ICS515: **ICS Visibility, Detection, and Response**

GRID
Response and Industrial Defense
giac.org/grid

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Analyze ICS-specific threats and take proper courses of action to defend the industrial control systems
- Establish collection, detection, and response strategies for your ICS networks
- Use proper procedures during ICS incident response
- Examine ICS networks and identify the assets and their data flows in order to understand the network information needed to identify advanced threats
- Use active defense concepts such as threat intelligence consumption, network security monitoring, malware analysis, and incident response to safeguard the ICS
- Build your own Programmable Logic Controller using the SANS ICS515 Student Kit, which you retain after the class ends
- Gain in-depth knowledge on ICS targeted threats and malware including STUXNET, HAVEX, BLACKENERGY2, CRASHOVERRIDE, TRISIS/TRITON, and EKANS
- Leverage technical tools such as Shodan, Wireshark, Zeek, Suricata, Volatility, FTK Imager, PDF analyzers, PLC programming software, and more
- Create indicators of compromise (IOCs) in YARA
- Take advantage of models such as the Sliding Scale of Cybersecurity, the Active Cyber Defense Cycle, the Collection Management Framework, and the ICS Cyber Kill Chain to extract information from threats and use it to encourage the long-term success of ICS network security

GRID
Response and Industrial Defense
giac.org/grid

GIAC Response and Industrial Defense

The GRID certification is for professionals who want to demonstrate that they can perform Active Defense strategies specific to and appropriate for an Industrial Control System (ICS) network and systems. Candidates are required to demonstrate an understanding of the Active Defense approach, ICS-specific attacks and how these attacks inform mitigation strategies. Candidates must also show an understanding of the strategies and fundamental techniques specific to core subjects with an ICS-focus such as network security monitoring (NSM), digital forensics and incident response (DFIR).

- Active Defense Concepts and Application, Detection and Analysis in an ICS environment
- Discovery and Monitoring in an ICS environment, ICS-focused Digital Forensics, and ICS-focused Incident Response
- Malware Analysis Techniques, Threat Analysis in an ICS environment, and Threat Intelligence Fundamentals

ICS515: ICS Visibility, Detection, and Response will help you gain visibility and asset identification in your Industrial Control System (ICS)/Operational Technology (OT) networks, monitor for and detect cyber threats, deconstruct ICS cyber attacks to extract lessons learned, perform incident response, and take an intelligence-driven approach to executing a world-leading ICS cybersecurity program to ensure safe and reliable operations.

The course will empower students to understand their networked ICS environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security. This approach is important to being able to counter sophisticated threats such as those seen with malware including STUXNET, HAVEX, BLACKENERGY2, CRASHOVERRIDE, TRISIS/TRITON, and ransomware. In addition, the efforts are also critical to understanding and running a modern day complex automation environment and achieving root cause analysis for non cyber-related events that manifest over the network. Students can expect to come out of this course with core skills necessary for any ICS cybersecurity program.

The course uses a hands-on approach with numerous technical data sets from ICS ranges and equipment with emulated attacks and real world malware deployed in the ranges for a highly simulated experience detecting and responding to threats. Students will also interact with and keep a programmable logic controller (PLC), physical kit emulating electric system operations at the generation, transmission, and distribution level, and virtual machine set up as a human machine interface (HMI) and engineering workstation (EWS).

Students will spend roughly half the course performing hands on skills across more than 25 technical exercises and an all day technical capstone. Students will gain a practical and technical understanding of defining an ICS cybersecurity strategy, leveraging threat intelligence, performing network security monitoring, and performing incident response. Frameworks such as the ICS Cyber Kill Chain, Collection Management Framework, and Active Cyber Defense Cycle will be taught to give students repeatable frameworks and models to leverage post class.

The strategic and technical skills presented in this course serve as a basis for ICS organizations looking to show that ICS defense is do-able.

Author Statement

"This class was developed from my experiences in the U.S. intelligence community, at Dragos and within the control system community dealing with advanced adversaries targeting industrial control systems. It is the class I wish I would have had available to me while protecting infrastructure against these adversaries. It is exactly what you'll need to maintain secure and reliable operations in the face of determined threats. ICS515 will empower you to prove that defense is do-able."

– Robert M. Lee

"This course was like a catalyst. It not only boosted my knowledge about the threats facing ICS environments and provided me with a framework to actively defend these threats, it also inspired me to learn more."

—Srinath Kannan, **Accenture**

Section Descriptions

SECTION 1: ICS Cyber Threat Intelligence

Industrial control system (ICS) security professionals must be able to leverage internal and external threat intelligence to critically analyze threats, extract indicators of compromise (IOCs), document tactics, techniques, and procedures (TTPs), and guide security teams to find threats in the environment. In this first course section, students will learn how threat intelligence is generated, how to critically analyze reports, and the basic tenets of active defense functions. Students will become better analysts and critical thinkers by learning skills useful in day-to-day operations, regardless of their jobs and roles. This section features five hands-on labs that include building a Programmable Logic Controller (PLC), identifying information available about assets online through Shodan, completing an analysis of competing hypotheses, visualizing the attack space combining Maltego and Shodan, and ingesting threat intelligence reports to guide their practices over the rest of the labs in the course.

