

Information Security Analyst

Job Description

Position Information

Position Title	Information Security Analyst
Position Number	
Department	Information Technology Service
Reports to (Title)	Director of Information Security
Seated Employee	

Employee First Name

Employee Last Name

Job Summary
In three to five sentences, please briefly describe the job's primary purpose to the department.

Job Summary

This position is responsible for: · Tier 1 information security ticket handling, resolution, or escalation · Supporting the College's information security team with an emphasis on monitoring security assets for vulnerabilities or potential incidents. · Supporting the evaluation and remediation of day-to-day alerts from Information security tools in place · Reviewing daily threat intelligence. · Supporting the management and maintenance of security tools with an emphasis on Security Information and Event Monitoring (SIEM) tools. · Maintaining baseline configuration standards · Maintaining controls related to operational risk management for the Grinnell College Systems Security Plan (SSP). · Assisting with the review of technical deployments for risk prior to deployment across the campus. · Working with the Lead Analyst to assist with the vulnerability management process and produce metrics to support the program

Position Summary Information

Select the level of education needed to successfully accomplish the essential duties of this job.

Associate's degree or equivalent from two-year college or technical school

If a specific degree, certification, license, or registration is necessary, please list.

N/A

Select the level of experience needed to successfully start the position and accomplish the essential duties of this job.

One year or more

Preferred Qualifications

Associate's degree from two-year college or university or equivalent experience relevant to this position

Preferred / beneficial:

- Membership and participation in professional cyber security organizations
- GIAC Security Essentials (GSEC); Certified Ethical Hacker (CEH); Microsoft Technology Associate (MTA) Security Essentials; CompTIA Security +

Knowledge and Experience

- Experience working in an Information Security environment as either an Analyst or similar position (including as a Penetration Tester).
- Experience working in a technical environment in either Network Engineering, Systems Administration, Application Development, or support of database management.
- Knowledge of Network, System and Application Security best practices.
- Ability to analyze complex and often fast-moving situations to bring alternative scenarios to the Information Security team to present options for remediation of risks.

Personal Attributes

- Exceptional analytical abilities.
- Strong written and oral communication skills.
- Excellent technical support documentation skills.
- Ability to conduct research into relevant topics, standards, and processes as required.
- Ability to present ideas in user-friendly language.
- Self-motivated and -directed.
- Keen attention to detail.

FLSA Category	Exempt
Staff/Faculty	Staff
Employment Status	Full-Time
Employment Category	Regular
Essential Staff (emergency situations)?	No
On-Call?	No

Essential Responsibilities

List the job's most important responsibilities. There are probably no more than six of these. Also indicate the approximate percent of time spent on each job function. (Note: Do not record how the job responsibilities are carried out.)

Essential Responsibility percentage of time needs to equal 100%

Responsibility	Perform Information Security risk evaluations
	• Evaluate risk for new systems, applications, and data repositories. • Perform routine information security system hygiene functions. • Develop standards for baseline configurations and review changes prior to systems being deployed, changed or retired. • Member of the vulnerability management program team.
Percentage Of Time	20
Responsibility	Operational Monitoring of Information systems

- Operational monitoring of information systems to assess the risk of alerts from Information Security monitoring tools.
- Review daily threat intelligence feeds to identify risks that could be associated with Grinnell College to elevate the threat to Senior Security Analyst and Director of Information Security.
- Working with Information Security team members as well as ITS and institutional colleagues to remediate any identified risks to their conclusion.
- Documenting identified risks for 'lessons learned' sessions.

Percentage Of Time 70

Responsibility Governance

- Maintains and updates the controls related to job duties in the Grinnell College Systems Security Plan (SSP) as well as any procedures related to the program.
- Provides regular metrics on the key information security areas of the department (SIEM alerts, vulnerability management results, incidents).

Percentage Of Time 10

General Responsibilities

General Responsibilities

- (1) Maintain regular attendance in accordance with department policy.
- (2) Comply with all safety policies, practices and procedures. Report all unsafe activities to supervisor and/or Human Resources.
- (3) Understand and comply with the policies of the College Staff Handbook.
- (4) Demonstrate commitment to customer service. Establish effective relationships with internal and external customers and respond to their needs.
- (5) Perform duties as a team member in a manner supportive of department and College procedures, policies and goals.
- (6) Protect confidentiality of College information.
- (7) Provide leadership to others through example and sharing of knowledge/skill.
- (8) Communicate with others in a courteous and helpful manner.
- (9) May be asked to fill positions considered essential during weather emergencies or other events requiring special staffing.
- (10) Perform other duties as assigned.

Supervisory Responsibilities

Does this job have supervisory responsibilities? No

If yes, then check all that are supervised by this position.

Supervise Student Staff No

If you supervise student staff, enter approximately how many and the total hours? (e.g., 2 students/XX hours)

Supervise Non-Exempt Staff No

If you supervise non-exempt staff please enter the number.

Supervise Exempt Staff No

If you supervise exempt staff please enter the number.

Select the level of supervision that this position provides.

Supervision Received

Select the level of supervision that this position receives from their supervisor. General supervision: routine duties are performed with minimal supervision; standard practices or procedures allow me to proceed alone at routine work; occasional check of work while in progress; work is reviewed upon completion.

