Risk Centric Threat Models for IoT Medical Devices

Course	**Risk Centric Threat Models for IoT Medical Devices**
Instructor	Tony UV
Short Description	This course begins by focusing on the overall importance of threat modeling in product/ application development and then quickly dives into helping students deconstruct product/ application components into use cases, abuse cases, call/data flows, trust boundaries, attack vectors and most importantly countermeasures.
Abstract	Risk Centric Threat Models is a threat modeling course abiding by the Process for Attack Simulation & Threat Analysis methodology. The course is provided over two days and begins with a very quick overview of threat modeling concepts, common inputs to the process, integration activities to secure SDLC workflows and extends into applying the 7 stages of the PASTA methodology to target IoT applications in the healthcare medical field. Risk centric threat modeling is an approach that focuses on correlating threat viability and business impact. Many other threat modeling approaches do not consider impact of threat scenarios beyond subjective analysis. For HCA (Healthcare Applications) (as an example), impact goes well beyond patient data privacy and includes impact of loss of life, particularly in the proliferation of IoT based medical devices where wearables have gone to become implantables. Regardless of the student's industry expertise, they will learn how to leverage threat modeling for any type of IoT application. We'll explore IoT protocols that support many IoT applications (e.g. – ZigBee, MQTT, CoAP) as well as common web related components that interface with client hardware devices. Beyond the basics of DFDs, attack tree build outs, kill chains, we'll address how to leverage tools to identify an application's attack surface (both client side and web), identify work processes, actors (callers) privileges, techniques for threat intel filtering and correlation, and recommendations for identifying weaknesses and attacks that are both present and related to the threat motives of the constructed model. The course is broken up into 7 parts -for each stage of the PASTA process. Details for each day is presented below:

Course Schedule – Day 1

Duration	Subject	Practice Problems
1 hour	TM Overview	Security, asset, risk centric approaches
45 min	Lab	RestFul API Threat Modeling Exercise using MS Tool
1.5 hours	Phase I – Defining Impact	Correlating use cases to SLAs, KRIs, BIAs
1.5 hours	Phase II – Attack Surface	Identify attack surface of client side IoT components
45 min	Lab	Tools to enum client side/ web components
1.5 hours	Phase III – App Decomposition	DFD exercises, call flows, data flows

***Note*:** *segments below are 2 hour intervals; doesn't reflect breaks, lunch*

Course Schedule – Day 2

Duration	Subject	Practice Problems
45 min	Lab	Data Flow Diagramming w/ jamboards
1.5 hours	Phase IV – Threat Analysis	Substantiating threat models w/ threat intel
45 min	Lab	Attack Tree build outs using ConceptDraw, Visio
1.5 hours	Phase V – Vuln Enumeration	Vuln Analysis and Vuln Correlation
45 min	Lab	Correlating CVEs to Attack Tree Nodes for IoT Client components
1.5 hours	Phase VI – Attack Modeling	Attack modeling restful webservices for IoT devices
45 min	Lab	Mapping & launching attack patterns using Burp/ Zed
1.5 hours	Phase VII – Countermeasure Development	Finalizing attack tree; Building countermeasure nodes to the threat model; residual risk analysis