



Job Title:	Security Analyst II
Reports to:	Vice President, Information Technology
Employees Supervised:	No

Position Summary: The Security Analyst is responsible for the evaluation, design, and implementation of security, regulatory, and risk management policies and controls, as well as support in the configuration and maintenance of information security standards, technologies, processes, and procedures. This position coordinates, administers, monitors, and maintains the security infrastructure relative to FFIEC, SANS, Cobit, NIST, and other industry frameworks. This includes, but is not limited to, intrusion detection/prevention systems, content filtering systems, SIEM, NAC, IAM, and event management systems, antivirus, and vulnerability assessment programs. The Security Analyst will also research, propose, test and implement new technologies, tools, software, products, policies, programs, standards and procedures as well as provide training, as needed. The Security Analyst II will lead security implementation projects and support the CIO in all aspects of information security and cybersecurity functions, including incident response, cyber investigations, and forensic analysis, as appropriate.

Essential Functions:

- Evaluates cybersecurity infrastructure to assess control adequacy, identify gaps, and make recommendations for enhancing controls or remediating deficiencies.
- Responsible for security systems reviews and control enhancements for new product implementations and upgrades in conjunction with vendor specifications, regulatory requirements, and audit recommendations.
- Reviews monthly risk portfolio and security KPIs to assess overall security profile to generate security health and fitness reports and mitigation recommendations
- Documents risk areas identified from attempted intrusions/threats, and devise procedures to mitigate future intrusion attempts.
- Collaborates with TSG management to evaluate and document security software, products, and programs.
- Partners with the Systems Administrator and Network Analysts to enhance the information security posture of the Credit Union.
- Reviews and respond to risk assessments performed on the credit union's critical information and security assets.
- Works together with internal and external audit groups to monitor, respond, and document mitigation and remediation efforts.
- Analyzes reports from security vendors and determine appropriate action plans.
- Provides due diligence for evaluation and selection of new vendors, software, or hardware applications.
- Develops security standards and best practices to strengthen credit union data security.
- Works with CIO to enhance the delivery of information security awareness across all departments of the credit union.
- Monitors area notifications and correlated risk advisories from established vendors and threat advisors.
- Reviews regulatory cybersecurity guidance for appropriate actions and make recommendations for policy changes.
- Provides after-hours coverage, when necessary, for security events and incident security tasks.
- Creates metrics dashboards and reports on security initiatives and daily information security tasks.

Non-Essential Functions:

- Performs special projects and other responsibilities as assigned.

Knowledge, Qualifications, and Skills:

- **Education:** Bachelor's degree in Information Systems / Technology, Computer Science or related discipline desired. CISA, CISSIP certification highly desired; CISM, CISX optional.
- **Experience:** 4+ A minimum of 5 years' experience providing support of information systems and complex technology infrastructures. Familiarity with SOLTRA, SIEM and other correlation technology highly desirable. Knowledge of the financial services industry, regulations, and operations desired.
 - Experience with virtualization, including NAS/SAN concepts and implementations.
 - 5+ Experience with security applications such as AntiVirus, Intrusion Prevention Systems, Firewalls, Vulnerability assessment tools, SIEM, and Patch Management Systems.
 - 5+ years Information Security experience including implementing and maintaining security controls.
 - Ability to be on call for incident handling as required.
- **Skills and Abilities:** Excellent written and oral communications and cross functional project management skills required. Strong technical knowledge of information security technologies including but not limited to networks, firewalls, intrusion detection/prevention systems, security event monitoring, log management, and vulnerability assessment. Excellent problem-solving skills and ability to offer multiple solutions to technical and operational support problems and challenges. Must be a self-starter who is able to follow projects through to completion with little supervision and meet deadlines in a fast-paced environment. Advanced knowledge of FFIEC IT, NIST, COSO, ITIL, Cobit, ISO frameworks a must. Proficiency in computer applications, e.g., Microsoft Office, networking architecture, Visio, Adobe suite, advanced Gantt Charting.
- **Additional Skills:** You will bring your enthusiasm, collaborative work-style, inquisitive attitude, flexibility, creativity, focus on excellence, and overall "great-to-work-with" demeanor. Previous experience with a financial institution with basic knowledge of financial products and services a plus.
- **Travel Required:** 10% local travel required. Travel during assigned shifts requires ability to operate personal vehicle. Occasional travel to more remote locations; similar, but not limited to our Fresno branch.
- **Hours Required:** Exempt employee with a work schedule of Monday through Friday, generally 8 a.m. to 5 p.m., with alternate work schedules, as required. Hours may fluctuate to accommodate response to incident and security events.
- **Environmental Conditions:** Work is primarily performed within an enclosed office. Subject to standard background noise found in an office environment.

Physical Job Requirements: The physical demands described here are representative of those that must be met by the person in this position to successfully perform the essential functions for the position.

- **Sit, Stand, Walk:** While performing the duties of the job the person in this position is regularly required to sit, stand, walk and move about inside the office to access file cabinets, office equipment etc. The duties in this position may require travel via personal vehicle which may result in long periods of sitting.
- **Use of Hands/Fingers:** To operate a computer, computer keyboard, mouse and other office productivity machinery, such as but not limited to; a calculator, copy machine and computer printer. The person in this position is frequently required to sit and reach with hands and arms.
- **Speech/Hearing:** The person in this position frequently communicates via phone and must be able to talk/hear to employees, staff and vendors to exchange accurate information in these situations.
- **Lifting/Pulling/Carrying:** The person in this position must occasionally lift/move up to 25 lbs.



**PACIFIC SERVICE
CREDIT UNION**

- Bending/Kneeling: The person in this position occasionally moves to retrieve items for use in daily work activities.

Approved by:

Date Approved: