Cybersecurity **Learning Saturday**

What it takes to Start a Career in Information Security

Saturday, July 25, 2020, at 3 PM EST

SISARGO
INSTITUTE
www.sisargo.org

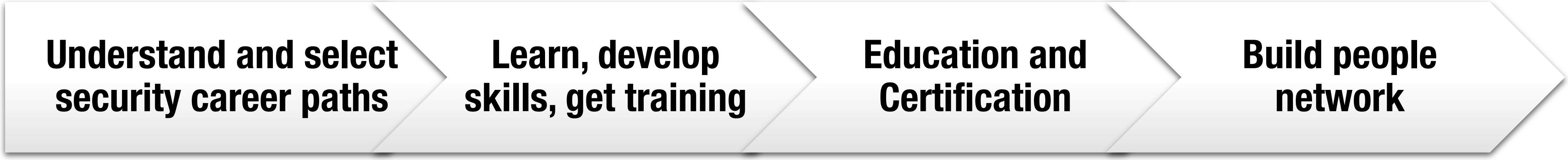
Discussion Topics

- Introduction
- Why get into security career?
- Career paths
- Skills, Education, Certification
- Where to start

Why get into Cybersecurity?

Skills shortage, one of the highest paying jobs, ever changing field, needs continuous skills development

What am I getting into?



Understand and select security career paths

Learn, develop skills, get training

Education and Certification

Build people network

- Security administrators
- SOC analysts
- Forensic investigations and incident response
- Security architecture
- Cloud security architects
- Vulnerability management
- Product development
- Governance, Risk and Compliance

- Operating systems
- Networking protocols
- Some development and programming, web applications
- Security tools
- Self practice
- Coursera free courses

- Education, masters programs
- Vendor-neutral certifications
- Vendor-specific certifications

- Join local groups
- ISSA
- ISACA
- (ISC)^2
- Conferences
- Open source contributions

What Makes you Successful?

Education, Certifications, Experience, Personal Network

Security Career Paths

Information security is a vast field with many careers to choose from. Each paths has its own requirements.

SECURITY CAREER PATHS

- **Security administration** (firewalls, IPS, other technologies, identity and access management)
- **Risk management** (governance, audit, compliance)
- **Threat management** (SOC analysts, incident responder, forensic investigations, vulnerability management, penetration testing, assessments, application security testing)
- **Cloud security** – Cloud security administrators, architects
- **Security architecture**
- **Are multiple paths possible?**

Personal Skills Development

What skills are needed in addition to education and certifications?

ESSENTIAL SKILLS

- **Operating Systems**
  - Linux/Unix and Windows
- **Networking and application protocols**
  - Very good knowledge of TCP/IP, DNS, HTTP, SMTP, SSH etc. Hands on practice for routers and switches, packet capture, nmap, curl, etc.
- **Programming** (at least basic level)
  - Shell scripting, Python, C would be great to know, understand how web applications are built, HTML, JavaScript, SQL/Databases
- **Encryption**
  - PKI concepts, TLS

Kali Linux

- Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering.
- https://www.kali.org/docs/introduction/what-is-kali-linux/
- YouTube videos on Kali Linux Training

Educational Background

What educational background is needed for careers in information security?

Security Certifications

What certifications are available? where should I start?

SECURITY CERTIFICATION

- **Vendor-neutral certifications**
  - (ISC)^2 – CISSP, CCSP
  - ISACA – CISM, CISA, CRISC
  - Cloud Security Alliance (CCSK)
  - Certified Ethical Hacker (CEH)
  - CompTIA Security+
  - Linux Foundation certifications
  - EC-Council Computer Hacking Forensic Investigator C|HFI
- **Vendor-specific certifications**
  - Security vendors (Cisco, Palo Alto)
  - IaaS Cloud vendors (AWS, Microsoft, Google)
  - CCNA Security

Where to Start From?

This is too much and overwhelming! Where should I start from?

MAKE A PLAN

- Build a plan for a particular career path
- See what you can do in your current job, opportunity to learn and apply skills
  - Many people are able to switch to security from other career paths at their work.
- Start building skills, pursue people network
- Decide a certification you want to pursue
- Use Coursera and find some free courses
- Install VirtualBox and Kali Linux. Start using Kali Linux tutorials

Free tools and training

- SANS free tools - https://www.sans.org/media/free/free-faculty-tools.pdf
- CIS Top 20 controls - https://www.cisecurity.org/controls/
- Kali Linux - https://www.kali.org/
- Coursera - https://www.coursera.org/search?query=security&