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

GIAC CERTIFICATIONS

SEC530: **Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise**

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
- Discover data, applications, assets and services, and assess compliance state
- Implement technologies for enhanced prevention, detection, and response capabilities
- Comprehend deficiencies in security solutions and understand how to tune and operate them
- Understand the impact of 'encrypt all' strategies
- 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 technologies
- 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
- Design and Implement Zero Trust strategies leveraging current technologies and investment

GDSA
Defensible Security Architecture
giac.org/gdsa

GIAC Defensible Security Architecture

"The GIAC Defensible Security Architecture (GDSA) certificate is an industry certification that proves an individual is capable of looking at an enterprise defense holistically. A GDSA no longer emphasizing security through a single control but instead applies multiple controls ranging from network security, cloud security, and data-centric security approaches to properly prevent, detect, and respond. The end result is defense-in-depth that is maintainable and works."
— Justin Henderson, SEC530 Course Author

- Defensible Security Architecture: network-centric and data-centric approaches
- Network Security Architecture: hardening applications across the TCP/IP stack
- Zero Trust Architecture: secure environment creation with private, hybrid or public clouds

SEC530: Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise is designed to help students establish and maintain a holistic and layered approach to security, while taking them on a journey towards a realistic 'less trust' implementation, based on Zero Trust principles, pillars and capabilities. Effective security requires a balance between detection, prevention, and response capabilities, but such a balance demands that controls be implemented on the network, directly on endpoints, and within cloud environments. The strengths and weaknesses of one solution complement another solution through strategic placement, implementation, and continuous fine-tuning.

To address these issues, this course focuses on combining strategic concepts of infrastructure and tool placement while also diving into their technical application. We will discuss and identify what solutions are available and how to apply them successfully to reduce attack surface and implement adaptive trust. Most importantly, we'll evaluate the strengths and weaknesses of various solutions and how to layer them cohesively to achieve a defensible security architecture.

SEC530 is a practical class, focused on teaching effective tactics and tools to architect and engineer for disruption, early warning detection, and response to most prevalent attacks, based on the experience of the authors, highly experienced practitioners with an extensive career in cyberdefense. There will be a heavy focus on leveraging current infrastructure (and investment), including switches, routers, next-gen firewalls, IDS, IPS, WAF, SIEM, sandboxes, encryption, PKI and proxies, among others. Students will learn how to assess, re-configure and validate these technologies to significantly improve their organizations' prevention, detection and response capabilities, augment visibility, reduce attack surface, and even anticipate attacks in innovative ways. The course will also delve into some of the latest technologies and their capabilities, strengths, and weaknesses. You will come away with recommendations and suggestions that will aid in building a robust security infrastructure, layer by layer, across hybrid environments, as you embark on a journey towards Zero Trust.

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

Multiple hands-on labs conducted daily 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.**

sans.org/sec530

- **Watch a preview of this course**
- **Discover how to take this course: Online, In-Person**

Section Descriptions

SECTION 1: Defensible Security Architecture and Engineering: A Journey Towards Zero Trust

This first section of the course describes the principles of designing and building defensible systems and networks. In this section we introduce the fundamentals of security architectures and the journey towards Zero Trust. We will cover traditional vs defensible security architectures, security models and winning techniques, and the defensible security architecture life cycle or DARIOM (Discover, Assess, Re-Design, Implement and Monitor) model. The main emphasis on Sections 1 is on practical threat modeling with models like MITRE ATT&CK and building a good foundation from the bottom up, starting with physical security, and network security at the lower layers, from VLANs and PVLANs, along with understanding what normal looks like by baselining network activity with NetFlow data across hybrid environments, on-prem and in the Cloud. Section 1 will also introduce you to the principle of Time-Based Security and how to implement it in real world.

TOPICS: Course Overview; Defensible Security Architecture; Traditional Security Architecture Deficiencies; Winning Defensible-Security Strategies; Security Models; Threat, Vulnerability, and Data Flow Analysis; Layer 1: Physical Security Best Practices; Layer 1: Network Security Best Practices; NetFlow

SECTION 2: Network Security Architecture and Engineering

This section continues the discussion on hardening critical infrastructure that is often found in hybrid environments, and moves on to concepts such as routing devices, firewalls, and application proxies. 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 over 30% percent of Internet backbone traffic, according to Google, while simultaneously being used and ignored by most organizations. We 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 continues with a discussion of a key Zero Trust topic: segmentation. This section includes principles and defensive tactics that cover firewalls and network segmentation but also identity and access segmentation. Section 2 wraps up with a discussion on web application proxies and smtp proxies.

TOPICS: Layer 3: Attacks and Mitigation; Switch and Router Best Practices; Layer 2 and 3: Benchmarks and Auditing Tools; Securing SNMP; Securing NTP; Bogon Filtering, Blackholes, and Darknets; IPv6; Securing IPv6; Segmentation; Application Proxies

Who Should Attend

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

SECTION 3: Network-Centric Security Application Security Architecture

Organizations own or have access to many network-based security technologies, ranging from Next-Generation Firewalls to IDS/IPS and malware sandboxes. These are often deployed on-prem but also in the Cloud. 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. This section focuses on improving the efficacy of prevention and detection technologies using application-layer security solutions with a Zero Trust 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; Network Security Monitoring (NSM); NIDS/NIPS; Sandboxing; Encryption; Secure Remote Access; Distributed Denial-of-Service Protection

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

“Trust but verify” has been a common security mantra. But this is a broken concept. Computers can calculate 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 culminates our journey towards Zero Trust by focusing on implementing an 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. On Section 5, we will review the zero trust principles, model and the latest US Government mandates (DISA, NSA, NIST), while we focus on practical implementations of this new philosophy. The focus will be on practical application of zero trust through existing infrastructure to maximize their value and impact for an organization’s security posture.

TOPICS: Zero Trust Architecture; Credential Rotation; Compromised Internal Assets; Securing the Network; Segmentation Gateways; Leveraging Endpoints as Hardened Security Sensors; Scaling Endpoint Log Collection/Storage/Analysis; MITRE ATT&CK Content Engineering; Tripwire and Red Herring Defenses

SECTION 4: Data-Centric Application Security Architecture

Our journey continues with the discussion of a strategy that is central to a Zero Trust Architecture: 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-premises or in the cloud. This section focuses on identifying core data where they reside and how to classify, label and protect those data. Protection includes using 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-premises 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 Challenges; Container Security

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 the knowledge, tools and skills obtained in class, as they defend Tyrell Corporation from the attack of the replicants.

TOPICS: Capstone – Design/Detect/Defend

> **“This training showed how the overall security posture of an organization can be improved. It helps connect the dots between different areas within security infrastructure.”**
>
> — Farruk Ali, **UPS**