SEC530: Defensible Security Architecture and Engineering

GDSA
Defensible Security Architecture
giac.org/gdsa

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Analyze a security architecture for deficiencies
- Apply the principles learned in the course to design a defensible security architecture
- Determine appropriate security monitoring needs for organizations of all sizes
- Maximize existing investment in security architecture by reconfiguring existing assets
- Determine capabilities required to support continuous monitoring of key Critical Security Controls
- Configure appropriate logging and monitoring to support a Security Operations Center and continuous monitoring program

Who Should Attend

- Security architects
- Network engineers
- Network architects
- Security analysts
- Senior security engineers
- System administrators
- Technical security managers
- CND analysts
- Security monitoring specialists
- Cyber threat investigators

SEC530: Defensible Security Architecture and Engineering is designed to help students build and maintain a truly defensible security architecture. "The perimeter is dead" is a favorite saying in this age of mobile, cloud, and the Internet of Things, and we are indeed living in new a world of "de-perimeterization" where the old boundaries of "inside" and "outside" or "trusted" and "untrusted" no longer apply.

This changing landscape requires a change in mindset, as well as a repurposing of many devices. Where does it leave our classic perimeter devices such as firewalls? What are the ramifications of the "encrypt everything" mindset for devices such as Network Intrusion Detection Systems?

In this course, students will learn the fundamentals of up-to-date defensible security architecture. There will be a heavy focus on leveraging current infrastructure (and investment), including switches, routers, and firewalls. Students will learn how to reconfigure these devices to better address the threat landscape they face today. The course will also suggest newer technologies to aid in building a robust security infrastructure.

While this is not a monitoring course, it will dovetail nicely with continuous security monitoring, ensuring that security architecture not only supports prevention, but also provides the critical logs that can be fed into a Security Information and Event Management (SIEM) system in a Security Operations Center.

Hands-on labs will reinforce key points in the course and provide actionable skills that students will be able to leverage as soon as they return to work.

"As a systems programmer working on the development of security tools, the architectural content provided has been highly informative and extremely valuable."

— Merv Hammer, **Workday Inc.**

"SEC530 provided an excellent understanding of application attacks and how to protect against them."

— Shayne Douglass, **AMEWAS Inc.**

Available Training Formats

Live Training

Live Events
sans.org/information-security-training/by-location/all

Summit Events
sans.org/cyber-security-summit

Private Training
sans.org/private-training

Online Training

OnDemand
sans.org/ondemand

Simulcast
sans.org/simulcast

Section Descriptions

SECTION 1: Defensible Security Architecture and Engineering

Section 1 of the course describes hardening systems and networks at every layer, from layer one (physical) to layer seven (applications and data). To quote Richard Bejtlich's The Tao of Network Security Monitoring, defensible networks "encourage, rather than frustrate, digital self-defense." The section begins with an overview of traditional network and security architectures and their common weaknesses. The defensible security mindset is "build it once, build it right." All networks must perform their operational functions effectively, and security can be complementary to this goal. It is much more efficient to bake security in at the outset than to retrofit it later. The discussion will then turn to layer one (physical) and layer two (data link) best practices, including many "ripped from the headlines" tips the course authors have successfully deployed in the trenches to harden infrastructure in order to prevent and detect modern attacks. Examples include the use of private VLANs, which effectively kills the malicious client-to-client pivot, and 802.1X and NAC, which mitigate rogue devices. Specific Cisco IOS syntax examples are provided to harden switches.

TOPICS: Traditional Security Architecture Deficiencies; Defensible Security Architecture; Threat, Vulnerability, and Data Flow Analysis; Layer 1 Best Practices; Layer 2 Best Practices; Netflow

SECTION 2: Network Security Architecture and Engineering

Section 2 continues hardening the infrastructure and moves on to layer three: routing. Actionable examples are provided for hardening routers, with specific Cisco IOS commands to perform each step. The section then continues with a deep dive on IPv6, which currently accounts for 23% of Internet backbone traffic, according to Google, while simultaneously being used and ignored by most organizations. This section will provide deep background on IPv6, discuss common mistakes (such as applying an IPv4 mindset to IPv6), and provide actionable solutions for securing the protocol. The section wraps up with a discussion of VPN and stateful layer three/four firewalls.

