

ICS515: ICS Active Defense and Incident Response



GRID
Response and
Industrial Defense
giac.org/grid

5
Day Program

30
CPEs

Laptop
Required

You Will Be Able To

- Perform ICS incident response focusing on security operations and prioritizing the safety and reliability of operations
- Determine how ICS threat intelligence is generated and how to use what is available in the community to support ICS environments. The analysis skills you learn will enable you to critically analyze and apply information from ICS threat intelligence reports on a regular basis.
- Identify ICS assets and their network topologies and how to monitor ICS hotspots for abnormalities and threats. The course will introduce and reinforce methodologies such as ICS network security monitoring and approaches to reducing the control system threat landscape
- Analyze ICS threats and extract the most important information needed to quickly scope the environment and understand the nature of the threat
- Operate through an attack and gain the information necessary to instruct teams and decision-makers on whether operations must shut down or it is safe to respond to the threat and continue operations
- Use multiple security disciplines in tandem to leverage an active defense and safeguard an ICS, all reinforced with hands-on labs and technical concepts

ICS515: ICS Active Defense and Incident Response will help you deconstruct industrial control system (ICS) cyber attacks, leverage an active defense to identify and counter threats to your ICS, and use incident response procedures to maintain the safety and reliability of 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 process of monitoring, responding to, and learning from threats internal to the network is known as active defense, which is needed to counter advanced adversaries targeting ICS, as has been seen with malware such as STUXNET, HAVEX, CRASHOVERRIDE, and TRISIS. Students can expect to come out of this course with the ability to deconstruct targeted ICS attacks and fight these adversaries and others.

The course uses a hands-on approach and real-world malware to break down cyber attacks on ICS from start to finish. Students will gain a practical and technical understanding of leveraging active defense concepts such as using threat intelligence, performing network security monitoring, and utilizing threat analysis and incident response to ensure the safety and reliability of operations. The strategic and technical skills presented in this course serve as a basis for ICS organizations looking to show that defense is do-able.

Author Statement

“This class was developed from my experiences in the U.S. intelligence community 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: 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 Section 1, 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, 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 Incident Response; Intelligence Life-Cycle and Threat Intelligence; ICS Cyber Kill Chain; Identifying and Reducing the Threat Landscape; Sharing and Consuming ICS Threat Intelligence

SECTION 3: 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 and create IOCs. In the previous section's labs, APT malware was identified in the network. In this section, the labs will focus on identifying which system is impacted and gathering a sample of the threat that can be analyzed.

TOPICS: Case Study: German Steelworks Attack; Incident Response and Digital Forensics Overview; Evidence Acquisition; Sources of Forensic Data in ICS Networks; Memory Forensics and Identifying Capabilities; Integrated Timely Analysis

SECTION 5: Active Defense and Incident Response Challenge

This section focuses on reinforcing the strategy, methodologies, skillsets, and tools introduced in the first four sections of the course. This entirely hands-on section will present students with two different scenarios. The first involves data collected from an intrusion into SANS Cyber City. The second involves data collected from a Distributed Control System (DCS) infected with malware. This section will truly challenge students to utilize their ICS active defense and incident response skills and test themselves.

TTOPICS:

Scenario One:

Identify the Assets and Map the ICS Networks; Perform ICS Network Security Monitoring to Identify the Abnormalities; Execute ICS Incident Response Procedures Into the SANS Cyber City Data Files; Analyze the Malicious Capability and Determine if the Threat Is an Insider Threat or a Targeted External Threat

Scenario Two:

Identify the Software and Information Present on the DCS; Leverage ICS Active Defense Concepts to Identify the Real-World Malware; Determine the Impact on Operations and Remediation Needs

SECTION 2: Asset Identification and Network Security Monitoring

Understanding the networked environment is the only way to fully defend it: you cannot defend what you do not know. This course section will teach students to use tools such as Wireshark, TCPdump, CyberLens, ELSA, Bro, and Snort to map their ICS network, collect data, detect threats, and analyze threats to drive incident response procedures. During this section, students will be introduced to the lab network and an advanced persistent threat (APT) that is present on it. Drawing on threat intelligence from the previous course section, students will have to discover, identify, and analyze the threat using their new active defense skills to guide incident responders to the affected Human Machine Interface (HMI).

TOPICS: Case Study: HAVEX; ICS Asset and Network Visibility; ICS Network Security Monitoring – Collection; ICS Network Security Monitoring – Detection; ICS Network Security Monitoring – Analysis

SECTION 4: 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 learn how to analyze initial attack vectors such as spearphishing emails, perform timely malware analysis techniques, analyze memory images, and create Indicators of Compromise in YARA. The previous section's labs identified the infected HMI and gathered a sample of the APT malware. In this section's labs, students will analyze the malware, extract information, and develop YARA rules to complete the active defense model introduced in the class and maintain operations.

TOPICS: Case Study: BlackEnergy2; ICS Threat and Environment Manipulation Goals and Considerations; Analyzing Acquired Evidence; Case Study: Ukraine Power Grid Attack, 2015; Malware Analysis Methodologies; Case Study: CRASHOVERRIDE; Documenting Knowledge; Case Study: TRISIS

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

“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