INFORMATION SECURITY ANALYSTS

A DEEP DIVE FOR SKILLS-BASED HIRING

REV: 04/04/16

SKILLFUL
A MARKLE INITIATIVE

Occupation Overview: Information Security Analyst

Foundational Competencies

- **Reading Comprehension:** Understanding written sentences and paragraphs in work-related documents.
- **Critical Thinking:** Using logic and reasoning to identify the strengths and weaknesses of alternative solutions, conclusions, or approaches to problems.
- **Complex Problem Solving:** Identifying complex problems and reviewing related information to develop and evaluate options and implement solutions.
- **Speaking:** Talking to others to convey information effectively.
- **Active Listening:** Giving full attention to what other people are saying, taking time to understand the points being made, asking questions as appropriate, and not interrupting at inappropriate times.
- **Writing:** Communicating effectively in writing as appropriate for the needs of the audience.
- **Time Management:** Managing one's own time and the time of others.
- **Judgment and Decision Making:** Considering the relative costs and benefits of potential actions to choose the most appropriate one.
- **Systems Analysis:** Determining how a system should work and how changes in conditions, operations, and the environment will affect outcomes.
- **Active Learning:** Understanding the implications of new information for both current and future problem solving and decision making.

Occupation-Specific Competencies

- **Intermediate Information Security:** Demonstrated ability to install, configure, troubleshoot, and maintain networks, hardware, software, etc. in a secure manner to ensure their confidentiality, integrity, and availability; utilize security solutions (access control, intrusion detection, etc.) to defend, monitor, and remediate; and identify/analyze/mitigate security risks and threats; familiarity with computer forensics, cyber investigation, incident response, vulnerability assessment/management, and security policies/procedures/plans.
- **Intermediate General Networking Tools and Concepts:** Demonstrated ability to provide network support with commonly-used tools/devices, including routers, switches, Ethernet, firewalls, frame relay, LAN, VPN, and WAN; demonstrated ability to set up IP addresses and run cabling.
- **Intermediate Network Protocols:** Demonstrated ability to facilitate communications across DNS, DHCP, SMTP, SNMP, TCP/IP, and other common network protocols.
- **Intermediate Core Operating Systems:** Demonstrated ability to install, configure, and maintain multiple core operating systems (e.g., Apple, Microsoft, Android) for computer and mobile devices; familiarity with the operation and maintenance of such non-traditional operating systems as Linux/Unix.
- **Basic Systems Design and Implementation:** Demonstrated ability to assist customers in the gathering of requirements and design, implement, and support simple technology solutions to existing business problems.
- **Intermediate Office Machines:** Demonstrated ability to assemble, configure, maintain, and repair multiple commonly-used office appliances and hardware components beyond computers/devices such as modems, printers, workstations, routers, and modems.
- **Intermediate Tech Support:** Demonstrated ability to diagnose customer problems and provide troubleshooting and issues resolutions for commonly-used computer hardware, software, applications, etc.; Provide support in areas such as computer/software installation and setup, computer repair, and general technical troubleshooting; Accurately record requests/resolutions from users into technical support software, escalating issues as appropriate; and Train users in the use of commonly-used system components.
- **Basic General Database:** Demonstrated proficiency with SQL basics (e.g., selecting, inserting, updating, deleting records), at least one database management software application, and database fundamentals such as normalization, schemas, and relationships.
- **Basic Auditing:** Basic familiarity with system records/logs to monitor status, identify security threats, evaluate risk and escalate issues
- **Basic Testing:** Demonstrated ability to design tests, create test scripts, ensure that test cases mimic user usage, execute and validate unit tests, and use appropriate test tools for their own changes. Familiarity with system and performance testing.

Job Description (Example)

Plan, implement, upgrade, or monitor security measures for the protection of computer networks and information. May ensure appropriate security controls are in place that will safeguard digital files and vital electronic infrastructure. May respond to computer security breaches and viruses.

- May execute security controls to prevent hackers from infiltrating company information or jeopardizing e-commerce programs and research attempted efforts to compromise security protocols.
- May maintain security systems for routers and switches, including company firewall.
- May use applicable encryption methods.
- May administer security policies to control access to company systems. May provide information to management regarding the negative impact on the business caused by theft, destruction, alteration, or denial of access to information.
- Work is usually non-routine and very complex in nature, involving the application of advanced technical/business skills in area of specialization.

