PHOENIX FORWARD
strengthening the road to prosperity

**WORKFORCE COLLABORATIVE: CYBERSECURITY**

***BUILDING THE TALENT PIPELINE***

***SECURITY ANALYST CAREER PATHWAY***

UPDATED: 10/17/16

# CYBERSECURITY

# SECURITY ANALYST CAREER PATHWAY

## Senior Level

Senior Specialty Threat, Consultant, Engineer, Manager

## Mid Level Analyst

IT Security Analyst, Information Security Analyst, Information Security Reporting Analyst, IT Security Governance, Identity Management, Security Assurance Analyst, Network Analyst

## Junior Analyst

Security Analyst, Security Analyst I, Network Analyst,
Information Security Developer (Identity Management)

***Developed by the GPCF– Cybersecurity Collaborative. Updated October 17, 2016***

## Senior Level

### Job Titles

Senior Specialty Threat: Senior Principal Architect, Cloud Security Architect, Senior Security Engineer, Senior IT Engineer, Security Analysts – Process & Audit, CISO

Consultant: IT Security Senior Consultant, Senior Security Consultant, IT Security Consultant, Security Architect , IT Architect Senior

Engineer: Senior Security Engineer, IT Security Engineering, Information Security Architect, Information Security Engineer (IT Security Gov.)

Manager: Chief Information Security Officer, IT Security Assurance & Risk

### Senior Level Certifications

Junior & mid-level certifications plus: CCAr, CCIE Security, CCIE (Data Center, Collaboration, Wireless) CCNA Security, CISA, CIPP, CISM, CISSP, GCPM, GNFA, GPEN, GREM, GSE, GSLC, GWAPT, GXPN, HIPAA, RHCA

### Competencies & Technical Skills

Mid-level experience plus: SQL; API; VMS; DLP; data classification; firewall; network security; security architecture and design; application and database security; InfoSec legal expert; crisis communications; cryptography; computer forensics; and SIEM separate noise from vital information.

### Education

Bachelor Degree and/or years of experience to substitute

### Experience

6 – 10 years

# Mid Level Analyst

**Job Titles**

IT Security Analyst, Information Security Analyst, Information Security Reporting Analyst, IT Security Governance, Identity Management, Security Assurance Analyst, Network Analyst

**Mid Level Certifications***

CCFP, CCNP (Cloud, Data Center, Collaboration, Wireless), CCNP R&S, CCNP Security, CEH, CRISC, GCFE (GIAC), GCIA (GIAC), GCIH (GIAC), GFCE, GISP (GIAC), GLEG (GIAC), IAM, IEM, MCSE, RHCE

**Competencies & Technical Skills**

Junior Analyst experience plus: audit; pen testing; reporting (C2M2, NIST Framework, KPI creation, monitoring, reporting; threat analysis and data classification; business process mapping; application security; cryptography concepts and techniques; enterprise storage; network and security components; risk mitigation, planning, strategies and controls; conduct incident response and recovery procedures; authentication and authorization technologies;  and threat hunter.

**Education**

Associate Degree, Bachelor Degree preferred, and/or years of experience to substitute

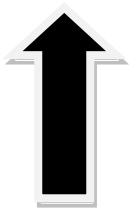
**Experience**

3-6 years

*Certifications and explanations attached at end of document

**Technical skills required to advance**

Recommend bachelor degree; incident response process; additional attack types; data obfuscation and encoding techniques; traffic analysis; in-depth IDS vs. IPS; IDS (Snort/Suricata/Bro) signature creation



**Employability skills required to advance**

Learn event avoidance; demonstrate thought leadership; project management; critical thought process; ability to influence without authority and ability to hunt for and triage threats.

## Junior Analyst

**Job Titles**

Cybersecurity Analyst, Security Analyst I, Information Security Developer (Identity Management), Network Analyst

**Basic Certifications**

A+ (CompTIA), Network+ (CompTIA), Security+(CompTIA), Linux+, MCSA, MCP, GSEC – GIAC Security Essentials, SAN, Cisco CCENT, CCNA R&S, CCNA Security, CCNA Cyber Ops and RHCSA

**Qualities for Employment**

CIA Triad: confidentiality, integrity and availability; problem solver; highly technical; self-driven; resourceful; sound judgment; communications and analytical skills; ability to communicate and collaborate with other functions and departments within the organization.