TOPICS: Case Study: STUXNET; Introduction to ICS Active Defense and Course Scenario; Cyber Threat Intelligence Primer; ICS Cyber Kill Chain; Threat Intelligence Consumption; ICS Threat Landscape

SECTION 2: Visibility and Asset Identification

Understanding the networked environment is the only way to fully defend it: you cannot defend what you do not know. This section starts off with leveraging the PLC to perform electric grid system operations in an attempt to understand ICS operations better and what aspect of asset identification can help operations. Students will analyze packet captures, ICS protocols, and topologies across four hands-on labs to learn what they can extract from network information to build asset inventories inclusive of equipment make and models, firmware, serial numbers, ports, protocols, and logical addressing information. The section is guided around the concept of a Collection Management Framework teaching students how to build a collection and visibility strategy tailored to their needs for both industrial operations and security operations.

TOPICS: Case Study: Bhopal Disaster; Asset Inventories and Collection Management Frameworks; ICS Network Visibility and IT Discovery Protocols; Case Study: Ransomware and Prevention Atrophy; ICS Protocols; Case Study: DRAGONFLY – HAVEX; ICS Network Architectures and Topologies

Who Should Attend

- ICS incident response team leads and members
- ICS and operations technology security personnel
- IT security professionals
- Security Operations Center team leads and analysts
- ICS red team and penetration testers
- Active defenders

SECTION 3: ICS Threat Detection

Threat detection is core to remaining resilient in the face of targeted and untargeted ICS threats. In this section students will learn about the different types of detection and build a detection strategy for their ICS/OT networks. This will begin with instruction on what threat hunting is and how to accomplish it in the ICS safely. Students will spend the day in network captures from the course's ICS range to identify the beginning of an attack on the industrial environment and follow it through to completion. Across five hands-on labs, students will learn to identify the difference between intrusions and Stage 1 of the ICS Cyber Kill Chain intrusions and then investigate a Stage 2 intrusion where the adversary is attempting to manipulate the logic of a controller.

TOPICS: Case Study: German Steelworks Attack; ICS Threat Hunting; Threat Detection Strategies; Case Study: SANDWORM – BlackEnergy 2 and BlackEnergy 3; ICS Network Security Monitoring; Event Analysis and Physical Consequence

SECTION 4: Incident Response

The ability to prepare for and perform ICS incident response is vital to the safety and reliability of control systems. ICS incident response is a core concept of ICS active defense and requires that analysts safely acquire digital evidence while scoping the environment for threats and their impact on operations. ICS incident response is a young field with many challenges, but during this section students will learn effective tactics and tools to collect and preserve forensic-quality data. Students will then use these data to perform timely forensic analysis leveraging techniques such as memory forensics. In this section's five hands-on labs, students will learn to safely acquire data, analyze initial infection vectors such as phishing emails, perform memory forensics, and analyze manipulated PLC logic.

TOPICS: Case Study: SANDWORM – Ukraine 2015; ICS Digital Forensics and Incident Response Overview; Preparing an ICS Incident Response Team; Case Study: ELECTRUM and CRASHOVERRIDE – Ukraine 2016; Initial Compromise Vectors; Forensic Data Sources in ICS

SECTION 5: Threat and Environment Manipulation

Understanding the threat is key to discovering its capabilities and its potential to affect the ICS. The information extracted from threats through processes such as malware analysis is also critical to being able to make the necessary changes to the environment to reduce the effectiveness of the threat. The information obtained is vital to an ICS active defense, which requires internal data collection to create and share threat intelligence. In this section, students will finish out the course scenario to identify the root cause of the failure in the ICS networks and craft a YARA rule on the malware for an IOC. For half of the section, students will experience a mini-capstone with another complete scenario for students to put their skills to the test in a guided scenario that is educational.

TOPICS: Case Study: XENOTIME – TRISIS; ICS Threat and Environment Manipulation Goals and Considerations; Threat Analysis and Malware Triaging; YARA; Mini-Capstone

SECTION 6: Capstone Day, Under Attack!

This section is a full day-long technical capstone where students will complete challenges that cover packet captures, logic, memory images, and more from compromised ICS ranges and equipment. This is intended to provide a fun and educational experience attempting to score the most points possible by solving technical challenges that prepare students for real world scenarios in ICS and OT.

"ICS515 integrated the OT/ICS side of security into the course well, not like other courses I've taken that taught general IT security with OT added as an afterthought."

—Josh Tanski, **Morton Salt**