Train and Certify

For Organizations Security Awareness Resources Get Involved

About

Q 🌐 Log In Join

Talk with an expert

Home > Webcasts > Tech Tuesday Workshop Cobalt Strike Detection via Log Analysis

Tech Tuesday Workshop Cobalt Strike Detection via Log Analysis



Tuesday, 11 May 2021 1:00PM EDT (11 May 2021 17:00

UTC)

Speaker: Chad Tilbury

Cobalt Strike has become the attack tool of choice among enlightened global threat actors, making an appearance in almost every recent major hack. Cobalt Strike is an extremely capable and stealthy tool suite, but log analysis can level the playing field, providing many opportunities for detection. This workshop will leverage data sourced from SANS FOR508: Advanced Incident Response, Threat Hunting and Digital Forensics to provide insight into how Cobalt Strike operates and how to detect many of its characteristics via endpoint logs. Whether you are just starting out in threat hunting or a FOR508 alumni, there will be something for everyone in this new workshop!

Prerequisites: Participants will need a system running the Windows operating system to perform Windows event log analysis (virtual machines are okay). While logs will be provided in CSV format for attendees without access to Windows, your experience will be greatly diminished without native access to Windows logging libraries. Some familiarity with Windows event log is desirable.

System Requirements: Prior to the workshop, participants should prepare the following:

- A host or virtual machine running a Windows 64-bit operating system (Win7-Win10)
- Download and install Event Log Explorer 'https://eventlogxp.com/download.php
- Download and install Microsoft Sysinternals Sysmon: 'https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
- Install a tool capable of viewing and filtering CSV files (this is particularly important for attendees who do not have a system running the Windows OS)

Lab materials should be downloaded here: https://sansurl.com/cobalt-strikeworkshop-labs/

An optional final part of the workshop will include working with Cobalt Strike beacon malware. Examples will be given using SANS Linux-based SIFT virtual machine available here: https://digital-forensics.sans.org/community/downloads

*Please note: Due to the nature of these workshops, many have a capacity limit, so to help us offer this opportunity to as many people as possible, we are asking that you please only register if you plan to attend live.



En cliquant sur « Accepter tous les cookies », vous acceptez le stockage de cookies sur votre appareil pour améliorer la navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing.

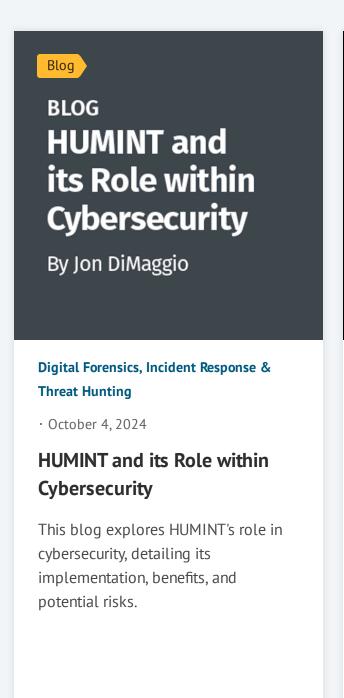
Autoriser tous les cookies

X

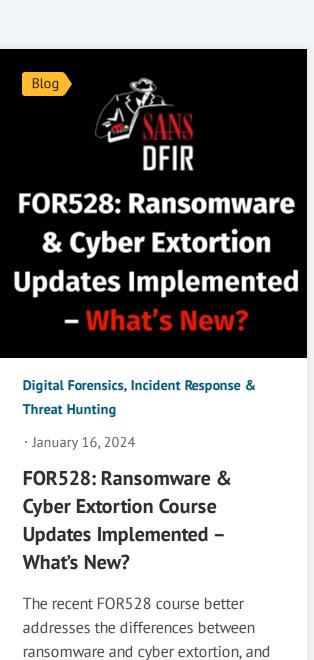
Paramètres des cookies



Related Content



Jon DiMaggio



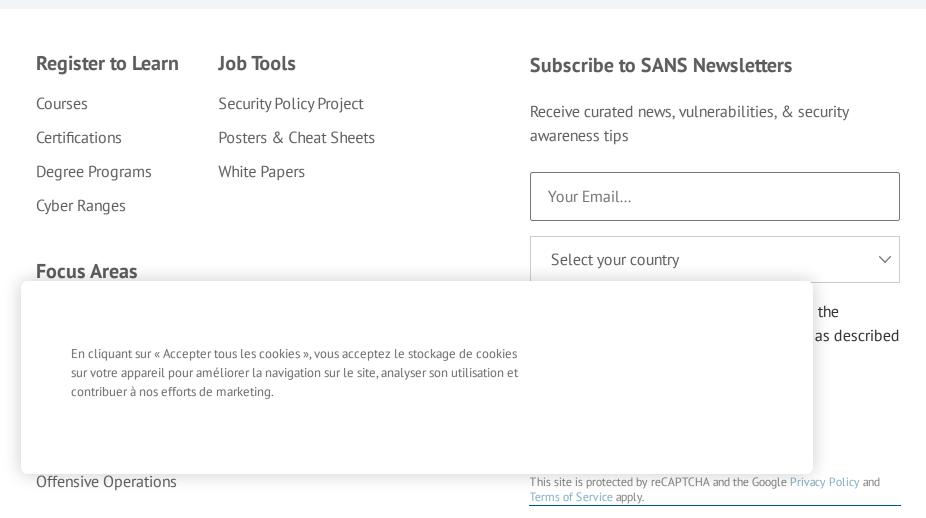
provides new hands-on labs and

Ryan Chapman

 \rightarrow

bonus content.





Tech Tuesday Workshop Cobalt Strike Detection via Log Analysis | SANS Institute - 02/11/2024 11:12 https://www.sans.org/webcasts/tech-tuesday-workshop-cobalt-strike-detection-log-analysis-119395/

Subscribe

© 2024 SANS® Institute Privacy Policy Terms and Conditions Do Not Sell/Share My Personal Information Contact Careers 💥 🕇 🕒 in

En cliquant sur « Accepter tous les cookies », vous acceptez le stockage de cookies sur votre appareil pour améliorer la navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing.