.](#) – Webcast
Our experts provided an overview of the ongoing research in this area, and answered questions about how the threat landscape continues to evolve.

[Navigating the Insider Threat Tool Landscape: Low-Cost Technical Solutions to Jump-Start an Insider Threat Program](#) – White Paper
Low-cost technical solutions that can help organizations prevent, detect, and respond to insider incidents.

[Insider Threat Blog](#)

- [Maturing Your Insider Threat Program into an Insider Risk Management Program](#)
- [5 Best Practices to Prevent Insider Threat](#)

 SEI News

[CERT Symposium to Explore Insider Risk Management](#)
SEI experts will host the virtual event in September in support of National Insider Threat Awareness Month.

[SEI Releases Source Code for Internet-of-Things Security Platform Kalki](#)
The innovative, software-defined IoT security platform is now available to the community for testing.

[Can We Trust Our Cyber-Physical Systems?](#)
An SEI-led team is developing the rapid certifiable trust approach: a

lightweight, scalable method to rapidly validate safe behavior of cyber-physical systems.

See more news »

 Latest Blogs

[Is Your Organization Using Cybersecurity Analysis Effectively?](#)
Angela Horneman defines analysis, describes what constitutes a security problem, and surveys analysis methods.

[Follow the CUI: 4 Steps to Starting Your CMMC Assessment](#)
Matt Trevors gives four steps for identifying DIB organizations' controlled unclassified information exposure.

[Managing the Risks of Adopting AI Engineering](#)
Brett Tucker describes some steps for exploring and controlling the risks of adopting AI in organizations.

See more blogs »

 Latest Podcasts

[Developing an Effective CMMC Policy](#)
Andrew Hoover and Katie Stewart, Cybersecurity Maturity Model Certification (CMMC) architects, present guidelines for developing an effective CMMC policy.

[The Future of Cyber: Educating the Cybersecurity Workforce](#)
Bobbie Stempfley interviews Dr. Diana Burley, executive director and chair of the Institute for Information Infrastructure Protection, or I3P, and vice provost for research for American University.

[Documenting Process for CMMC](#)
Andrew Hoover and Katie Stewart, Cybersecurity Maturity Model Certification (CMMC) architects, discuss process documentation, a Level 2 requirement.

📄 Latest Publications

[Using Deep Neural Networks to Detect Compromised Hosts in Large-Scale Networks](#)
This presentation discusses the generation of a dataset based on real network data fused with actual threat lists and contextual information.

[Code Similarity Detection Using Syntax-Agnostic Locality Sensitive Hashing](#)
This presentation shows how to maintain the security of large codebases by using Syntax-Agnostic Locality Sensitive Hashing (LSH) to detect and search for code similarity.

[NICE Framework Cybersecurity Evaluator](#)
This cybersecurity evaluator assesses members of the cyber workforce within the scope of the NICE Cybersecurity Workforce Framework.

🎬 Latest Videos

Webcast - [Risk Management for the Enterprise–How Do You Get Executives to Care About Your Risks?](#)
Brett Tucker and Matthew Butkovic discuss the OCTAVE FORTE process.

Webcast - [Quality Attribute Concerns for Microservices at the Edge](#)
Marc Novakouski and Grace Lewis review characteristics of edge environments with a focus on architectural qualities.

Webcast - [Agile in Government: Go for Insight, Not Just Oversight](#)
This webcast provided practical insights into how a Government Program Office can productively engage with a contractor using Agile and Lean methods.

📅 Upcoming Events

Webcast - [Follow the CUI: Setting the Boundaries for Your CMMC Assessment](#)
Model architects Gavin Jurecko and Matt Trevors will review several steps for identifying controlled unclassified information (CUI) exposure.

[National Insider Threat Center (NITC) Symposium 2020, Sep. 10 & 24](#)
This year's event will focus on proactive approaches to reducing the impact and likelihood of insider incidents within organizations.

[NatCSIRT 2020](#)
National CSIRTs can share information, tools, techniques, and strategies that address problems unique to CSIRTs that are responsible for a nation or an economy.

[FloCon 2021](#)
Our theme of Using Data to Defend is more critical than ever, given the security challenges of moving customers and vendors online and supporting a remote workforce.

> **Note:** The SEI is evaluating all upcoming courses, conferences, and events case-by-case in light of COVID-19 developments. Check individual event pages for the latest information.

[See more events »](#)

📜 Upcoming Training

[Insider Threat Program Manager: Implementation and Operation](#)
October 27-29, 2020 (SEI, live online)

[Insider Threat Vulnerability Assessor Training](#)
December 8-10, 2020 (SEI, live online)

> **Note:** The SEI is evaluating all upcoming courses, conferences, and events case-by-

case in light of COVID-19 developments. Check individual training pages for the latest information. You may also contact us at courseregistration@sei.cmu.edu or +1-412-268-7388.

See more courses »

Employment Opportunities

Software Engineer - C Programmer

Embedded Software Developer

All current opportunities »

Carnegie Mellon University
Software Engineering Institute