Computer Operations

Please check one of the following Demonstrated use of intermediate computer operations (relational databases, and operating systems) and intermediate software packages (word processing, spreadsheet, graphics, etc.)

Travel

Please check one of the following Minimal overnight travel (up to 10%) by land and/or air.

Essential Function Analysis

Accurate identification of essential and marginal functions and the time required is important for making a variety of personnel decisions, including recruitment, hiring, performance evaluation, discipline, training and accommodation. The analysis explains the components of the job by identifying who, what, why, how much, and when.

Essential functions are those functions that individual must be able to perform either unaided or with the assistance of a reasonable accommodation. A job function may be considered essential if it meets one of the following criteria:

- the position exists for performance of the function;
- a limited number of employees can perform the function, and it, therefore cannot be reassigned;
- the function is specialized and requires certain expertise to perform it.

Many jobs will also have marginal functions. Marginal functions are those that may be performed by the position but are not tasks critical to job success, can be completed in a number of ways by a variety of people, and are not the primary functions for which the position exists.

Mental/Cognitive Requirements

How much on-the-job time is spent in the following mental/cognitive activities? Show the amount of time by checking the appropriate boxes below.

Analyzing information or data Over 2/3

- Essential or Marginal? Essential

Effective communication skills Over 2/3

- Essential or Marginal? Essential

Composing & comprehending communication materials Over 2/3

- Essential or Marginal? Essential

Establishing effective interpersonal Over 2/3

relationships

- Essential or Marginal? Essential

Adjusting to changes (work load, environment, department structure, etc.) Over 2/3

- Essential or Marginal? Essential

Using logic to define problems, collect information, establish facts, draw valid conclusions, etc Over 2/3

- Essential or Marginal? Essential

Making decisions of moderate to substantial consequence 1/3 to 2/3

- Essential or Marginal? Essential

Performing mathematical calculations Under 1/3

- Essential or Marginal? Marginal

Editing reports or technical materials 1/3 to 2/3

- Essential or Marginal? Essential

Planning and organizing (work load, schedules, events, etc.) 1/3 to 2/3

- Essential or Marginal? Essential

Handle stressful, emotional and/or frustrating situations Under 1/3

- Essential or Marginal? Marginal

Working with numerous distractions Under 1/3

- Essential or Marginal? Marginal

Working under a time pressure and within timelines/deadlines Under 1/3

- Essential or Marginal? Marginal

Coordinating work with others Over 2/3

- Essential or Marginal? Essential

Handling multiple assignments and priorities 1/3 to 2/3

- Essential or Marginal? Essential

Completing work in an accurate manner Over 2/3

- Essential or Marginal? Essential

Concentrating - maintaining attention to details and task Over 2/3

- Essential or Marginal? Essential

Memory functions (remembering names, details and procedures) Over 2/3

- Essential or Marginal?

Essential

Physical Requirements

How much on-the-job time is spent in the following physical activities? Show the amount of time by checking the appropriate boxes below.

Remaining in a stationary position	Under 1/3
Traverse/move locations	1/3 to 2/3
Ascend or descend between floors	1/3 to 2/3
Reach with hands and arms	Under 1/3
Ascend or descend ladder	None
Position self to access small or restricted spaces	Under 1/3
Communicate or exchange information	Over 2/3
Detect specific flavors or odors	None

Does this job require that weight be moved or force be exerted? If so, how much and how often? Check the appropriate boxes below.

Weight lifted or force exerted: up to 10 pounds (with or without assisted device)	Under 1/3
Weight lifted or force exerted: up to 25 pounds (with or without assisted device)	Under 1/3
Weight lifted or force exerted: up to 50 pounds (with or without assisted device)	None
Weight lifted or force exerted: up to 100 pounds (with or without assisted device)	None
Weight lifted or force exerted: more than 100 pounds (with or without assisted device)	None

Please check one of the following Light physical activity performing non-strenuous daily activities.

Does this job have any essential vision requirements? Check all that apply. Close vision (clear vision at 20 inches or less)

Work Environment

How much exposure to the following environmental conditions does this job require? Show the amount of time by checking the appropriate boxes below.

Wet or humid conditions (non-weather)	None
Extreme cold (non-weather)	None
Extreme heat (non-weather)	None

Outdoor weather conditions	None
Work near moving mechanical parts	None
Work in high, precarious places	None
Air Contamination (i.e., dust, fume, smoke, toxic conditions, disagreeable odors)	Under 1/3
Toxic or caustic chemicals	None
Work with explosives	None
Risk of electrical shock	None
Vibration (i.e. operating jackhammer, impact wrench)	None
Risk of radiation	None
Confined Spaces	Under 1/3
Please check one or more of the following locations where this job would work	Well-lighted, heated and/or air-conditioned indoor setting with adequate ventilation.
How much noise is typical for the work environment of this job? Check the appropriate level below.	Moderate noise (examples: business office with computers and printers, light traffic)

Additional Information

Include any other physical, mental or environmental information that will aid in the preparation of an accurate description of this job.

Position Documents

No documents have been attached.