Industrial Cybersecurity by LOGITEK

Propuesta temario curso formación

Ciberseguridad en sistemas ICS (Industrial Control Systems), redes OT e IoT

David Soler
Cybersecurity Solutions Manager

Barcelona, 18/10/2019

INDICE DE CONTENIDOS

1. Introducción

Nuestros clientes nos han comunicado su voluntad de ampliar sus conocimientos en las tecnologías y sistemas específicos que convergen en los entornos industriales y de infraestructuras críticas y en cómo la ciberseguridad les afecta.

Por ello ICLK, la unidad de Consultoría e Ingeniería de Ciberseguridad Industrial de Logitek, les propone la realización de una serie de jornadas de formación que les permitirán:

- Tener una visión clara acerca de los conceptos más importantes asociados a los entornos operacionales e IoT.
- Entender las diferencias entre la idiosincrasia de los entornos IT y OT y los diferentes equipos y sistemas de cada uno de ellos.
- Entender las principales diferencias existentes entre las políticas de seguridad que se llevan a cabo en entornos IT y en entornos OT.
- Analizar las principales vulnerabilidades y amenazas que se pueden sufrir en entornos industriales e infraestructuras críticas.
- Conocer los diferentes tipos de ataques que pueden realizarse a una red OT o una infraestructura crítica.
- Describir las principales contramedidas que pueden incluirse para fortificar las redes y protocolos industriales.
- Esbozar las principales normas y estándares relacionados con este entorno que intentan facilitar el despliegue de políticas de seguridad efectivas.
- Facilitar recomendaciones y consejos prácticos que permitan fortificar los sistemas y redes vinculados al ámbito industrial de las organizaciones.

2. Alcance

A convenir:

- Días de formación.
- Horario.
- Lugar de impartición.
- Iteraciones.
- Número de alumnos.

.

3. Contenidos propuestos

A continuación, se realiza una propuesta de contenidos para consensuar con los responsables de las empresas y organizaciones interesadas. Cada bloque se imparte en un tiempo aproximado de 2 horas.

Bloque I. Informática industrial y ciberseguridad industrial.

- Conceptos básicos asociados a la industria e infraestructuras críticas: separación de sistemas por niveles dentro de la pirámide de automatización, aplicación e interconexión de los distintos niveles.
- Conceptos básicos asociados a la informática industrial.
- Tipos de sistemas industriales, y su rol dentro del proceso productivo.
- Indicadores o KPIs clave en los procesos productivos. Para qué se utilizan y por qué son importantes.
- Principales diferencias entre ciberseguridad IT vs ciberseguridad OT.

Bloque II. Comunicaciones industriales y protocolos industriales seguros.

- Modbus-TCP.
- Ethernet/IP.
- Siemens TCP/IP Ethernet.
- Profinet.
- DNP3. Seguridad en DNP3.
- OPC-DA y OPC-UA. Seguridad en OPC UA.

Bloque III. Prácticas de comunicación con sistemas industriales.

- Práctica con servidor OPC y PLCs Siemens.
- Práctica de comunicación entre cliente OPC-UA y servidor OPC-UA.
- Práctica con comunicación DNP3 y RTUs.

Bloque IV. Ataques y vulnerabilidades del entorno OT e infraestructuras críticas.

- Consecuencias típicas de los ataques en entornos OT (escalado de privilegios, DoS y DDoS, backdoor access, robos y modificaciones de datos).
- Recorrido por los principales ataques ocurridos en entornos OT (Stuxnet, Duqu, Flame, Shamoon, Dragonfly, Laziok, entre otros).
- Estudio sobre los vectores de ataque utilizados durante el 2018 y vulnerabilidades publicadas.

Bloque V. Vulnerabilidades típicas de los entornos de operación.

- BBDD de vulnerabilidades OT.
- Técnicas y herramientas de identificación de vulnerabilidades en entornos OT.

Bloque VI. Prácticas de ataques a sistemas industriales.

- Utilización de maqueta con equipamiento industrial.

Bloque VII. Contramedidas específicas para fortificar los entornos industriales. Redes.

- Topología de redes en entornos industriales.
- Mejores Prácticas para la segmentación y fortificación de redes industriales.
- Medios y protocolos para la redundancia de redes: RSTP, MRP y VRRP.

Bloque VIII. Contramedidas específicas para fortificar los entornos industriales. Tecnologías y mejores prácticas.

- Mejores prácticas para los accesos remotos.
- Firewalls DPI. Concepto y aplicación.
- Segmentación mediante whitelisting de protocolos.
- Sistemas IPS e IDS industriales.
- Segmentación mediante diodo de datos.
- Monitorización de las redes.
- Sistemas de control de cambios para entornos OT.

Bloque IX. Práctica. Configuración de firewalls DPI para fortificación de comunicación ModbusTCP.

- Pruebas con comunicación entre SCADA y RTU.
- Configuración de dobles factores de autenticación en túneles VPN.
- Exposición de caso práctico de despliegue de IDS industrial.

Bloque X. La ISA/IEC 62443 para proteger los sistemas de control.

- Autoevaluación de los sistemas de control, mitos comunes en la seguridad de los IACS.
- Reglamentos, normas y estándares.
- ISA/IEC 62443: Terminología, conceptos, modelos y métricas
    - Objetivos de Seguridad.
    - Defensa en profundidad.
    - Evaluación de Riesgos.
    - Políticas.
    - Zonas y Conductos.
    - Niveles de Seguridad.
    - Modelos de Ciclo de Vida de Seguridad.