**Competencies & Technical Skills**

MS Office; fundamental knowledge of: Linux CLI; Windows CLI; coding; common ports and protocols; ethernet frames and packets; signature vs. heuristic detection; network devices; understand common attack vectors and associated countermeasures; underlying principles of access control systems and implement, manage and secure those systems; risk identification and analysis; implement incident processes; policy; standards and compliance

**Education**

Associates degree

**Experience**

0-3 years

**Cybersecurity Certifications Definitions**

Appropriate for junior positions and do not require work experience. For example, students from Embry-Riddle Aeronautical University (ERAU) BS can graduate with all four CompTIA certificates while community college programs also cover this material. Note an ERAU student may be a CISSP associate (they pass test but lack the 5 years full time work experience). Even this listing is only partial (see end for listing found in a recent ad!).

# Basic Certifications

- **A+** – indicates the individual has baseline knowledge of computers; CompTIA
- **Network+** – indicates the individual has baseline knowledge of networks; CompTIA
- **Security+** – indicates the individual has baseline knowledge relating to securing a network and managing risk; CompTIA
- **Linux+** – indicates the individual has the knowledge, skills and abilities to build, use, and manage Linux operating systems; appropriate for IT professionals.
- **MCSA** – Microsoft Certified Solutions Associate – a series of certifications that indicate the individual has an understanding of the named Microsoft Operating System (e.g. MCSA: Windows 10); appropriate for an IT professional.
- **MCP** – Microsoft Certified Professional – indicates the individual has an understanding of Microsoft products, technologies, and solutions; appropriate for an IT professional or developer.
- **GSEC** – GIAC Security Essentials – indicates the individual has an understanding of information security beyond simple technology and concepts; appropriate for anyone seeking a hands-on role with respect to security tasks.
- **CCENT** – Cisco Certified Entry Networking Technician – equivalent to Network+ with a focus on Cisco technologies. It is the first stage of Cisco's certification system. CCENT qualified individuals have the knowledge and skills to install, manage, maintain and troubleshoot a small enterprise branch network, including network security.
- **CCNA R&S** – Cisco Certified Network Associate Routing and Switching – includes the competencies of the CCENT and adds depth to WAN and LAN protocols, router and switch security, VLANs and network management.
- **CCNA Security** – Cisco Certified Network Associate Security – Includes the competencies of the CCENT and adds IOS (router and switch) network security technologies including AAA, IPS, Firewalls and system hardening. Compliant with NSA / CNSS 4011.
- **CCNA Cyber Ops** – Cisco Certified Network Associate Cyber Operations – Two part exam validates associate-level Security Operations Center Security Analyst skills. Part one is equivalent to Security+. Part two evaluates threat analysis, intrusion analysis and incident response skills.
- **RHCSA** – Red Hat Certified System Administrator - able to perform the core system administration skills required in Red Hat Enterprise Linux environments. Requires passing the performance-based RHCSA exam (EX200).

**Note**: Other vendor and non-vendor specific certification may be equivalent substitutes for one of more of the **Intermediate Certifications** listed in this document.

Appropriate for mid-level and even some senior positions. As noted, some are quite specific to particular roles and jobs. Some of these are more process oriented and less technical.