Activities (Example List)

- Encrypt data transmissions and erect firewalls to conceal confidential information as it is being transmitted and to keep out tainted digital transfers.
- Develop plans, policies, and procedures to safeguard computer files against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs.
- Review violations of computer security procedures and discuss procedures with violators to ensure violations are not repeated.
- Monitor use of data files and regulate access to safeguard information in computer files.
- Monitor current reports of computer viruses to determine when to update virus protection systems.
- Modify computer security files to incorporate new software, correct errors, or change individual access status.
- Perform risk assessments and execute tests of data processing system to ensure functioning of data processing activities and security measures.
- Train users and promote security awareness to ensure system security and to improve server and network efficiency.
- Provide technical support to resolve security incidents.
- Conducts threat and vulnerability assessments.
- Evaluate security requirements and provide guidance for security of specific hardware and software components.

Prioritized Foundational Competencies: Information Security Analyst

Most Common Required Competencies	
1	**Critical Thinking:** Using thorough critical analysis to identify risks and rewards of alternative solutions, conclusions, or approaches to problems related to security controls; using independent thought to think outside the box and read between the lines when looking for problems.
2	**Active Listening:** Giving full attention to what seniors and clients are saying, taking care to fully understand by restating observation, and asking questions to clarify needs over wants; providing enough feedback to make sure the other person is comfortable you thoroughly understood.
3	**Judgment and Decision Making:** Applying logic when considering the relative risks and rewards of potential actions to choose the most appropriate one; evaluating impact of vulnerabilities and possible solutions; considering both micro and macro impacts of a decision; willingness to take a step back to gather enough information before acting.

Most Common Break Point Competencies	
1	**Time Management:** Managing one's own time through prioritization of tasks based on impact (e.g., financial value, population effected, system vulnerability); keeping focus and following tasks through completion.
2	**Active Listening:** *See previous.*
3	**Communication:** Effectively using the appropriate mode of communication to clearly convey a message (e.g., writing an enterprise wide security alerts, presenting findings to a supervisor); regularly sharing information within a team environment; adjusting message for varying audiences.

Most Preferred Competencies	
1	**Critical Thinking:** *See previous.*
2	**Complex Problem Solving:** Independently identifying complex problems and reviewing related information to develop, evaluate, and implement solutions; moving around roadblocks by collecting additional insights or resources.
3	**Systems Analysis:** Determining how a system should work and the downstream business impact of changes in conditions, operations, or the environment; applying risk analysis in the evaluation of inputs/outputs when determining expected outcomes.

Most Hard-to-Find Competencies	
1	**Critical Thinking:** *See previous.*
2	**Complex Problem Solving:** *See previous.*
3	**Communication:** *See previous.*

Most Evolving Competencies	
1	**Active Learning:** Evolution driven by constant changes in threats and technology as more components of business are digitized; changes make it important to stay abreast of current topics and industry standards through membership in industry groups and certification organization.
2	**Systems Analysis:** Evolution driven by growing systems, leading to increased complexity and more areas of vulnerability; changes make it important to leverage new tools in analysis of conditions, operations, and performance of a system allowing for better risk/reward decisions to be made.
3	**Complex Problem Solving:** Evolution driven by increasing trend of data availability across multiple platforms and networks; changes make it important to develop new strategies to resolve never-before-seen issues.

Prioritized Occupation-Specific Competencies: Information Security Analyst

Most Common Required Competencies

1	**Intermediate Core Operating Systems:** Demonstrated ability to install, configure, and maintain multiple core operating systems (e.g., Windows, Linux, OSX, iOS, Android) for computer and mobile devices in local and enterprise-wide scenarios; proficiency with A+ certification domain areas.
2	**Basic Network Protocols:** Familiarity with how to facilitate and protect communications utilizing common TCP/IP suite protocols like DNS, DHCP, SMTP, SNMP, FTP, TCP, ILS, etc.
3	**Basic Information Security:** Familiarity with CISSP domain concepts like how to install, configure, troubleshoot, and maintain networks, hardware, software, etc. in a secure manner to ensure their confidentiality, integrity, and availability; utilize security solutions (access control, intrusion detection, etc.) to defend, monitor, and remediate; identify/analyze/mitigate security risks and threats.

