JOB DESCRIPTION: Security Operations Analyst

Dell SecureWorks is a market leading provider of world-class information security services with over 2,800 clients worldwide spanning North America, Latin America, Europe, the Middle East and the Pacific Rim. Organizations of all sizes, including more than ten percent of the Fortune 500, rely on Dell SecureWorks to protect their assets, improve compliance and reduce costs. The combination of strong client service, award-winning security technology and experienced security professionals makes Dell SecureWorks the premier provider of information security services for any organization. Positioned in the Leader's Quadrant of Gartner's Magic Quadrant for MSSPs, Dell SecureWorks has also won SC Magazine's "Best Managed Security Service" award for 2006, 2007, 2008 & 2009.

POSITION SUMMARY

Security Analysts perform real-time log analysis to provide network and data security for Dell SecureWorks client leveraging Dell SecureWorks' Sherlock technology platform. Analysts provide excellent client service while evaluating the type and severity of security events by making use of packet analyses, and an in-depth understanding of exploits and vulnerabilities. Resolve client issues by taking the appropriate corrective action, or following the appropriate escalation procedures. Document all client communications. Work in a team environment and monitor the health and wellness of security devices on our client's networks.

Preferred Technical Experience:

- Significant experience with Linux, TCP/IP, UNIX, NT, IP Routing
- Firm understanding of regular expressions
- Understanding of database structure and queries
- Understanding of basic network services, vulnerabilities and attacks
- Good knowledge of NDIS platforms, as well as exploits and vulnerabilities

Essential Duties & Responsibilities

- Respond to inbound phone and electronic requests for technical assistance with Dell SecureWorks products
- Manage all customer situations in a professional manner with emphasis on customer satisfaction
- Configuration and troubleshooting of Dell SecureWorks iSensor and associated infrastructure
- Assess incident severity and escalate to the next level as needed
- Keep customers abreast of changes in status during issue resolution
- Set clear expectations and provide timely follow-up to customers as appropriate
- Utilize internal guidelines for effective call processing and escalation and client service
- Interact with network intrusion detection devices and other security systems via proprietary and commercial consoles, both local and remote

Additional Responsibilities

- Must be able to manage customer accounts and confidently communicate technical information to Dell SecureWorks client base
- Maintain keen understanding of evolving Internet threats to ensure the security of Dell SecureWorks Client networks
- Learn prerelease products in the area(s) of support responsibility in order to support them when released
- Write technical articles for internal knowledge base
- Participate in knowledge sharing with other analysts and develop customer solutions efficiently
- Coordinate or participate in individual or tem projects to ensure quality support for our clients
- Perform other essential duties as assigned

Knowledge, Skills, & Abilities

- Must have strong written and verbal communication skills
- Customer Service background and good written and verbal communication skills
- Cisco Security Agent experience is a plus
- Attention to detail and great organizational skills
- Good interpersonal, and organizational skills, as well as phone and customer service skills
- Ability to maintain focus while performing in depth log analysis

Education and Experience:

- Bachelor's Degree or equivalent in Computer/Electrical Engineering or Computer Science or equivalent work experience.

Desirable:

- three or more of experience as Network Intrusion Analyst
- Experience / Knowledge of Cisco NIDS devices
- Experience / Knowledge of Cisco Security Agents, Cisco Pix , ASA or CheckPoint Firewalls desirable
- Experience / Knowledge of variety of Intrusion Detection platforms
- Experience with VPN, SSL, other encryption methodology / technology a plus

Certifications Desired

- CCNA, CCSP, CSPFA Certifications a plus
- GIAC, GCIA, GCIH, GCFW, GHTO, GSEC or similar certification desirable