VAILLANCE
GROUP

2022 Course List

Please note:

All courses are custom made for each client, taking into account their industry, specific vulnerabilities, threats, and culture within their organization. If you don’t see a specific focus area you need covered, please contact us.

1. Introduction to Insider Threat

This course dives into what an Insider Threat is, what it means to your company, and why you should care. Focused on definitions, present day statistics to demonstrate the urgency, and detailed explanations on the various ways someone becomes an Insider Threat, this course touches on The Critical Pathway, Unintentional, Malicious, and Best Practices you can start today!

2. Insider Threat - Espionage

Stories of spies stealing corporate secrets are not just for the movies! Today espionage is a very real fact of doing business and this course explains how both competitors and nation states target your company and people. Real world examples are given by a former Case Officer on how potential assets were targeted, and how you can recognize those threats.

3. Insider Threat - Insider Fraud

Insider fraud is the largest threat to a given organization. Not only can fraud have massive financial impacts, but insider fraud can also lead to the compromise of Personally Identifiable Information (PII) or substantial personal information, bad publicity, and government reporting requirements. In cases like this, blowback can be swift and severe. Here we learn about various types of Insider fraud, and key things to look for to prevent it.

4. Insider Threat - IT Sabotage

The threat of IT sabotage is a nightmare scenario, oftentimes conducted by an insider who was moving along The Critical Pathway. Examples of real cases are addressed, as well as ways organizations could have better responded to the threat. Here, we explain the need to understand and implement Defense in Depth in order to avoid threats of IT sabotage.

5. Insider Threat - Unintentional Insider Threat

Every organization is made up of people – mostly loyal, hard working people with no mal intent, but what happens when your employees don't recognize threats and unintentionally leave your organization vulnerable to attack or theft of intellectual property? This course shows you ways employees leave companies vulnerable and how to mitigate those risks.

6. Insider Threat - Malicious Acts

Perhaps the most frightening of intentional acts is the malicious insider. Whether they are stealing corporate trade secrets to start their own company, selling them to a nation-state for profit, or intentionally trying to harm your business, these are the Insider Threat risks that must be identified early.

7. Insider Threat - Theft of Intellectual Property

Many businesses don't understand the Crown Jewels they hold, where they are located, what they are worth, and how best to protect them. The threat by competitors and, specifically nation-states, is very real and this course shows you how to understand what you have and how best to protect it.

8. Insider Threat - The Critical Pathway

The Critical Pathway, as identified by Eric Shaw, explains how personal predispositions, stressors, and concerning behaviors can lead up to Insider Threat-like behaviors and/or malicious acts. This course provides details into each of those factors and addresses what companies can do when faced with related situations.

9. Insider Threat - Travel

If you ever travel for work such as to attend conferences or business meetings, your cyber hygiene and physical security awareness leave you and your organization vulnerable. In this course, you will learn how to travel smarter, recognizing where you can improve your operational security and reduce risk.

10. Insider Threat - Work from Home

Employees today have been thrust into a sudden, drastically different working environment than they are used to. While wearing pajama bottoms all day is a perk, companies need to understand the added risks their employees bring while working from home. This course provides useful factors to consider to improve cyber security of WFH employees.

11. Insider Threat - Program Development (this has a 4 hour live class)

As you progress through this training you may be wondering what you as an organization can do to build your own Insider Threat Program. This course gives you a basic understanding of factors to consider and steps to take.

12. Insider Threat - Technical Controls

All organizations should have a strong understanding how physical and technical controls can limit the threats that insiders pose. There are general industry standards that will help add layers of security to your day-to-day operations.

13. Insider Threat - Mitigation and Best Practices

This course is where you can find best practices related to Insider Threat. We provide consistent, relevant, and detailed examples of ways to improve everything from cyber hygiene to personal security practices. Processes for when and how to report and action concerns of a potential Insider Threat are addressed.

14. Insider Threat - Contractors and Trusted Business Partners

An insider risk program is not complete unless an organization looks beyond their own staff to understand the associated personnel - including contractors and trusted business partners - that have access to the company assets. This training walks through considerations for onboarding, managing and offboarding these individuals in a way that maintains the integrity of the insider risk program.

15. Managing Staff during COVID-19

COVID-19 brings with it the necessity to focus on management skills which support the transformation of a workforce that is separated not just by physical proximity, but often time zones and technical resources. Making sure your organization's team members are engaged, feel connected and effective in their roles, and understanding the indicators of compromise that lead to sabotage, theft of IP or espionage, is the focus of this training.

16. Corporate Espionage

In this course you will learn the difference between industrial espionage, corporate espionage, and competitive intelligence. Methods of corporate espionage, the legal landscape, and the xx between organized crime, insider threat, cyber security, foreign intelligence, and intellectual property are all discussed.

17. Employee Lifecycle Management to Address Insider Threat

An employee's lifecycle encompasses several stages throughout their career. This begins with recruitment and concludes with resignation, retirement, or termination. This course addresses how organizations can establish a lifecycle program in order to give employees consistency throughout their careers and teaches you how to prevent insider threats as a result. It also provides a framework to understand important interdependencies, touchpoints, interactions, and gaps in insider protection strategies.

About Us:

Vaillance Group leverages our extensive knowledge of Insider Threat behavior to protect clients' assets, people, and confidential information from the vulnerabilities that come from both malicious and unintentional threats.

We are a licensed partner with Carnegie Mellon's Software Engineering Institute (SEI) to conduct vulnerability assessments utilizing the Cyber Emergency Response Team (CERT) Insider Threat Vulnerability Assessment tool. We additionally conduct SEI-Authorized Insider Threat training. Vaillance Group is a leader in the insider threat space, with specialized experience in both the public and private sectors, as well as the investigative space related to complex insider threat cases.

To schedule your course, contact:
Shawnee Delaney | CEO, Vaillance Group
shawnee@vaillancegroup.com
www.vaillancegroup.com