SEI Bulletin

Trouble reading this email? View in browser.

AI Engineering Report Highlights Needs and Challenges to Focus Emerging Discipline

November 11, 2020 — A report recently released by the SEI highlights three areas of focus for the growing artificial intelligence (AI) engineering movement: robust and secure AI, scalable AI, and human-centered AI. The report is based on ideas shared in a 2019 workshop the SEI convened to identify challenges and opportunities for AI engineering for defense and national security.

Read more »

SEI News

AI Engineering Report Highlights Needs and Challenges to Focus Emerging Discipline

The conclusions of a 2019 SEI workshop describe nine areas of need for the defense and national security AI systems of the future.

SEI Releases Software Engineering Measurement and Analysis Course Materials
Presentations and sample datasets for three courses on software product and process improvement are now available to download from the SEI website.

Office of the Director of National Intelligence Sponsors SEI to Lead National AI Engineering Initiative
The SEI, with funding and guidance from the ODNI, will lead a national initiative to advance the discipline of AI engineering for defense and national security.

See more news »

Latest Blogs

3 Ransomware Defense Strategies
Marisa Midler explores strategies to mitigate RDP attacks and software vulnerabilities, as well as how to protect against data exfiltration.

A Public Repository of Data for Static-Analysis Classification Research
Lori Flynn describes a new repository of labeled data that CERT is making publicly available for many code-flaw conditions.

Vulnonym: Stop the Naming Madness!
Leigh Metcalf describes the CERT/CC's new tool for giving vulnerabilities neutral names.

See more blogs »

Latest Podcasts

A Stakeholder-Specific Vulnerability Categorization
Eric Hatleback, Allen Householder, and Jonathan Spring, vulnerability and

incident researchers, discuss SSVC and go through a sample scoring vulnerability.

Optimizing Process Maturity in CMMC Level 5
Andrew Hoover and Katie Stewart, CMMC model architects, discuss the Level 5 process maturity requirements: standardizing and optimizing a documented approach for CMMC.

Reviewing and Measuring Activities for Effectiveness in CMMC Level 4
Andrew Hoover and Katie Stewart, CMMC model architects, discuss reviewing and communicating CMMC activities and measuring those activities for effectiveness, Level 4 requirements of the model.

See more podcasts »

Latest Publications

Analytic Capabilities for Improved Software Program Management
This white paper describes an update to the SEI Quantifying Uncertainty in Early Lifecycle Cost Estimation approach.

AI Engineering for Defense and National Security: A Report from the October 2019 Community of Interest Workshop
this report identifies recommended areas of focus for AI Engineering for Defense and National Security.

DevSecOps Days DC 2020
Presentations from DevSecOps Days DC 2020, held virtually on October 1.

See more publications »

Latest Videos

Webcast - Threats for Machine Learning
Mark Sherman explains where machine learning applications can be attacked, the means for carrying out the attack, and some mitigations you can use.

Webcast - Cyber Workforce Development and the Cybersecurity Engineer
Dennis Allen talks about how the SEI's Cyber Workforce Development team aims to streamline the building of cybersecurity expertise and amplify it to a globally distributed workforce.

Webcast - Follow the CUI: Setting the Boundaries for Your CMMC Assessment
CMMC architects review several steps for identifying CUI exposure in terms of their critical services and the assets that support them.

Upcoming Events

What Is Cybersecurity Engineering and Why Do I Need It? November 17
Cybersecurity engineering consolidates the tools and analyses used in various lifecycle steps to ensure effective operational results.

Artificial Intelligence for Humanitarian Assistance and Disaster Response Workshop, December 11
This workshop establishes dialogue between the AI and Humanitarian Assistance and Disaster Response (HADR) communities.

FloCon 2021, January 11-14, 2021
The 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

Software Architecture: Principles and Practices

January 19-22, 2021 (SEI, Live Online)

Cybersecurity Oversight for the Business Executive
January 20-21, 2021 (SEI, Live Online)

Insider Threat Program Manager: Implementation and Operation
January 26-28, 2021 (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, including live-online and eLearning offerings »

Employment Opportunities

Data Scientist

IT Security Engineer

All current opportunities »

Carnegie Mellon University
Software Engineering Institute