CYBER EMERGENCY RESPONSE

HOW THE CyberCENTS® TRNEX TEAM SUPPORTS SAN FRANCISCO'S CYBER EMERGENCY RESPONSE EFFORTS

BRAD WOLFENDEN
Sr. Cyber Business Analyst

For three days in early November 2021, members of the CyberCENTS® Training and Exercise (TRNEX) team hosted the first of six cohorts of a Cyber Emergency Response course designed and delivered by By Light for the City and County of San Francisco (CCSF). This course, originally bid in March 2021 and awarded to By Light in May 2021, brings together cybersecurity, business continuity, and emergency management professionals from various agencies and departments within CCSF to provide the cross-functional teams with an in-depth training on Cyber Emergency Response.

Upon award, the CyberCENTS TRNEX team worked alongside CCSF leadership to author the course. The foundations of the content come from globally recognized standards in cyber incident handling (i.e., NIST SP 800-61r2); however, California- and CCSF-specific legislation, policies, procedures, and tactics were incorporated into each module. For example, ESF-18, Unified Cyber Command, the formal emergency response plan for CCSF was a central document used throughout the instruction. In addition to the 10 teaching modules, the course consisted of four activities, a mini exercise/tabletop, knowledge checks throughout, and a final exam.

Two of the four activities as well as the mini exercise used SLAM-R®, By Light's cyber range product (SLAM-R: Sentinel, Legion, AutoBuild, Myrmidon, Reconstitution).

Participants in the course that attend all three days of the Cyber Emergency Response course, complete all assignments and activities, and score a 70% or higher on the final exam received a digital badge issued by By Light via the online digital badging platform, Badgr. The CyberCENTS TRNEX Team has plans to repurpose much of this content in the design of a Cyber Resiliency course that will become part of its overall Course Catalog that is made available to SLAM-R customers and partners.

Cyber Emergency Response course digital badge

The remaining five cohorts of the Cyber Emergency Response course will run from January – October 2022, and a total of 150 participants have already self-enrolled for the course. Course participants represent agencies and departments across the CCSF such as: Public Utilities Commission, Human Services Agency, Dept. of Building Inspection, City Attorney's Office, Elections Commission, Sherriff's Office, Office of Housing and Community Development, Airport Commission, Port Authority, Dept. of Human Resources, Dept. of Public Health, and more. ■

DAY 1 - CYBER EMERGENCY RESPONSE	DAY 2 - CYBER INCIDENT HANDLING METHODS & STRATEGY	DAY 3 - EMERGENCY RESPONSE & INCIDENT HANDLING APPLICATION
INTRODUCTIONS & CYBERCENTS OVERVIEW	DAY 1 REFRESH & LAB BRIEF	DAY 2 REFRESH
Module 1: (60 mins.) Cybersecurity Awareness	**Module 5: (45 mins.) ICS Structure & Integrating Cyber Ops in ICS**	**Activity 4: (60 mins.) After Action Review**
Activity 1: (30 mins.) CATI Aptitude Assessment	**Module 6: (45 mins.) ESF-18, Unified Cyber Command**	**Turn 1 - Scenario Begins**
Module 2: (90 mins.) Business Continuity & Disaster Recovery	**Module 7: (60 mins.) Cyber Incident Response: Preparation**	
LUNCH	LUNCH	LUNCH
Activity 2: (60 mins.) • **EMP: Business Impact Analysis** • **CP: Performing Network Discovery Using Tools**	**Module 8: (45 mins.) Cyber Incident Response: Detection & Analysis** **Module 9: (45 mins.) Cyber Incident Response: Containment & Eradication**	**Exercise Review & Status** **Turn 2 - Scenario Continues**
BREAK	BREAK	
Module 3: (60 mins.) Foundation of Cyber Incident Management	**Activity 3: (60 mins.)** • **EMP: Cyber Response "Crawl" / Walk-Through** • **CP: Managing Devices, Detection Tools, Protocols**	**Post-Incident Review**
Module 4: (60 mins.) Cyber Incident Handling		
DAY 1 RECAP	DAY 2 RECAP	COURSE RECAP & SURVEY

Example: Cyber Emergency Response course schedule

Originally published in By Light Synergy, Vol. 3, December 2021