SECURONIX™

FREE CPE CREDITS (ISC)² | CPE SUBMITTER

Hands-on Threat Hunting Workshops

With many organizations opening up remote access for the first time to a broad segment of their workforce, attackers have begun exploiting users with less secure access in terms of weak passwords, and lack of MFA.

Securonix, the leader in next-gen SIEM and the visionary who introduced the industry to user and entity behavior analytics, invites you to join us for a **Virtual Hands-on Threat Hunting Workshop** on **Wednesday, May 27th**. We will provide an informational, educational, and interactive session for practitioners that focuses on how advanced analytics capabilities and threat hunting tools can help Cyber and Insider Threat teams quickly detect and investigate threats. The workshop is free to attend, and we are partnering with **(ISC)²** to offer **3.0 free CPE credits** upon completion of the workshop, for you to put toward maintaining your cybersecurity certifications.

Join us if you're experiencing any of the pain points below:

- Are you tired of swivel chair threat hunting?
- Do you struggle with alert fatigue, and the ability to attribute an alarm to a specific user or system to determine the level of risk?
- Are you interested in transitioning from countless alarms to critical threat alerts?

Here are some of the topics and activities you can expect:

- Strategies to enable more efficient threat hunting (hands-on exercises)
- A discussion on the benefits of a Modern SIEM:
    - UEBA capabilities automate the manual work of identified anomalies and high-risk activity in the environment
    - Threat models tie together disparate anomalies on the network and reduce time to investigate
    - Spotter and other investigation tools (i.e. link analysis) speed up the process of conducting investigation

Agenda:

- Securonix welcome (5 min)
- Introduction to the Securonix solution and how it enables more efficient threat hunting (20 min)
- Live demo of the Securonix environment and an explanation of the threat hunting exercise (15 min)
- Threat hunting exercise. (A PDF of the threat hunting exercise book and login credentials will be shared) (20 min)
- Break (15 min)
- Threat hunting exercise continued. Additional assistance will be provided to complete the exercise (30 min)
- Recap of the threat hunting exercise and follow-up demo of the Securonix solution. Deep dive walk-through of all of the steps documented in threat hunting exercise. Discuss the benefits of a Modern SIEM (45 min):
    - UEBA capabilities automate the manual work of identified anomalies and high-risk activity in the environment
    - Threat models tie together disparate anomalies on the network and reduce time to investigate
    - Spotter and other investigation tools (i.e. link analysis) speed up the process of conducting investigations
- Q&A and Networking (30 min)

And remember, attendees who complete the full workshop will receive **3.0 CPE credits awarded by (ISC)²** to apply toward their cybersecurity certifications.

Space is limited. Register today to save your seat for this exclusive opportunity:

REGISTER NOW