baytechIT
HEALTHCARE FOCUSED. IT MINDED.

JOB DESCRIPTION: Security Analyst

Company Overview

Keeping patients healthy is their specialty. Healthcare IT is ours. We strive to make technology invisible and allow our clients to spend as much time with their patients as possible. We never forget that it's not about bits and bytes but about how it all helps to make a patient smile, a loved one be reassured, and a caregiver feel confident. We manage IT services for health systems, medical practices, clinics, and social service non-profits so technology works for them, and not the other way around.

Employee Value Proposition

Handing a stethoscope to an auto mechanic doesn't make him a doctor. Anyone can "fix" a problem but it takes a specialist to diagnose, heal, and implement change for the long-term. At baytechIT, we understand healthcare, business, and technology (in that order).

Healthcare, because there is no other Managed Service Provider that can say "that's all we do."

Business, because we understand it all has to do with managing IT to make an organization more profitable, save them more money, or make them more efficient.

Technology, because we've designed and managed some of the most advanced healthcare IT networks on the planet and can back up our work by offering the only "thirty day out clause" in the industry.

For *us*, it's all about being one of *them*. Everything we say and everything we do must be about becoming a client's IT partner. An employee would never think about telling the boss that "it's not in my job description." They might think about it, but if they say it, it'll probably be the last thought they have as the door shuts behind them.

If we're going to *be* their IT department then we have to *act* like it. That means no in scope and out of scope arguments. That means always doing what we think is best for them knowing that if we put ourselves first, they can show us that door at any time and for any reason.

We'll never compete on price because no one offers more for one monthly fixed fee.

We're the experts but they're always right. If they're not, we listen and offer alternatives. No one likes a preacher (except in church).

The only attitude we carry with us is gratitude. We never forget that the lifeblood of every healthcare organization is technology. They've entrusted it to us. That's a responsibility we'll never take lightly.

baytechIT
HEALTHCARE FOCUSED. IT MINDED.

Title
Security Analyst

Location
Western Massachusetts, National - Remote

Role Description
Looking to make a difference?

If you put people first, love technical solutions that make people smile, and believe that good people can do great things, then come work for baytechIT.

This position reports to the Director of Operations and is responsible for assisting our clients in maintaining administrative, physical and technical information security safeguards that strengthen their information system posture.

Under general guidance of the client's CISO, our security analyst will:

- Conduct incident response investigations
- Work with client management and Human Resources to ensure appropriate and consistent corrective action
- Help identify opportunities for improvement
- Maintain policies and procedures that are designed to be operationally effective and efficient
- Maintain workforce training programs and awareness communications
- Monitor compliance to policies, laws, and regulations.

Overall, the security analyst works with members of the client IT team to select and deploy technical controls to meet specific security requirements and defines processes and standards to ensure that security configurations are maintained.

To be successful, you'll expected to bring your working knowledge of security frameworks such as HIPAA, NIST, ISO or other industry standards that are relevant to healthcare.

Our team is comprised of committed individuals that understand that every action they take impacts the health and well-being of our community. We seek to partner with our customers, becoming trusted advisors to all aspects of their business. We are looking for someone that can tell that story and lay the groundwork for successful partnerships that will last years.

Passion for people, comfort in a varied work environment, patience, and sense of calm among competing priorities are key attributes of your personality. You enjoy working on complex problems that lack obvious answers and are not afraid to innovate and experiment.

Qualifications and Education Requirements

- Minimum 5 years in an IT technical role, preferably in healthcare
- Minimum three years in an IT Security role
- Working knowledge of:
    - Security reporting tools
    - Internal controls & IT Risk Assessment and Mitigation procedures.
    - HIPAA, Massachusetts 201 CMR 17.00, and ISO 27002:2005
- Current experience with security-related technologies such as Active Directory, encryption, remote access, anti-virus systems, etc.
- Security+ certification
- Bachelor's Degree or equivalent preferred
- Demonstrable knowledge of healthcare workflows and the role technology plays
- Security certification from a nationally recognized institution. Examples include:
    - Certified Information Systems Security Professional (CISSP)
    - Computer Hacking Forensic Investigator (CHFI)
    - GIAC Security Experrt (GSE)
    - CompTIA Ceybersecurity Analyst (CySA+)