Most Common Break Point Competencies

1	**Intermediate Tech Support:** Demonstrated ability to diagnose customer problems and provide resolutions. Proficiency with the use of some components of commonly-used computer hardware, software, applications, etc. and a demonstrated ability to intake, triage, diagnose, and provide issue resolution support.
2	**Basic Systems Design and Implementation:** Demonstrated ability to assist customers in the gathering of requirements and design, implement, and support simple technology solutions to existing business problems.
3	**Basic General Networking Tools and Concepts:** Familiarity with how to provide network support for commonly-used tools/devices, including: routers, switches, Ethernet, firewalls, frame relay, LAN, VPN, and WAN; understanding of network fundamentals including network OSI model.

Most Preferred Competencies

1	**Basic Information Security:** *See previous.*
2	**Basic General Networking Tools and Concepts:** *See previous.*
3	**Basic Auditing:** Demonstrated ability to examine and analyze system records/logs to monitor status, identify security threats, evaluate risk, and escalate issues; familiarity with audit planning and management concepts from common certifications (e.g., CISA); utilizing analysis to measure performance against baselines.

Most Hard-to-Find Competencies

1	**Basic Information Security:** *See previous.*
2	**Basic General Networking Tools and Concepts:** *See previous.*
3	**Basic Auditing:** *See previous.*

Most Evolving Competencies

1	**Basic Information Security:** Evolution driven by information security becoming a key business focus as more complex systems bring greater vulnerability to sensitive data; changes make it important to keep credentials and methodologies up-to-date to protect from constantly evolving threats.
2	**Basic Auditing:** Evolution driven by frequently updated auditing and legal standards; changes make it more important to participate in regular continuing professional education courses.
3	**Basic Testing:** Evolution driven by accelerated time to market, increased prevalence of live testing, and constant development mindset; changes make it important to design and implement tests that can assess multiple types of vulnerabilities across a variety of systems, and additionally add to the value of being up-to-date on the newest testing methods.

Work Scenarios: Information Security Analyst

Work Scenario: Everyday virus detection and remediation	List of Competencies
In the early afternoon, Jane gets an email alert that says a user's system has a virus on it. Jane goes to her security monitoring tools to get additional details on the virus. Jane then gets the name and details of the virus and verifies that the virus is valid (e.g., the identified virus can take hold on the user's system) and begins to assess the severity of the virus (e.g., did the user's anti-virus software clean out the virus auJamalatically or not?, does this virus change the user's home page or start stealing credentials?, does the virus encrypt files or not?). Jane verifies that the virus is valid but appears to post limited risk. Jane calls desktop user support and gives the support staff the user's name, the virus name and a recommended set of actions to take with the user to resolve the problem. The desktop team reaches out to the user. Jane then goes into the company's ticking system and documents the alert, the actions taken and details about the virus. She leaves the ticket open until the desktop team contacts her and verifies that the virus has been removed from the user's system. She then closes the ticket.	• Critical Thinking • Judgment and Decision Making • Communication • *Information Security* • *Tech Support* • *Auditing*

Work Scenario: Serious virus infiltration	List of Competencies
In the morning, Tom gets an email alert that says a user has a virus on their system. Tom goes to his security monitoring tools and determines that the same virus is on twenty systems. Tom queries his security monitoring tools to gather evidence to determine how the virus propagated across the twenty systems. In particular, he wants to know whether the virus is spreading on its own or whether twenty different users were exposed to the virus independently. Tom determines that the virus is spreading and knows this is a serious security risk. Tom consolidates his findings and calls his manager and brings the manager up-to-speed. While the manager alerts the broader term, Tom continues to use his security tools to see if the virus is continuing to spread and what actions the virus may be taking. The manager comes to Tom's desk and says the incident response team is going to take over handling the problem at this point. Tom is asked to continue observing the viruses behavior and report any new information to his manager and the incident response team.	• Critical Thinking • Judgment and Decision Making • Communication • Complex Problem Solving • *Information Security* • *Tech Support* • *Auditing*

