Protecting Emerging Technology Data Against Cyber Threats in Taiwan

Summary of Planned Event: Sandia National Laboratories, in partnership with the U.S. Department of State and the American Institute in Taiwan, invites key stakeholders in Taiwan to participate in a three-day event aimed at enhancing cybersecurity capabilities in emerging technology sectors. Scheduled for **14-16 April 2026** at the **Courtyard by Marriott Taipei Downtown (venue subject to change)**, this event will focus on monitoring, detecting, and responding to cyber incidents, with an emphasis on protecting sensitive dual-use technologies from cyber threats. The event is free to attend and will include a business lunch and refreshments provided to participants each day. The event will be conducted in English with simultaneous translation available if necessary. **You may register for the event online at:** https://rsec.sandia.gov/protecting-emerging-technology-data-against-cyber-threats-taiwan/

Who Should Attend:

- **IT and Cybersecurity Professionals in the Drone Industry, with Participation from Other Emerging Technology Fields:** Individuals responsible for monitoring, detecting, and responding to cybersecurity incidents within organizations or research institutions engaged in drone technologies, as well as related emerging technology areas such as artificial intelligence (AI), aerospace, smart manufacturing, and quantum technologies.
- **Example Job Titles:** SoC Analysts, Threat Hunters, Cyber Threat Intelligence Analysts, Incident Responders, Digital Forensics Practitioners, IT Administrators, etc.
- **Skill Levels:** This event is designed for participants of all skill levels, from beginners to experienced professionals. The lab-based format allows students to progress at their own pace; advanced participants can tackle more complex challenges, while beginners can focus on foundational concepts.

Topics Covered:

- **Cyber Threat Landscape:** Insights into current cyber threats posed by advanced persistent threats (APTs) targeting dual-use technologies.
- **Digital Forensics and Threat Hunting Techniques:** Participants will learn to leverage forensic data and analytical techniques to identify and mitigate cyber threats. The training will cover querying forensic data sets, extracting artifacts, and analyzing network and memory forensics.

Event Details

- **Format:** Three-day event with a mix of presentations and interactive exercises
- **Required Materials:** Participants should bring an internet-capable laptop, Hypervisor that supports x64 Windows (VMWare Workstation, Virtual Box, etc), 100GB of free hard drive storage for course virtual machine and ample memory to support the VM's 16GB+.
- **Dates:** 14-16 April 2026
- **Location:** Courtyard by Marriott Taipei Downtown; Taipei, Taiwan (subject to change)

For questions regarding this event, please contact RSEC@sandia.gov

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.
SAND2026-17013O

Protecting Emerging Technology Data from Cyber Attacks in Taiwan
Event Agenda

Taipei, Taiwan
14-16 April 2026

Day 1

Time	Agenda Module
8:30-9:00	Participant Arrival and Registration
9:00-9:15	Introduction *Brief background of instructors and structure of the course.*
9:15-10:15	Cyber Threat Landscape *Overview of Advanced Persistent Threats (APTs) along with their structures, capabilities, and motivations. Introduction to dual-use implications of emerging technologies.*
10:15-10:45	Group Photo & Break
10:45-12:00	Cyber Attack Case Studies Against Emerging Technology Sectors *Participants will learn from past incidents to strengthen current cybersecurity measures.*
12:00-13:00	Lunch
13:00-14:00	Overview of Forensic Data Sets Stored for Exercises *Go over data sources common to investigating cyber incident in security incident and event management platforms that will be used during the training exercise*
14:00-15:00	Introduction to KQL and How to Query Forensic Data Sets *Brief primer on utilizing Kusto Query Language for cyber incident investigation, hunting and response in Azure Data Explorer*
15:00 -15:15	Break
15:15 -16:15	How to Use Network Forensic Data Sets with Malcom *Overview of how to use network forensics tool Malcom and review network events and packet captures*
16:15	Wrap Up and Adjourn

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.
SAND2026-17013O

Protecting Emerging Technology Data from Cyber Attacks in Taiwan
Event Agenda

Taipei, Taiwan
14-16 April 2026

Day 2

Time	Agenda Module
9:00-09:30	Host Forensics Data Collection *Learn how to identify and collect relevant forensic data from host systems during a cyber incident.*
9:30 – 10:30	Host Forensics Memory Analysis – Processes and Network *Learn how to perform memory analysis to enumerate and examine process and network connections*
10:30-10:45	Break
10:45-12:00	Host Forensics Memory Analysis – Non-Volatile Artifacts *Learn how to perform memory analysis to enumerate and examine files, registry and event logs*
12:00-13:00	Lunch
13:00-15:00	Host Forensics Memory Analysis – Artifact Analysis and Timelines *Learn how to identify process injection and do temporal analysis on memory forensic images*
15:00-15:15	Break
15:15-17:00	Incident Response Exercise (Session 1) *Participants work in teams to review memory images and forensic data in SIEM environments to understand and respond to simulated incidents. They will be guided through investigation steps by answering questions in a capture the flag platform.*
17:00	Event Adjourn

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.
SAND2026-17013O

Protecting Emerging Technology Data from Cyber Attacks in Taiwan
Event Agenda

Taipei, Taiwan
14-16 April 2026

Day 3

Time	Agenda Module
9:00-10:15	Documentation Best Practices and Incident Information Management Systems *Learn what to document and how to keep track of incident information to brief management and executives*
10:15-10:30	Break
10:30-12:00	Incident Response Exercise (Session 2) *Participants continue their work from session 1, collaborating in teams to further analyze memory images and forensic data with ongoing guidance from facilitators.*
12:00-13:00	Lunch
13:00-15:00	Incident Response Exercise (Session 3) *Participants continue their work from session 2, collaborating in teams to further analyze memory images and forensic data with ongoing guidance from facilitators.*
15:00-15:15	Break
15:15-16:45	Final Incident Out-brief of Findings *Teams present executive out-brief of incident response findings*
16:45-17:00	Closing Remarks and Presentation of Course Certificates
17:00	Event Adjourn

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.
SAND2026-17013O