TOPICS: Layer 3: Router Best Practices; Layer 3 Attacks and Mitigation; Layer 2 and 3 Benchmarks and Auditing Tools; Securing SNMP; Securing NTP; Bogon Filtering, Blackholes, and Darknets; IPv6; Securing IPv6; VPN; Layer 3/4 Stateful Firewalls; Proxy

SECTION 3: Network-Centric Security

Organizations own or have access to many network-based security technologies ranging from next-generation firewalls to web proxies and malware sandboxes. Yet the effectiveness of these technologies is directly affected by their implementation. Too much reliance on built-in capabilities like application control, antivirus, intrusion prevention, data loss prevention, or other automatic evil-finding deep packet inspection engines leads to a highly preventative-focused implementation, with huge gaps in both prevention and detection. Section 3 focuses on using application layer security solutions that an organization already owns with a modern mindset. By thinking outside the box, even old controls like a spam appliance can be used to catch modern attacks such as phishing via cousin domains and other spoofing techniques. And again, by engineering defenses for modern attacks, both prevention and detection capabilities gain significantly.

TOPICS: NGFW; NIDS/NIPS; Network Security Monitoring; Sandboxing; Encryption; Secure Remote Access; Distributed Denial-of-Service (DDOS)

SECTION 4: Data-Centric Security

Organizations cannot protect something they do not know exists. The problem is that critical and sensitive data exist all over. Complicating this even more is that data are often controlled by a full application stack involving multiple services that may be hosted on-premise or in the cloud. Section 4 focuses on identifying core data where they reside and how to protect those data. Protection includes the use of data governance solutions and full application stack security measures such as web application firewalls and database activity monitoring, as well as keeping a sharp focus on securing the systems hosting core services such as on-premise hypervisors, cloud computing platforms, and container services such as Docker. The data-centric security approach focuses on what is core to an organization and prioritizes security controls around it. Why spend copious amounts of time and money securing everything when controls can be optimized and focused on securing what matters? Let's face it: Some systems are more critical than others.

TOPICS: Application (Reverse) Proxies; Full Stack Security Design; Web Application Firewalls; Database Firewalls/Database Activity Monitoring; File Classification; Data Loss Prevention (DLP); Data Governance; Mobile Device Management (MDM) and Mobile Application Management (MAM); Private Cloud Security; Public Cloud Security; Container Security

SECTION 5: Zero-Trust Architecture: Addressing the Adversaries Already in Our Networks

Today, a common security mantra is "trust but verify." But this is a broken concept. Computers are capable of calculating trust on the fly, so rather than thinking in terms of "trust but verify" organizations should be implementing "verify then trust." By doing so, access can be constrained to appropriate levels at the same time that access can become more fluid. This section focuses on implementing a zero-trust architecture where trust is no longer implied but must be proven. By doing so, a model of variable trust can be used to change access levels dynamically. This, in turn, allows for implementing fewer or more security controls as necessary given a user's and a device's trust maintained over time. The focus is on implementing zero trust with existing security technologies to maximize their value and impact for an organization's security posture. During this section encryption and authentication will be used to create a hardened network, whether external or internal. Also, advanced defensive techniques will be implemented to stop modern attack tools in their tracks while leaving services fully functional for authorized assets.

TOPICS: Zero-Trust Architecture; Credential Rotation; Compromised Internal Assets; Securing the Network; Tripwire and Red Herring Defenses; Patching; Deputizing Endpoints as Hardened Security Sensors; Scaling Endpoint Log Collection/Storage/Analysis

SECTION 6: Hands-On Secure-the-Flag Challenge

The course culminates in a team-based Design-and-Secure-the-Flag competition. Powered by NetWars, day six provides a full day of hands-on work applying the principles taught throughout the week. Your team will progress through multiple levels and missions designed to ensure mastery of the modern cyber defense techniques promoted throughout this course. Teams will assess, design, and secure a variety of computer systems and devices, leveraging all seven layers of the OSI model.

TOPICS: Capstone – Design/Detect/Defend

Course Preview
available at: **sans.org/demo**