Flyer

Professional Services

Grow Security Experts

Train your IT personnel to protect your critical assets with the Micro Focus Security Intelligence & Operations Consulting (SIOC) Analyst Development Program

Train and Retain

Training and retaining security experts that are in high demand is an integral piece of any security operations organization. Micro Focus recognizes this need and has developed an analyst training program that prepares an analyst to be fully capable of operational security without immediate supervision. Areas covered in the development program include:

- Intrusion analysis
- Information security principles (defense and offense)
- Network (TCP/IP) foundations
- UNIX, Windows
- Security tools and research

SOC Analyst Development Program

The basic mission of security operations is to recognize and respond to critical information security events in a timely and effective manner. In the face of very high event volumes, an analyst is rapidly overwhelmed without the appropriate supporting technology and most importantly, the right training and experience to see through and eliminate noise. Because of extreme levels of competition for security talent in the market, it is critical to leverage Micro Focus SIOC's experience to train personnel with a cost-effective mix of internal training, formal classroom training, external training, and on-the-job training.

The security operations center (SOC) Analyst training program is designed to take a reasonably technical person and train them in skills required of a security operations analyst. The training program combines classroom lecture, reading assignments, research assignments, and practical exercises.

All exercises are graded and may involve multiple iterations until an acceptable product is produced by the trainee. Another area of focus for the training method is to help ensure that all analysts can effectively communicate verbally, in writing and in front of an audience.

This training is designed to challenge the analyst to conceive their own approaches and to cement their understanding of one topic before the next is started. It is critical to train analysts to learn how to operate with incomplete information as it is the most likely scenario they will face while performing security investigations.

Training Content

The typical time to complete the entire training program is approximately three months, as this training is completed while the analyst is also undergoing on-the-job training.

Areas of emphasis include:

- Analytical thinking (psychology)
- Communications (written, verbal, presentation)
- Intrusion analysis
- Information security principles
- UNIX fluency
- Windows fluency
- Network fluency
- Research skills
- Tools (Wiki, security information event monitoring (SIEM))
- Use cases and business context
- SANS training preparation

Benefits

The Analyst training program provides several benefits, including:

- Consistency in analysts and analysis
- Shared baseline for analysts
- Repeatable program that can be used with new analysts in the future (promotions, attrition, or other employee turnover)
- Baseline security intelligence skills assessment to identify or measure coverage and gaps
- Security operations job certification program (optional)

Training Plans

SIOC will create and enrich all training plans using self-study, on-site training, and on-the-job training to produce a training syllabus for security analysts. SIOC experts will track analyst progress and introduce appropriate classroom work to reinforce the lessons learned in the customer's environment. All of the training resources and plans are maintained on a collaboration server to provide repeatability, transparency, and ease of access.

Our experts generate and provide a skills proficiency matrix for the SOC analysts, identifying where strengths and development opportunities exist for each member of the analyst team so that professional and skills development activity can continue under the guidance of your security leaders.

Learn more at
www.microfocus.com/sioc