Primary Job Requirements

- Conduct investigations of suspected security and privacy incidents, whether intentional or unintentional.
- Organize, document and report investigation results within the organization.
- Coordinate investigations with client clinical and administrative departments including Human Resources, client department management, Security, Corporate Compliance, Administration, and others as needed.
- Monitor and test application and network activity for assurance that systems of controls are in place and effective, and for compliance to client policies as well as state and federal regulations.
- Utilize security/system reporting tools such Rapid7, ProofPoint, McAfee DLP, Splunk, etc. to assist in incident response investigations, monitoring security effectiveness and analyzing the output to suggest security improvements.
- Assist with identifying, designing and implementing information security projects, provide subject matter expertise to other client IT department teams and ensuring that IT division project plans include appropriate security activities.
- Assist with developing security training, awareness reminders and related communications.
- Assists other department members advising client security administrators on normal and exception-based processing of security authorization requests.
- Assists other client security department members planning and conducting penetration testing and vulnerability assessments.

Additional Job Expectations

- Assist with monitoring, assessing and suggesting enhancements to client's business continuity and recovery programs.
- Assist with developing and publishing information security policies, procedures, standards and guidelines based on knowledge of best practices and compliance requirements along with processes that enable implementation.
- Assist with risk assessments of information and technology systems by conducting accurate and thorough assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of client's information and technology systems.
- Assist with conducting periodic evaluations of technical and non-technical security safeguards to demonstrate and document compliance with client's security policy and the requirements of the HIPAA Security Rule as required by HIPAA.
- Assist other security department members working with client departments to identify requirements, using methods that may include risk and business impact assessments.
- Assist other security department members working with security leadership to develop strategies and plans to enforce security requirements and address identified risks.
- Assists other security department members advising in application development or acquisition projects to assess security requirements and controls and to ensure that security controls are implemented as planned.
- Assists other client security department members monitoring data loss prevention.
- Assists other client security department members define security configuration and operations and standards for security systems and applications, including policy assessment and compliance tools, network security appliances and host-based security systems.
- Assist in researching new threats and vulnerabilities and mitigating administrative, physical and technical safeguards.

Skills

- Familiar with implementation of Technical information systems, especially Active Directory
- A basic knowledge of the 10 domains of the Common Body of Knowledge for information security:
    1. Access Controls
    2. Telecommunications & Network Security
    3. Information Security & Risk Management
    4. Application Security
    5. Cryptography
    6. Security Architecture
    7. Operations Security
    8. Business Continuity Planning
    9. Regulations & Compliance
    10. Physical & Environmental Security

- Ability to work well in a team environment. Values information sharing, but recognizes situations requiring confidentiality.
- Effective interpersonal, organizational, and administrative, communication and presentation skills, both oral and written.
- Effective analytical/troubleshooting skills and ability to multi-task.
- Effective negotiation and conflict management skills.
- Experience in dealing effectively with people at different levels.
- Self-motivated and able to work with little or no guidance.Ability to develop practical knowledge of malware prevention/detection technologies, handling techniques and patch deployment.
- Familiar with implementation of application or technical information systems
- Ability to work well in a team environment. Values information sharing, but recognizes situations requiring confidentiality.
- Effective interpersonal, organizational, and administrative, communication and presentation skills, both oral and written.
- Effective analytical/troubleshooting skills and ability to multi-task.
- Effective negotiation and conflict management skills.
- Experience in dealing effectively with people at different levels.
- Self-motivated and able to work with little or no guidance.
- Works independently demonstrates initiative when presented with complex problems
- Ability to work well in a team-based, fast paced/multitasking environment.
- Tracks and maintains current records of all work, including future planning
- Respond knowledgeably & in a manner understandable to the customer with regards to questions or technical enquiries.

Additional Notes

- Assesses own strengths and weaknesses; Pursues training and development opportunities; Strives to continuously build knowledge and skills; Shares expertise with others
- Approaches others in a tactful manner; Reacts well under pressure; Treats others with respect and consideration regardless of their status or position; Accepts responsibility for own actions; Follows through on commitments.

Click Here to Apply