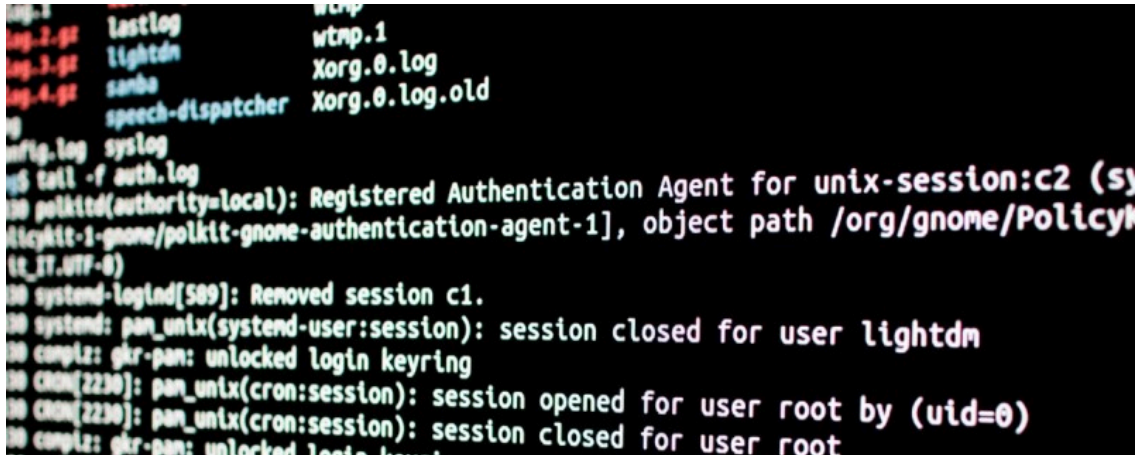


# SEI Bulletin

Trouble reading this email? [View in browser.](#)



```
log-1      wtmp
log-2.gz  lastlog   wtmp.1
log-3.gz  lightdm   Xorg.0.log
log-4.gz  samba     Xorg.0.log.old
          speech-dispatcher
          mftg.log  syslog
          tail -f auth.log
00 polkit(authority=local): Registered Authentication Agent for unix-session:c2 (sy
00 polkit-1-gnome/polkit-gnome-authentication-agent-1], object path /org/gnome/Policyh
00 system-logind[509]: Removed session c1.
00 system: pan_unix(system-user:session): session closed for user lightdm
00 complitz: gkr-pan: unlocked login keyring
00 CRON[2230]: pan_unix(cron:session): session opened for user root by (uid=0)
00 CRON[2230]: pan_unix(cron:session): session closed for user root
00 complitz: gkr-pan: unlocked login keyring
```

## How to Evaluate Large Language Models for Cybersecurity

**February 28, 2024**—Large language models (LLMs) could be an asset for cybersecurity professionals, but they should be evaluated using real and complex scenarios to better understand the technology’s capabilities and risks. These findings appear in a white paper released last week by the SEI and OpenAI.

*Considerations for Evaluating Large Language Models for Cybersecurity Tasks* provides a framework of 14 recommendations for evaluating LLMs for cybersecurity applications.

“Without a clear understanding of how an LLM performs on applied and realistic cybersecurity tasks, decision makers lack the information they need to assess opportunities and risks,” write the SEI coauthors of the paper in a recent blog post. “We contend that practical, applied, and comprehensive evaluations are required to assess cybersecurity capabilities.”

[Read more »](#)

[Download the paper »](#)

[Read the blog post »](#)

---



[SEI and OpenAI Recommend Ways to Evaluate Large Language Models for Cybersecurity Applications](#)

A new white paper says evaluation of LLM capability and risk should include real-world cyber scenarios, not just factual knowledge tests.

[Acquisition Security Framework for Managing Engineering and Supply Chain Cyber Risk Released](#)

The latest version of the framework completes the set of practices for acquiring and operating secure and resilient systems across the systems lifecycle.

[See more news »](#)

---



[CERT Releases 2 Tools to Assess Insider Risk](#)

The average insider risk incident costs organizations more than \$600,000. Roger Black talks about two new SEI CERT Division tools that help organizations assess their insider risk programs.

[OpenAI Collaboration Yields 14 Recommendations for Evaluating LLMs for Cybersecurity](#)

Jeff Gennari, Shing-hon Lau, and Samuel J. Perl summarize recommendations to help assessors accurately evaluate LLM cybersecurity capabilities.

[See more blogs »](#)

---



## Latest Podcasts

### [When Agile and Earned Value Management Collide: 7 Considerations for Successful Interaction](#)

Patrick Place and Stephen Wilson discuss seven considerations for successful use of Agile and EVM.

### [The Impact of Architecture on the Safety of Cyber-Physical Systems](#)

Jerome Hugues discusses challenges that arise from the increasing autonomy in cyber-physical systems, including transferring and processing multiple data streams.

[See more podcasts »](#)

---



## Latest Videos

### [Ask Us Anything: Supply Chain Risk Management](#)

Brett Tucker and Matthew Butkovic answer your enterprise risk management questions to help your organization achieve operational resilience in the cyber supply chain.

### [The Future of Software Engineering and Acquisition with Generative AI](#)

SEI researchers explore the future of software engineering and acquisition using generative AI technologies.

---



## Latest Publications

### [Considerations for Evaluating Large Language Models for Cybersecurity Tasks](#)

In this paper, researchers from SEI and OpenAI explore the opportunities and risks associated with using large language models (LLMs) for cybersecurity tasks.

### [Navigating Capability-Based Planning: The Benefits, Challenges, and Implementation Essentials](#)

Based on industry and government sources, this paper summarizes the benefits and challenges of implementing capability-based planning (CBP).

[Acquisition Security Framework \(ASF\): Managing Systems Cybersecurity Risk \(Expanded Set of Practices\)](#)

This framework of practices helps programs coordinate their management of engineering and supply chain risks across the systems lifecycle.

[See more publications »](#)

---



## [Upcoming Events](#)

Symposium - [Supply Chain Risk Management Symposium 2024](#), February 28

Join us to hear about the latest challenges and best practices in supply chain risk management (SCRM) from recognized leaders in SCRM research, as well as leading-edge practitioners from government and industry.

[Zero Trust Industry Day 2024](#), May 14-15

The SEI hosts the Zero Trust Industry Day request-for-information exercise to collect information from those who develop solutions for implementing a zero trust architecture.

[See more events »](#)

---



## [Upcoming Appearances](#)

[Inaugural Billington State and Local Cybersecurity Summit](#), March 19-20

This SEI-sponsored event convenes the senior-most cyber leaders to enhance cybersecurity at the state and local level. Visit the SEI booth in the exhibitor hall.

[Navy League Sea Air Space \(SAS\) 2024](#), April 8-10

Visit the SEI at booth 218 at the largest maritime exposition in the United States.

[See more opportunities to engage with us »](#)

---



## [Upcoming Training](#)

[Designing Modern Service-Based Systems](#)

March 12 (SEI Live Online)

[Design Guidelines and Patterns for Microservices](#)

March 18-21 (SEI Live Online)

[Insider Threat Analyst](#)

March 19-21 (SEI Pittsburgh)

[See more courses »](#)

---



## [Employment Opportunities](#)

[AI Security Researcher](#)

[Vulnerability Analysis - Technical Manager](#)

[Associate Machine Learning Engineer - Autonomy Lab](#)

[All current opportunities »](#)

**Carnegie Mellon University**  
Software Engineering Institute



Want to subscribe or change how you receive these emails?  
You can [subscribe](#), [update your preferences](#) or [unsubscribe from this list](#).