Work Scenario: User password problem	List of Competencies
Monique gets a ticket that says a user cannot log into their account. Monique contacts the user and verifies that the user is who they say they are. Monique then goes into her access tool and determines whether the user has been locked out of their account, forgot their password or has an expired password. Monique determines that the user has been locked out of their account. Monique picks up on the fact that the user is stressed about not being able to access their computer and tells the user that this problem can be resolved quickly. Monique asks if the user has tried to log-in multiple times, and the user says he has tried five times. Monique then queries the administrator tool and sees that the user has tried to log-in seven times and was locked out after hitting the maximum number of log-in attempts. Monique then unlocks the account, verifies that the user can log-in, updates the ticket and then closes the ticket.	• Critical Thinking • Active Listening • Judgment and Decision Making • Communication • *Tech Support* • *Information Security* • *Auditing*

Work Scenario: Potential brute force attack	List of Competencies
Jamal gets a call from a user who has been locked out of their account. While talking to the user, Jamal creates a ticket. The user says he updated his password three days ago and has no idea why his username and password are not working. Jamal queries his administrative tool and finds that there have been more than 500 failed log-in attempts over the last twenty-four hours. Jamal realizes this could be serious and suspects someone may be trying to brute force the user's account. Jamal explains to the user that the account has an issue and that he needs time to investigate. Jamal gets the user's contact information and says he will be in touch shortly. Jamal hangs up on the user, calls the security operations team and explains the situation to them. Jamal then waits for the security operations team to get back to him regarding the event and when the user can regain access. Ten minutes later, the security operations team calls Jamal to let him know the user can be granted access. Jamal unlocks the account, calls the user to let them know they can log back in, verifies the user can log-in and then updates and closes the ticket.	• Critical Thinking • Active Listening • Judgment and Decision Making • Communication • *Tech Support* • *Information Security* • *Auditing*

Occupation Deep Dive: Information Security Analyst

Job Titles Within This Occupation

- Security Engineer
- Security Analyst
- Network Security Engineer
- Information Technology Security Analyst
- Information Security Analyst
- Information Assurance Engineer
- Security Architect
- Cyber Security Engineer
- Information Systems Security Officer
- Information Security Manager
- Information Assurance Analyst
- Cyber Security Specialist
- Information Security Officer
- Security Compliance
- Security Technician
- Security Administrator
- Security Operations Analyst

Certification and Education Preferences (Example)

- Certified Information Systems Security Professional (CISSP)
- Cisco Certified Network Associate (CCNA)
- GIAC Security Essentials
- Security+
- Systems Security Certified Practitioner
- Certified Ethical Hacker (CHE-EC Council)
- CompTIA Advanced Security Practitioner (CASP)
- Microsoft Technology Associate (MTA) (Basic Certification)
- Microsoft Certified Solutions Associate (MCSA)
- SANS Training

Tools Used (Example List)

- LINUX
- CISA
- UNIX
- Cisco
- TCP/IP
- Oracle
- Virtual Private Network (VPN)
- Nmap (Network Mapper)
- Kali Linux
- Metasploit
- Netstat
- Ping
- Tracert
- Nessus
- Libwhisker
- Splunk
- Snort
- IPS
- IDS
- WireShark

Other Relevant Foundation Competencies

1	Reading Comprehension
2	Critical Thinking
3	Complex Problem Solving
4	Speaking
5	Active Listening
6	Writing
7	Time Management
8	Judgment and Decision Making
9	Systems Analysis
10	Active Learning
11	Monitoring
12	Management of Personnel Resources
13	Systems Evaluation
14	Negotiation
15	Service Orientation
16	Social Perceptiveness
17	Coordination
18	Operation Monitoring
19	Quality Control Analysis
20	Instructing
21	Persuasion
22	Operations Analysis
23	Learning Strategies
24	Programming
25	Technology Design

Other Relevant Occupation-Specific Competencies

1	Information Security
2	General Networking Tools and Concepts
3	LINUX/UNIX
4	Network Protocols
5	Core Operating Systems
6	Systems Design and Implementation
7	Office Machines
8	Tech Support
9	General Database
10	Auditing
11	System Administration
12	IT/Hardware
13	Microsoft Office
14	Software Administration
15	General Data Techniques
16	Business Process and Analysis
17	Scripting
18	Regulation and Law Compliance
19	Risk Management
20	Server Administration
21	Engineering Activities
22	Network Administration
23	Core Coding Languages
24	Telecommunications
25	Basic Web Development Languages

skillful.com