SANS COURSE

ICS515: ICS VISIBILITY, DETECTION, AND RESPONSE

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.

This 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.

MORE ICS CURRICULUM FROM SANS

ICS410: ICS/SCADA Security Essentials
ICS456: Essentials for NERC Critical Infrastructure Protection
ICS612: ICS Cybersecurity In-Depth

ICSPS_ICS515_0921_v1.3

ics.sans.org

poster

INTELLIGENCE-DRIVEN ICS CYBERSECURITY

Over the years, many security controls deployed in ICS/OT networks have been copy/pasted IT security controls.

It is vital to develop a tailored strategy for ICS cybersecurity. Start with the threats (intel driven) and scenarios (consequence driven) that you or others in your industry have faced.

Start with 3-5 scenarios and develop what the response plan would need to look like to meet your organization's objectives. From the response plan determine what your detection strategy should be; from your detection strategy determine what information you need to collect and integrate with your asset identification capabilities.

Working backwards from response → detection → collection will yield the best results.

ACTIVE CYBER DEFENSE CYCLE

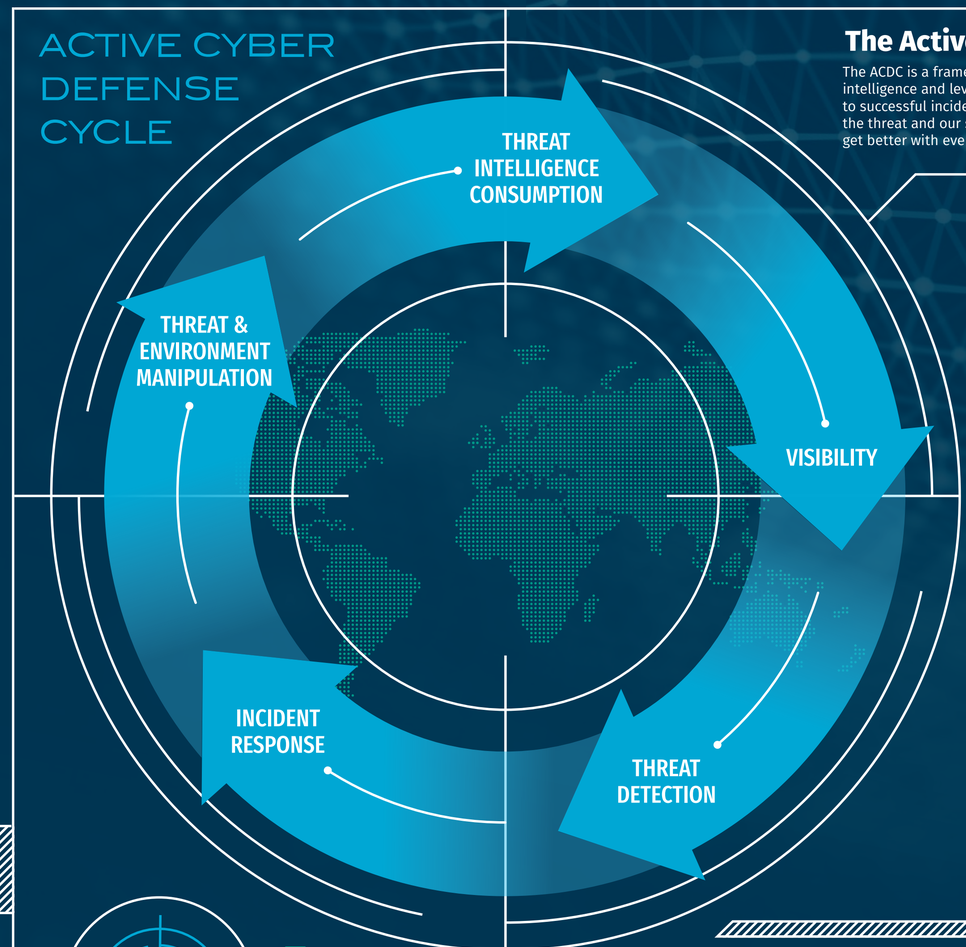

Figure. 1

The Active Cyber Defense Cycle (ACDC)

The ACDC is a framework used in SANS ICS515 to teach students how to consume intelligence and leverage it to drive monitoring efforts. This framework will lead to successful incident response engagements and an improved understanding of the threat and our systems. Consistently utilizing this framework, defenders will get better with every engagement with an adversary.

Focus on ICS threat behaviors (tactics and techniques); Indicators of Compromise (IOCs) can be valuable but should be secondary to a focus on threat behaviors which will provide more coverage and a more durable detection strategy.

