SEC301: **Introduction to Cyber Security™**

GISF
Information Security Fundamentals
giac.org/gisf

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Explain cybersecurity fundamentals using clear, business-ready language
- Identify common threat types and the vulnerabilities they exploit
- Understand how cryptography, authentication, and access control establish digital trust
- Describe how networks, data flows, and Zero Trust principles reduce risk
- Recognize how malware, phishing, and social engineering attacks operate—and how to disrupt them
- Connect frameworks such as NIST CSF, CIS Controls, and MITRE ATT&CK/D3FEND to practical defense strategies
- See how cloud, IoT, and AI reshape both opportunities and risk
- Collaborate confidently with technical teams on security policies and incident response

Business Takeaways

- Speak the language of cybersecurity—bridging the gap between technical and business teams
- Identify and communicate risk clearly in terms of impact, accountability, and resilience
- Support compliance and governance efforts with an informed understanding of frameworks and controls
- Strengthen organizational security culture by promoting awareness and shared responsibility
- Contribute to strategy and decision-making with confidence rooted in understanding, not fear
- Empower others—becoming the person in the room who can translate cybersecurity into action

"SEC301 is an extremely valuable course, even for someone with 12 years of IT experience!"

—Brian Pfau, **Banfield Pet Hospital**

Cyber Starts Here: Building Confidence, Not Confusion

Cybersecurity isn't just a technical discipline anymore—it's the language of modern business. Every department, from IT and finance to HR, legal, and operations, depends on secure systems and trustworthy data. Every project carries risk, and every decision, from approving a vendor to opening an email, has security implications. Yet most professionals are never given the chance to learn cybersecurity in a way that feels clear, relevant, and approachable.

SEC301: Introduction to Cybersecurity changes that. It's designed for anyone who needs to understand cybersecurity fundamentals without drowning in jargon or acronyms. This course provides a common foundation that connects people, process, and technology. You'll learn how threats exploit vulnerabilities, how human behavior can make or break defenses, and how security controls from encryption to access management create resilience when applied thoughtfully.

Rather than memorizing definitions, you'll build fluency in the core ideas that drive cybersecurity decisions across every industry: how data moves, where trust begins, and how risk is managed. Whether you're supporting a security team, auditing compliance, advising leadership, or simply trying to make sense of today's headlines, SEC301 gives you the context to see the bigger picture and the confidence to contribute meaningfully to it.

Across five focused days, you'll explore the modern cybersecurity landscape through stories, visuals, and hands-on activities that make abstract ideas tangible:

- **Day 1: Why Cyber Matters—**Explore how threat, vulnerability, and impact intersect to create risk, and why security failures have real business, legal, and human consequences.
- **Day 2: Building Digital Trust—**Learn how cryptography, authentication, and modern identity frameworks establish confidentiality and integrity across systems.
- **Day 3: Data in Motion—**Trace how information moves through networks, understand ports, protocols, and DNS, and discover how Zero Trust principles protect data wherever it flows.
- **Day 4: How Attacks Work—**Demystify malware, phishing, and adversary tactics using MITRE ATT&CK examples and behavioral clues analysts rely on to detect and disrupt intrusions.
- **Day 5: Defending What Matters—**Connect the dots across web security, SOC operations, cloud, IoT, and AI, and see how people, tools, and frameworks combine to sustain digital trust.

No technical background is required just curiosity and a willingness to learn. Each topic blends plain-language instruction with realistic scenarios and guided labs that turn theory into experience. You'll practice analyzing risk, mapping attacks to defenses, and explaining security concepts in terms that business leaders understand.

By the end of the week, you won't just recognize cybersecurity vocabulary you'll understand the reasoning behind it. You'll be able to connect technical controls to organizational outcomes, translate security concepts into decisions, and support a culture of shared responsibility for digital trust.

Because in today's world, cybersecurity isn't just an IT issue, it's a leadership skill.

"SEC301 is a great class for the individual who wants to learn an extensive amount of material in one week."

