PERSONA

Dan

SECURITY OPERATIONS CENTER MANAGER

- Employed at a 1,000+ employee organization
- Mid-career with three or more years in current role
- BS in electrical engineering, information systems, Computer Science, IT systems administration or related field
- May have professional certifications like CEH, CISSP, GSEC/GCED
- Strong experience with DLP, SIEM, IDS/IPS, WAFs, and familiarity with different attack tools, vulnerability management and threat intelligence
- Reports to the CISO, and security analysts report to him. Keep in mind that reporting structure may vary by company size and type
- Participates in discussions and provides input on purchasing decisions

> " On top of keeping my organization safe from attacks, I'm also responsible for making sure my team is effective, that they're engaged, and that they're equipped with the latest tools."

PROTECTWISE™

JOB ROLE

- Ensure analysts maintain investigative and response consistency across different geographies.
- Develops, implements, and manages a strategic infosec monitoring and operations program and policies.
- Acts as the primary point of contact for investigations and executive reporting.
- Leads incident response on behalf of the security operations team.
- Implements processes and methods for assessing and addressing threats.
- Provides direction with defining, developing, and managing SecOps.
- Manages SoC's hiring and its budget to ensure costs align with expectations.

ALTERNATE TITLES

Cybersecurity Operations Manager, Head of Data Monitoring & Loss Prevention, Data Center Operations Manager, Computer Incident Response Team (CIRT) Manager

MOTIVATIONS

- Ensuring proper response to alerts in the security environment.
- Avoiding my organization becoming the next Target or Home Depot.
- Being around other talented security professionals, working with bleeding edge technology, finding evil.
- Setting myself up to be considered for similar roles or opportunities for advancement elsewhere.

GOALS

- Ensure the team efficiently resolves events and meets SLA requirements for fast resolution of issues. .
- FProactively find and neutralize vulnerabilities and threats proactively.
- Motivate security team to meet its goals, and to improve mythe team'sir job satisfaction.

FRUSTRATIONS

- I feel the most pain from the talent gap, and am fighting fires constantly.
- Time is precious, so I probably don't want to hear a sales or marketing pitch—just tell me what the product actually does.
- I'm under tremendous pressure to keep corporate data secure amidst increasing attacks and tighter budgets.
- Existing products lack integration, so they can only offer a limited view into some network segments.
- Finding skilled security talent is hard to find, and it's even harder to keep engaged.
- May suffer from large churn rate.
- Probably has been burned by security vendors before.
- If running a 24/7/365 shop, logistics and staffing are extremely stressful.

MORE ABOUT DAN

Dan's job performance relies on his commitment to incorporate security into daily decisions he makes. That means prioritizing and triaging events at a rapid pace, and often without the number of resources he needs to be as effective as he'd like. He's keenly aware of the career goals and job frustrations of his analysts that, if left unaddressed, can cause turnover and disruption to his team.

FOR INTERNAL USE ONLY

©2017 ProtectWise, Inc. All rights reserved.

1601 Wewatta St • Suite 700 • Denver, CO 80202 • 1.303.625.6802
www.protectwise.com • info@protectwise.com
20170511