ICS Activity Group Top Techniques

Activity Groups are representations of threats targeting ICS/OT environments. It is a cluster of the threat, their capabilities, infrastructure, and victimology. There are NUMEROUS teams that specifically target ICS around the world. These are MITRE ICS ATT&CK techniques (see reverse side of poster) that all defenders should be considering with preventive, detection, and response-based controls.

activity group	common technique	mitre att&ck ics designation number
ALLANITE	Point and Tag Identification for Collection	T852
CHRYSENE	Scripting for Execution	T853
COVELLITE	Spearphising Attachments for Initial Access	T865
DYMALLOY	Screen Capture for Collection	T852
ELECTRUM	Wiper to Inhibit Response Function	T809
HEXANE	User Interaction for Execution	T863
MAGNALIUM	Loss of View	T829
PARISITE	Exploitation of Remote Services	T866
RASPITE	Drive-by Compromise for Initial Access	T817
WASSONITE	Valid Accounts for Persistence	T859
XENOTIME	Safety Engineering Workstation Compromise	T818

Fig. 2

mapping example

ics cyber kill chain | mitre att&ck framework

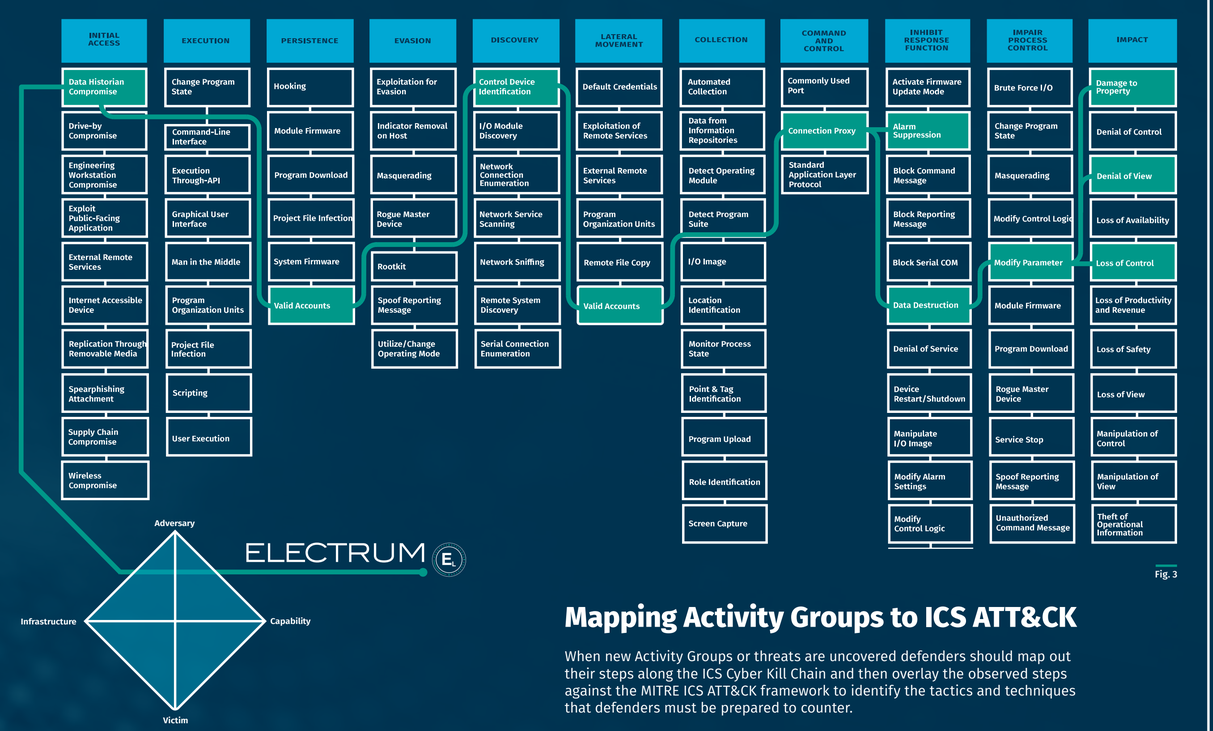

Fig. 3

Mapping Activity Groups to ICS ATT&CK

When new Activity Groups or threats are uncovered defenders should map out their steps along the ICS Cyber Kill Chain and then overlay the observed steps against the MITRE ICS ATT&CK framework to identify the tactics and techniques that defenders must be prepared to counter.

Top Four ICS Cybersecurity Controls To Counter ICS Cyber Threats

ICS-specific incident response plan

Rehearse with a Tabletop Exercise against a threat scenario in your industry and ensure you have the people, process, and technology to be successful in detecting and responding to the incident with a technical assessment post Table Top Exercise.

ICS-specific visibility and threat detection

Ensure you have key capabilities such as ICS deep packet inspection, timeline analysis, queryable and searchable logs beyond what is available with alerts, and the ability to detect ICS threat behaviors not just indicators and anomalies.

Multi-factor authentication

This will not be possible everywhere but will be doable for some of the most critical networks and plants. Always ensure to guide the communications through a chokepoint for monitoring such as a DMZ or take advantage of your existing segmentation to be able to monitor the communications in and out especially if they do not support multi-factor authentication.

Risk-based approach to patching

Observed ICS cyber threats have not typically taken advantage of specific vulnerabilities. Many identified ICS vulnerabilities provide functionality to a threat actor that can already be achieved by native features inherent to the system itself, therefore patching may not achieve the expected mitigations. Identify the vulnerabilities that give unique capabilities to adversaries such as remote access and sort vulnerabilities into a Green, Yellow, or Red category. CVSS numbers can be misleading for ICS vulnerabilities and after conducting a thorough operations risk review many ICS vulnerabilities may not need to be patched at all.

The MITRE ICS ATT&CK Framework

MITRE | ATT&CK™ FOR ICS

INITIAL ACCESS	EXECUTION	PERSISTENCE	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution Through-API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Module	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program Suite		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

SANS | ics.sans.org

SANS ICS | @SANSICS | SANS ICS

POSTER CONTENT:
Robert M. Lee
Senior Instructor, SANS Institute

ADDITIONAL CREDIT:
DRAGOS