—**Steven Chovanec**, Discover Financial Services

Section Descriptions

SECTION 1: Cybersecurity Foundations

Begin with the essentials that make cybersecurity practical. Learn how threats become risk, why availability can be life-critical, and how trust grows from clear process and communication. Each lab brings concepts to life so you can explain, choose, and apply controls with confidence.

LABS:

- The Risk Equation in Action
- The Missing Patch
- To Report or Not?
- Frameworks in the Wild
- Evidence Trail

SECTION 2: Building Digital Trust: Cryptography, Identity, and Access

Build the foundations of digital trust with the core ideas behind encryption, identity, and access. Learn how math protects data, how certificates prove who's who, and how authentication and authorization shape accountability. Each lab turns complex concepts into clear steps you can use with confidence.

LABS:

- Secrets, Salts, and the Trust Equation
- Keys to the Kingdom: Proving Identity
- Lock, Stock, and Certificate
- Who Are You? The AAA of Digital Identity
- The Passwordless Pivot

SECTION 3: Understanding Networks and Data in Motion

Explore how data travels and what it reveals along the way. You'll break down layers, packets, routing, and DNS, then see how firewalls and segmentation shape trust. Each lab turns network theory into clear understanding so you can follow data in motion and make smarter defense decisions grounded in visibility.

LABS:

- Ports and Protocols
- HopbyHop
- DNS Detective
- Encrypted, Not Invisible
- Zero Trust, Zero Assumptions

SECTION 4: Modern Attack Tactics: From Phishing to AI-Powered Threats

Step into the attacker's mindset to understand how threats evolve. Section 4 explores phishing, credential abuse, wireless compromise, malware behavior, and AI-driven campaigns. Labs help you trace attacker choices, map tactics to ATT&CK and D3FEND, and build defenses that break the chain of compromise.

LABS:

- The Many Doors In
- Rogue Signal
- Name That Malware
- The AI Arms Race: Who's Winning?
- ATT&CK & D3FEND

SECTION 5: Cybersecurity Technologies and Web Security

Section 5 ties the course together with the tools, teams, and web risks that shape real security. You'll break down common web flaws, see how SOC technologies work in practice, and explore cloud, IoT, and AI-driven defense. Each lab shows how people and systems combine to protect data, safety, and trust.

LABS:

- The Web We Built: Layers of Trust
- Inside the Glass Box
- The Cloud Breach That Wasn't
- The Factory Floor Goes Dark
- Human + Machine

"SEC301 was my first SANS course, and I was not disappointed! Keith was exceptional in presenting this information in a clear and concise manner. He took the time to really explain concepts and challenged us to think things through. I learned a great deal and look forward to future SANS events."

—Rebekah Wolf, **TenWolf Technology Information Services**

Who Should Attend

- Anyone new to information security and in need of an introduction to the fundamentals of security
- Those who feel bombarded with complex technical security terms they don't understand but want to understand
- Professionals who need to be conversant in basic security concepts, principles, and terms, but who don't need "deep in the weeds" detail
- Those who have decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification
- Managers who worry their company may be the next mega-breach headline story on the 6 o'clock news

NICE Framework Work Roles

- Authorizing Official/Designating Representative (OPM 611)
- Knowledge Manager (OPM 431)
- Privacy Officer/Privacy Compliance Manager (OPM 732)
- Cyber Instructor (OPM 712)
- Communications Security (COMSEC) Manager (OPM 723)

GISF

Information Security Fundamentals

giac.org/gisf

GIAC Information Security Fundamentals

The GIAC Information Security Fundamentals (GISF) certification validates a practitioner's knowledge of security's foundation, computer functions and networking, introductory level cryptography, and cybersecurity technologies. GISF certification holders will be able to demonstrate key concepts of information security including: understanding the threats and risks to information and information resources, identifying best practices that can be used to protect them, and learning to diversify our protection strategy.

- Cybersecurity terminology
- The basics of computer networks
- Security policies
- Incident response
- Passwords
- Introduction to cryptographic principles