Course: Building Cyber Threat Intelligence Capabilities for Organizations
Code: CTI100
URL: https://vidalintelligenceandconsulting.com/BuildingCTI

Pre-Requisites(s):

- Previous experience in Information Security or Cyber-Security would be considered an asset but it is not a requirement or pre-requisite.

Course Description:

This course is designed to enable organizations of any size to plan, build and operationalize a tailored Cyber-Threat Intelligence program based on their specific needs, requirements, and budget. Through identifying critical assets, technology and business processes, students will be able to detect cyber threats targeting your organizations crown-jewels and implement controls and detection capabilities to be able to proactively respond to these threats. Cyber Threat Intelligence programs do not need to be expensive or complex as long as they are designed to fit organizational intelligence objectives.

Course Outcomes:

Success completion of this course will enable students to:

1. Know and understand the basic concepts behind building a Cyber Threat Intelligence Team and its operations.
2. Discuss the key concepts behind Cyber-Threat Intelligence, including its benefits and capabilities and how these can be used to complement an organizations existing security monitoring and operations.
3. Understand how Cyber Threat Intelligence can complement and interact with other business units.
4. Scope the implementation of Cyber Threat Intelligence activities based on organizational priorities, requirements and existing resources and capabilities.
5. Proactively identify emerging cyber threats and provide mitigation controls and recommendations.
6. Provide operational support to security investigations, Incident Response, and vulnerability management teams.
7. Produce operational metrics to gauge the effectiveness of the Threat Intelligence Program aids your organization in reducing risk.
8. Create Intelligence Requirements (IRs) and supporting processes and procedures to support the day-to-day operations of your Cyber-Threat Intelligence program.
9. Understand key tools and technologies that can be used to automate and otherwise support the operations of the Cyber Threat Intelligence program.

10. Produce actionable intelligence products that can be easily consumable by various teams, stakeholders and tools.
11. Identify and implement appropriate Courses-of-Action based on identified threats that have been identified and also have the potential to impact an organization.

Unit Outcomes:

Successful completion of the following units will enable the student to:

1. **Introduction**
    a) Understand the key concepts behind Cyber Threat Intelligence, its benefits and capabilities, and how these can be used to compliment an organizations' existing security operations.
    b) Compare and contrast different types of adversaries (and their objectives) that have the potential to target your organization.
    c) Discuss the success factors related to an effective Cyber Threat Intelligence Program.
    d) Understand basic concepts and terminology associated to Cyber Threat Intelligence including but not limited to ThreatCon, Cyber Threat Kill Chain, Traffic Light Protocol (TLP), and the Intelligence Life Cycle.

2. **Discovery**
    - Identify assets and other keywords within an organization or industry.
    - Understand the business context of assets and resources that support critical functions in order to enable organizations to prioritize efforts consistent with internal risk management strategy and business requirements.
    - Identify stakeholders and internal teams that can benefit from Cyber Threat Intelligence operations.
    - Discover data sources within the organization that can assist in Cyber-Threat detection and/or data enrichment capabilities.

3. **Risk Assessment and Threat Modelling**
    - Identify threats that have the ability to impact the organizational assets identified within the Discovery phase.
    - Arrange and model high-level threats to identify similar assets at risk impact if compromised.
    - Generate data-driven metrics to support the business need and requirements for a CTI Program.
    - Categorize risks and threats to support the development of the Intelligence Requirements in the next unit.

4. **Intelligence Requirements**
    a) Definition
        - Determine threats that you have the ability to monitor and action.

- Structure and model high-level threats to identify similar assets at risk impact if compromised.
- Construct scenarios and situations where identified threats have the ability to be realized within an organization.
- Categorize identified threats in order to establish Intelligence requirements (IRs).

b) Collection Plans
- Establish the collection requirements and objectives for each General Intelligence Requirement.
- Evaluate intelligence sources to be used as part of your collection plans.
- Identify collection plan dependencies and their estimated costs.
- Understand the value of various intelligence sources and how they can support your Cyber Security operations.

c) Courses of Action, Service Catalogue, Communicate Plans and SLAs
- Determine what Courses-of-Action (COAs) that the CTI Team has the ability to perform.
- Classify COAs in order to be able to measure the strength and maturity of your capabilities in defending against emerging cyber threats.
- Establish communication plans for each product or service that is offered, and determine who should receive these, as well as how (i.e. email, pdf report.
- Implement Service Level Agreements (SLAs) for each product or service the CTI team provides.
- Construct a Service Catalogue of service offerings provided by the CTI Team.

5. **Intelligence Tools**
- Determine appropriate tools that can be used to support the operations of the Cyber-Threat Intelligence Team.
- Estimate cost requirements for hardware, software and other dependencies associated to various tools and intelligence requirements.
- Understand the basic concepts of Operational Security (OPSEC) and how your actions my provide forewarning to a threat actor.
- Discuss the benefits and capabilities of commonly used Threat Intelligence Platforms (TIPs).
- Compare and contrast the benefits and disadvantages of using online resources and services.

6. **Reporting and Metrics**
- Establish reporting cadence and requirements for executive and stakeholders reporting.
- Formulate meaningful operational metrics to be included in various reporting products.
- Prepare reporting templates and layouts based on reporting requirements and audience.

- Construct methods to easily acquire and generate updated data and metrics.

7. **Executive and Stakeholder Buy-in**
    - Develop executive and stakeholder presentations regarding the Intelligence Requirements and CTI operations that have been established in order to obtain support and buy-in.
    - Justify identified cyber-threats and their associated Intelligence Requirement proposals on how identify and defend against these.
    - Appraise, tailor and update Intelligence Requirements based on executive and stakeholder feedback.

Suggested Student Resources:

- Office suite of products such as Microsoft Word, Excel and PowerPoint.

Prepared By: Vidal Intelligence and Consulting
https://vidalintelligenceandconsulting.com

Date: September 13th, 2022