SANS The most trusted source for cybersecurity training, certifications, degrees, and research

GIAC CERTIFICATIONS

SEC547: **Defending Product Supply Chains**

3 Day Course	18 CPEs	Laptop Required

You Will Be Able To

- Create SBOMs from source code
- Create attestation pipelines
- Understand how vulnerabilities are published
- Learn to validate vulnerable components
- Identify counterfeit components
- Build a supply chain security program
- Understand how foreign adversaries manipulate supply chains
- Learn to use open-source supply chain security tools
- Work with developers to inject security into your product development process
- Become more effective at responding to supply chain threats
- Learn effective techniques to respond to the next major supply chain vulnerability

Business Takeaways

- Increase your organization's resilience in the face of adversarial threats
- Decrease the cost of your security program through risk reduction
- Conduct vendor and product supply chain assessments
- Reduce the impact of supply chain attacks on your organization
- Prioritize risks inside your supply chain program
- Identify leakage of sensitive intellectual property
- Identify foreign presence risks in your supply chain
- Coordinate supply chain security conversations with stakeholders

SEC547 covers the broad topic of supply chain risk management and expands on traditional definitions of vendor risk management to include more modern concepts such as software transparency and assurance. Tackling not only the why of supply chain security, but how as well. Through a series of case studies and real-world threat scenarios, the course provides effective guidance that transcends conventional wisdom to land at ground truths necessary to build and mature a supply chain program.

The landscape of supply chain security is fraught with peril, not only with the adversaries we seek to disrupt, but also the internal and external stakeholders that complicate this process. Through a blend of both traditional risk management disciplines interwoven with technical concepts required to defend against nation state level and criminal organizations, SEC547 will give you confidence in keeping your organization safe. Exploration of concepts such as procurement and contracting, risk assessments, software bill of materials (SBOMs), counterfeit and other hardware threats, and coordinated vulnerability remediation and response provide the context needed to secure your organization.

SEC547 is constructed around a fictional industrial manufacturing company as an illustrative showcase of the challenges faced by both buyers and sellers of technology. As we walk through course objectives, aspiring supply chain professionals will be able to identify with and apply the lessons learned to tackle these critical concerns.

What Is Supply Chain Security?

The practice of supply chain security is focused on securing the upstream dependencies we ingest into the products and services we rely upon to run our business. The scope of these activities can be broad and impact the people, processes, and technology we rely on to run the business. Likewise, our people, processes, and technology are the supply chain for other downstream organizations, and as such, both upstream and downstream concerns become part of the global supply chain concern. This connected ecosystem creates a rapidly expanding spider web of risks that function as a force multiplier for adversaries seeking to maximize the returns on their offensive investments.

Hands-On Supply Chain Security Training

SEC547's hands-on labs comprise of 11 immersive labs across three days and explores the concepts taught through instructor presentation. Using a custom Linux lab environment purposely built for this course, you will leverage industry supply chain tools such as Dependency Track, CycloneDX, in-toto, CSAF VEX standard, and even utilities such as gitgeo to interrogate GitHub for noteworthy observations about open-source projects. As working with supply chain artifacts is a big part of this work, we will also cover advanced command line introspection of these file formats such as processing and parsing of JSON files and learning to optimize testing workflows. Additional tools covered in the labs include sha1sum, openssl, sigstore, and a variety of open-source intelligence tools such as nmap, subfinder, and more, useful for information collection and assessment activities.

Section Descriptions

SECTION 1: Vendors and Products

Starting with an introduction to supply chain concepts, we explore how supply chains function and why they are such an attractive target. We will discuss corporate processes and the way people procure products and how these dynamics between buyer and seller influence supply chain risks. Going deeper into threat models for these attack vectors, we cover how to perform risk assessments that are contextual to the risk you are trying to manage. This section discusses the role that suppliers play in the product manufacturing process and how you can build and mature a supply chain risk management program.

TOPICS: An Introduction to Supply Chain; Risk Assessment Process; OSINT Analysis; Program Execution; Contracting and Foreign Ownership, Control, or Influence (FOCI); Product Development

SECTION 2: HBOM and SBOM

Diving deep into hardware threats, this section covers how to assess hardware risks and identify counterfeit hardware in your intake process. Hardware bill of materials (HBOMs) as a historical manufacturing technique have evolved, and we will show you how you can evolve your understanding for holistic product evaluation. Software authenticity and trust attributes such as provenance and pedigree and understanding how to prioritize the ocean of products to be assessed will all be covered in this section. The latter part of this section is focused solely on a variety of SBOM topics from exploring use cases to creating SBOMs yourself from existing open-source projects. Lastly, we explore how the SBOM space is evolving to include Software as a Service (SaaS), configuration management, and other bill of materials types.

TOPICS: Hardware Threats; Counterfeits; Building a Hardware Lab; Software Threats; Trust Attributes; Supply Chain Regulations; SBOM Basics; SBOM Challenges; CycloneDX SBOM; Software Package Data Exchange (SPDX) SBOM; Other BOM Types

SECTION 3: Software Transparency and Response

This final section starts with a focus on attestations and related tools and frameworks such as in-to, SLSA, and other models to measure the processes in your supply chains and CI/CD pipelines. By establishing verifiable evidence, we start to gain more trust in the software we use. We will dive deep into vulnerability management, one of the most important use cases for supply chain. Lastly, we will explore topics related to product security incident response teams (PSIRT) and the role they play in responding to supply chain incidents as well as a few notable attacks and how to disrupt them.

Section 3 concludes with a vulnerability incident simulation that pulls together many of the concepts covered in this course to provide context on all the material over this three-day course.

TOPICS: Supply Chain Attestations; Vulnerability Management; Vulnerability Exploitability eXchange (VEX) and Vulnerability Disclosure Report (VDR); Responding to Threats; PSIRT

Author Statement

With high-profile incidents such as Solarwinds and Log4j dominating news cycles and urgent action called for from the federal government and industry at large, supply chain risk management is one of the most charged topics in security today. It's a vast topic covering many domains of knowledge and is challenging for many to understand where to even start. The guidance from industry is deafening but hard to navigate. Do we need security questionnaires? Vendor scorecards? SBOMs? Firmware analysis? AppSec tools? Something else?

There are many fantastic solutions out there, but the reality is they are not all well-suited for where you are in your security journey, nor do the terms mean the same thing to everyone. The guidance from industry analysts is also dated and unhelpful. This can be very confusing! I drew on a career of over 25 years, supporting supply chain use cases in electronics manufacturing, vendor risk and software supply chain for critical infrastructure in writing this course to help navigate through the noise and provide real-world examples of what works and what doesn't. Join me as we chart a path forward to defending product supply chains!

—Tony Turner, SANS Instructor

Who Should Attend

- Supply chain risk management professionals
- Product security and PSIRT teams
- Asset owners and operators responsible for security
- Security analysts and incident responders
- Security leaders responsible for product security