SANS EMEA

Hands On | Five Days | Laptop Required | 30 CPEs

ICS 515

ICS ACTIVE DEFENSE AND INCIDENT RESPONSE

This course teaches the skills needed to protect industrial control system networks against cyber threats. Students learn how to respond to and deny those threats by utilising active defence mechanisms in concert with incident response.

A fully hands-on approach to teaching ensures students develop a deep, technical understanding of key processes including:

- Generating and using threat intelligence
- Communicating control system needs to the IT team in order to deploy appropriate defences
- Detecting malicious actors or threats on control system networks
- Performing threat triage and incident response to ensure the safety and reliability of operations technology

Take ICS515 at SANS ICS Europe 2015

Amsterdam 22 - 26 Sept, 2015
Register online at **www.sans.org/event/ics-amsterdam-2015**

NEW

Who should attend

- IT and OT support
- IT and OT cybersecurity
- ICS engineers

Participants will gain hands-on experience with:

- CYBATIWorks Kit and Virtual Machine with PeakHMI
- Snort and Bro for tailoring and tuning Intrusion Detection System rules
- Wireshark and TCPDump for network traffic capturing and packet analysis
- FTK Imager and MD5Deep for forensic data acquisition and validation
- OpenIOC and YARA for developing Indicators of Compromise
- Xplico and NetworkMiner for network flow and data analysis

Hands-on training

- CYBATI Kit Setup
- Pattern and Information Mapping
- ICS Honeypot
- Consuming Threat Intelligence
- Asset Discovery and Network Visualisation
- Collecting the Right Data
- Detecting the Bad Data
- Analysing and Responding
- Acquisition and Verification
- Indicators in Action
- Capturing the Malware
- Dynamic Malware Analysis
- Neutralising Malware Callbacks
- IoC Development
- Targeted Attack Identification
- Day 5 is an entire day working through hands- on activities

For more information see our course catalogue or visit **www.sans.org/emea**

515.1 HANDS ON: ICS Threat Intelligence

Students will gain an understanding of threat intelligence and learn how to generate their own as well as utilise what is available in the community. Additionally, they will be able to write a technical report that can be used internally with IT defense teams to ensure control system defense needs are met.

Topics: Case Study: HAVEX; Introduction to Active Defense and Response; Lab: CYBATI Kit Setup; Intelligence Life Cycle and Threat Intelligence; ICS Information Attack Surface; Lab: Pattern and Information Mapping; External Threat Intelligence; Internal Threat Intelligence; Lab: ICS Honeypot; Sharing and Consuming Threat Intelligence; Lab: Consuming Threat Intelligence

515.2 HANDS ON: Asset Identification and Network Security Monitoring

Students will be introduced to the idea of active defense as well as cyber counter intelligence to limit their control system threat landscape and deploy effective detection and defense measures against known and unknown threats.

Topics: ICS Asset and Network Visibility; Lab: Asset Discovery and Network Visualisation; Identifying and Reducing the Threat landscape; ICS Network Security Monitoring – Collection; Lab: Collecting the Right Data; ICS Network Security Monitoring – Detection; Lab: Detecting the Bad Data; ICS Network Security Monitoring – Analysis; Lab: Analysing and Responding

515.3 HANDS ON: Incident Response

Students will learn how to safely and properly respond to an incident internally.They will be able to identify device malfunctions vs. cyber threats as well as prepare and utilise sources of forensic data that can benefit incident response.The outcome will be to determine if a shutdown is necessary in the facility or if they have time and the ability to triage and learn more.

Topics: Incident Response and Digital Forensics Overview; Incident Response Fundamentals; Building an ICS Incident Response Team; Preparing Ahead of Time; Sources of Forensic Data in ICS Networks; Remote and Local Systems; Lab: Acquisition and Verification; Time Critical Incident Response; Lab: Indicators in Action; Maintaining and Restoring Operations; Lab: Capturing the Malware

515.4 HANDS ON: Threat and Environment Manipulation

Students will learn how to operate through an attack and gain the information necessary to instruct teams and management on when operations must shutdown or if it is safe to respond to the threat and continue operations.The outcome will be identifying ways forward as well as additional information which can feed back to incident response teams and threat intelligence teams.

Topics:ICS Threat and Environment Manipulation Goals and Considerations; Establishing a Safe Working Environment; Malware Analysis Methodologies; ICS Malware Analysis Essentials; Lab: Dynamic Malware Analysis; Malware manipulation; Lab: Neutralising Malware Callbacks; Indicators of Compromise; Lab: IoC Development; Uncovering Ongoing Campaigns; Lab: Targeted Attack Identification; Environment Manipulation and Lessons Learned

515.5 HANDS ON: Active Defense and Incident Response Challenge

Students will go through a single scenario that combines the concepts and skills from the categories of threat intelligence, active defense, incident response, and threat triage. It will stress the circular nature of the process and how teams can work together to ensure safety and reliability on control networks.

Take ICS515 at SANS ICS Europe 2015

Amsterdam 22 - 26 Sept, 2015
Register online at:
www.sans.org/event/ics-amsterdam-2015

You will receive

- This course provides the student with a full functioning Cybati Works Mini-Kit
- The ICS515 kit includes a Raspberry PI with PiFace Digital, Snap-Circuit components, Wireless and Magnetic I/O, USB cables (with Volt/Amp meter), memory, and the Virtual Machine with OPC, HMI, PLC, RTU, I/O, industrial protocols, commercial control system demonstration software from Rex Controls and PeakHMI
- This course also makes use of numerous Virtual Machine environments throughout the hands-on labs

SANS EMEA

www.sans.org/emea

Email: emea@sans.org • **Tel:** +44 20 3384 3470
Address: SANS EMEA, PO Box 124,
Swansea, SA3 9BB, UK