# Intermediate Certifications

- **GISP** – GIAC Information Security Professional – technical information security information; appropriate for security professionals, IT and managers
- **GCFE** – GIAC Certified Forensic Examiner – indicates the individual has the knowledge, skills and abilities to collect and analyze data from Windows systems; appropriate for security, IT, legal, and law enforcement professionals.
- **GCIA** – GIAC Certified Intrusion Analyst – indicates the individual has the knowledge, skills and abilities to configure and monitor intrusion detection systems, and to read, interpret, and analyze network traffic and related log files; appropriate for security operations personnel.
- **CEH** – Certified Ethical Hacker – indicates the individual has the knowledge, skills and abilities to understand what a malicious hacker is doing, and to use the same techniques to improve the security of friendly networks; appropriate for security professionals.
- **GCIH** – GIAC Certified Incident Handler – indicates the individual has the knowledge, skills and abilities to manage security incidents by understanding common attack techniques, vectors and tools, has the ability to defend against and/or respond to such attacks when they occur; appropriate for anyone who may respond to an incident.
- **GLEG** – GIAC Law of Data Security and Investigations – indicates the individual has knowledge regarding the law of business, contracts, fraud, crime, IT security, IT liability and IT policy with a focus on electronically stored and transmitted records; appropriate for security, IT, legal and law enforcement professionals.
- **CFCE** –Certified Forensic Computer Examiner – indicates the individual has the knowledge, skills and abilities to conduct a computer forensics examination; appropriate for security, IT and law enforcement professionals.
- **CCFP** – Certified Cyber Forensics Professional: indicates the individual has the knowledge, skills and abilities to conduct a computer forensics examination; appropriate for security, IT and law enforcement professionals.
- **CRISC** – Certified in Risk and Information Systems Control – indicates the individual has knowledge, skills and abilities in the field of managing IT risks; it is appropriate for information technology professionals.
- **CCNP R&S** – Cisco Certified Network Professional Routing and Switching – validates enterprise-level skills with the ability to plan, implement, verify and troubleshoot local and wide-area enterprise networks and work collaboratively with specialists on advanced security, voice, wireless and video solutions.
- **CCNP Security** – Cisco Certified Network Professional Security – aligns specifically to the job role of the Cisco Network Security Engineer responsible for security in routers, switches, networking devices and appliances, as well as choosing, deploying, supporting and troubleshooting firewalls, VPNS, and IDS/IPS solutions for their networking environments.
- **CCNP Cloud/Data Center/Collaboration/Wireless** – Cisco Certified Network Professional – certification acknowledge advanced networking knowledge and skills in the technologies related to the specialty listed. In general, CCNP certification holders have industry experience in the area related to their certification.
- **RHCE** – Red Hat Certified Engineer – a RHCSA who possesses the additional skills, knowledge and abilities required of a senior system administrator responsible for Red Hat Enterprise Linux systems. Required deep knowledge of Red Hat Enterprise Linux kernels, system utilization, Linux networking, SMB, SMTP, SSH and iSCSI.

**Note**: Other vendor and non-vendor specific certification may be equivalent substitutes for one of more of the **Intermediate Certifications** listed in this document.

Some of these are more managerial and others more technical but require more knowledge of overall systems; may require experience.

# Advanced Certifications

- **CISSP** – Certified Information Systems Security Professional – indicates the individual has knowledge, skills and abilities in the field of information security; appropriate for information assurance professionals. (Requires 5 years full time work experience and referral by current CISSP) A leading certification.
- **CISM** – Certified Information Security Manager – indicates the individual has knowledge, skills and abilities in the field of information security management; appropriate for information security managers
- **GSLC** – GIAC Security Leadership – indicates that the individual has advanced knowledge, skills and abilities requisite for managing information security personnel; appropriate for security professionals with managerial or supervisory responsibility for information security staff
- **GSE** – GIAC Security Expert – requires passing a multiple-choice exam and a lab exam involving an incident scenario. Considered one of the top security certifications.
- **GCPM** – GIAC Certified Project Manager – indicates the individual has the knowledge, skills and abilities to participate in or lead project teams and demonstrates an understanding of technical project methodology and implementation, while ensuring effective communication, time, cost, quality, procurement, and risk management; appropriate for security professionals and mangers
- **GPEN** – GIAC Penetration Tester – indicates the individual has the knowledge, skills and abilities to assess target networks and systems to find security vulnerabilities; appropriate for security professionals.
- **GWAPT** – GIAC Web Application Penetration Tester – indicates the individual has the knowledge, skills and abilities to assess web applications for vulnerabilities and conduct web application penetration testing; appropriate for security professionals.
- **GNFA** – GIAC Network Forensic Analyst – indicates the individual has the knowledge, skills and abilities to perform examinations employing network forensic artifact analysis; appropriate for security personnel involved in forensic analysis.
- **GCFA** – GIAC Certified Forensic Analyst – indicates the individual has an understanding of computer forensic analysis such that they may conduct typical incident investigations on Windows machines; appropriate for professionals in information security, legal and law enforcement.
- **GXPN** – GIAC Exploit Researcher and Advanced Penetration Tester – indicates the individual has the knowledge, skills and abilities to conduct advanced penetration tests, how to model the abilities of an advanced attacker to find significant security flaws in systems, and demonstrate the business risk associated with these flaws; appropriate for security personnel involved in assessing target networks to find vulnerabilities.
- **GREM** – GIAC Reverse Engineering Malware – indicates the individual has the knowledge and skills to reverse-engineer malicious software (malware) that targets common platforms, such as Microsoft Windows and web browsers. These individuals know how to examine inner-workings of malware in the context of forensic investigations, incident response, and Windows system administration; appropriate for anyone involved in protecting against malware and/or malware analysis.
- **CISA** – Certified Information Systems Auditor – indicates the individual has knowledge, skills, and abilities in the fields of IT security, IT audit, and IT risk management and governance; it is appropriate for auditors of information systems.
- **CCIE R&S** – Cisco Certified Internetwork Expert Routing and Switching – certifies the skills required of expert-level network engineers to plan, operate and troubleshoot complex, converged network

infrastructure. Requires passing both comprehensive written and lab exams. Expects years of industry experience to have the necessary background for the exams.

