Track 1 - Realtime Defense

This track is intended for individuals involved in day-to-day security efforts including log management and monitoring, incident response, threat hunting.

Track 2 - OT for Security Professionals

This track is intended for any security or IT professional that desires an understanding of operational technology used within the electric sector.

	Monday, Sep 23rd	
7:30 AM	**Registration**	
8am - 12pm	Instructors: Steve Parker, Andrew Zambrano, Sebastian Galvin **Threat Intelligence and Information Sharing** This session will cover the fundamentals of threat intelligence and information sharing. Students will learn how and where to obtain information on active threats, how to leverage this information to defend their systems, and how to engage in information sharing groups to both support and benefit from their broader community	Instructor: Michael Firstenberg, GICSP, CISSP, GCIH | Manager of Industrial Security | Waterfall Security Solutions **Secure Operations Technology** This course surveys industrial network security problems and introduces Secure Operations Technology (SEC-OT) – a perspective, methodology and set of best practices for designing secure industrial control systems. The world's most secure industrial sites generally deploy comprehensive IT-SEC programs as part of their OT-SEC posture. These sites also deploy a number of additional OT-centric mechanisms unique to operations networks. SEC-OT describes these additional mechanisms.
12pm - 1pm	**Lunch Provided**	
1pm - 5pm	**Threat Intelligence and Information Sharing** Course continues	**Secure Operations Technology** Course continues
5pm - 6:30pm	**Dinner Provided - Location TBA**	
7pm+	**Evening Networking Event - TBA**	

	Tuesday, Sep 24th	
8am - 12pm	Instructor: Slade Griffin **Introduction to Security Assessments** In this course, students will learn the fundamentals of technical security assessments and become familiar with several common tools utilized for such work. Students will come away with the required knowledge to begin assessing their environments for security issues.	Instructor: James McQuiggan, Siemens **Generation - Wind, Solar, DER** This session will cover the major systems and controls used in renewable and distributed energy such as wind and solar.
12pm - 1pm	**Lunch Provided**	
1pm - 5pm	**Introduction to Security Assessments** Course Continues	Instructor: Matthew Cosnek, Emerson Automation Solutions Generation - Fossil and Hydro This session will cover the major systems and controls involved in traditional generation facilities such as coal, gas, and hydro
5pm - 6:30pm	**Dinner Provided - Location TBA**	
7pm+	**Evening Networking Event - TBA**	

	Wednesday, Sep 25th	
7:45 AM		
8am - 12pm	Instructors: Slade Griffin, EnergySec Staff **Incident Detection and Threat Hunting** This session will build on lessons learned in Monday and Tuesday's courses. Students will learn techniques to detect and investigate potentially malicious activity using the open source RockNSM platform.	Instructor: TBA **Distribution Systems and Smart Grids** This session will cover technologies used in electric distribution and grid modernization. This includes distribution automation, advanced metering, demand response, and similar technologies
12pm - 1pm	**Lunch Provided**	
1pm - 5pm	**Incident Detection and Threat Hunting** Course continues	Instructor: Jim Terpenning | Archer **Substation Technology** This session will expore technology used in substation environments, how it can be attacked, and what defensive measures are needed. This includes protection systems, transformers and breakers, Reactive resources, switching, Special Protection Systems, PMUs, DFRs, and similar.
5pm - 6:30pm	**Dinner Provided - Location TBA**	
7pm+	**Evening Networking Event - TBA**	

	Thursday, Sep 26th	
8am - Noon	Facilitators: Slade Griffin, EnergySec Staff **Incident Response Exercise** This full-day table top exercise will introduce students to incident response fundamentals and develop skills to successfully address cyber incidents. A variety of incident scenarios will be presented as response exercises.	Instructor: Jim Terpenning | Archer **Control Center Operations** This session will cover technology used in Control Center environments, how it can be attacked, and what defensive measures are needed. This includes EMS, SCADA control, inter-Control Center communications, scheduling, market systems, state estimation, black start, and more
12pm - 1pm	**Lunch Provided**	
1pm - 5pm	**Incident Response Exercise** Exercise Continues	Instructor: Utility Staff - TBA **Telecommunications Technology** This session will cover communication technology used in the Electric sector. Includes traditional POTS lines, frame relay, MPLS, SONET, microwave, cellular (commercial and private), power line carrier. Discussion of various types of equipment and manufacturers
5pm - 6:30pm	**Dinner Provided - Location TBA**	
7pm+	**Evening Networking Event - TBA**	

	Friday, September 27	
8am - Noon	Facilitators: Slade Griffin, EnergySec Staff **After Action Review** We will review the exercsie results from the previous day, discuss lessons learned and takeaways from the event.	Instructor: Utility Staff - TBA **Communication Protocols** Students will learn details of various communication protocols in use in operational environments, such as DNP3, Modbus, 62443, ICCP, serial protocols, and others.
12pm -1pm	**Lunch Provided**	