- **CCIE Security** - Cisco Certified Internetwork Expert Security – recognizes security experts who have the knowledge and skills to architect, engineer, implement, troubleshoot and support the full suite of Cisco security technologies and solutions using the latest industry best practices to secure systems and environments against modern security risks, threats, vulnerabilities and requirements.
- **CCIE Data Center/Collaboration/Wireless** – Cisco Certified Internetwork Expert – certification acknowledges expert-level networking knowledge and skills in the technologies related to the specialty listed. In general, CCIE certification holders have a number of years of industry experience in the area related to their certification.
- **CCAr** – Cisco Certified Architect – the highest level of accreditation achievable within the Cisco Career Certification program. CCAr recognizes those who can effectively translate complex business strategies into infrastructure requirements and clearly communicate and advocate the proposed architecture.
- **RHCA** – Red Hat Certified Architect - a RHCA is a RHCE or Red Hat Certified JBoss Developer who attained Red Hat's highest level of certification by passing and keeping current five additional hands-on exams on Red Hat technologies. Focused technology areas include data center, DevOps, cloud, applications platform and application development.

**Note**: Other vendor and non-vendor specific certification may be equivalent substitutes for one of more of the **Advanced Certifications** listed in this document.

**Desirable certifications:**

Network+, Security+ and Linux+, SANs GSEC, GCIH, GCIA, GCFA, GPEN, GWAPT, GCFE, GSNA, GPPA, GCWN, GISF, GCED, GAWN, GXPN, GSSP, GWEB and GNFA. Offensive Security OSCP, OSCE, OSWP, OSEE. Carnegie Mellon SEI and Certified Incident Handler. ISC2 CCFP, CCSP, CISSP, CSSLP, SSCP. Cisco CCNA, CCNP, CCNA Security. EC Council C|EH, CHFI, LPT, ECSA, ECIH, CNDA, ECSS, ECSP, ECES. Microsoft MCSE. EnCase EnCE.

## NICCS (National Initiative for Cybersecurity Careers and Studies)

**Workforce Framework 7 Categories**

1. **Securely Provision** - Specialty areas concerned with conceptualizing, designing and building secure IT systems, with responsibility for some aspect of the systems' development.
2. **Protect and Defend** - Specialty areas responsible for the identification, analysis, and mitigation of threats to internal IT systems or networks.
3. **Oversight and Development** - Specialty areas providing leadership, management, direction and/or development and advocacy so all individuals and the organization may effectively conduct cybersecurity work.
4. **Collect and Operate** - Specialty areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
5. **Operate and Maintain** - Specialty areas responsible for providing the support, administration and maintenance necessary to ensure effective and efficient IT system performance and security.
6. **Analyze** - Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
7. **Investigate** - Specialty areas responsible for the investigation of cyber events and/or crimes of IT systems, networks and digital evidence.

31 Specialty Areas within the 7 Categories

1. **Securely Provision**
    a. Information Assurance Compliance
    b. Software Assurance and Security Engineering
    c. Systems Development
    d. Systems Requirements Planning
    e. Systems Security Architecture
    f. Technology Research and Development
    g. Test and Evaluation
2. **Protect and Defend**
    a. Computer Network Defense Analysis
    b. Computer Network Defense Infrastructure Support
    c. Incident Response
    d. Vulnerability Assessment and Management
3. **Oversight and Development**
    a. Education and Training
    b. Information Systems Security Operations (Information Systems Security Officer)
    c. Legal Advice and Advocacy
    d. Security Program Management (Chief Information Security Officer)
    e. Strategic Planning and Policy Development
4. **Collect and Operate**
    a. Collection Operations
    b. Cyber Operations
    c. Cyber Operations Planning
5. **Operate and Maintain**
    a. Customer Service and Technical Support
    b. Data Administration
    c. Knowledge Management
    d. Network Services

e. System Administration
f. Systems Security Analysis

6. **Analyze**
    a. All Source Intelligence
    b. Exploitation Analysis
    c. Targets
    d. Threat Analysis
7. **Investigate**
    **a.** Digital Forensics
    **b.** Investigation