أسم البرنمح : أخصائي تحليل مراكز تشغيل الأمن السيبراني Blue Team – SOC Analyst L1

برنامج "Blue Team - SOC Analyst L1" هو برنامج تدريبي متخصص مهني يهدف إلى تأهيل المشاركين لشغل وظيفة محلل مراكز تشغيل الأمن السيبراني المستوى الأول (SOC Analyst L1) والذي يعتبر من الوظائف الأكثر طلباً في سوق العمل اليوم. يتميز هذا البرنامج بأنه فريد من نوعه، حيث يقدم تدريبًا عمليًا على سيناريوهات تحليل فعلية لاكتساب المهارات الحقيقية التي يحتاجها أي محلل مركز تشغيل الأمن السيبراني.

في إطار البرنامج، سيتعرف المشاركون على أساسيات عمل مراكز تشغيل الأمن السيبراني وكيفية العمل كجزء من فريق الدعم الأمني. سيتم تناول مواضيع مثل استخدام أدوات التحليل والرصد المتقدمة، التعامل مع التحذيرات والإنذارات الأمنية، وتقييم المخاطر والتهديدات الأمنية.

بالإضافة إلى ذلك، سيتعلم المشاركون كيفية إجراء التحليل الرقمي للحوادث الأمنية وتحديد أصلها ومدى تأثيرها على الأنظمة المستهدفة. سيتضمن البرنامج أيضاً تطبيق عملي على سيناريوهات حقيقية لاختبار مهارات المشاركين وتعزيز قدراتهم على اتخاذ القرارات الأمنية السريعة والفعّالة.

كما سيُعرّف البرنامج المشاركين بأفضل الممارسات والإجراءات القياسية المتبعة في مجال الأمن السيبراني، وذلك لضمان التعامل الأمثل مع التحديات الأمنية وحماية المنظمات من المخاطر المحتملة.

في نهاية البرنامج، سيكون المشاركون قادرين على تنفيذ جميع المهام الخاصة بعمل ال SOC Analyst L1

|  |  |
| --- | --- |
| Blue Team | **أسم البرنامج** |
| SOC Analyst L1 | **الوظيفة المؤهل لها الدارس** |
| 80 ساعة (محاضرتين أسبوعيا) | **مدة البرنامج** |
| GSOC or CompTIA CYSA+ | **الاختبار الدولي** |
| أون لاين | **تنقيذ البرنامج** |
| الرسوم 5 ألاف ريال بدلا من 10 ألاف غير شامل ضريبة القيمة المضافة بخصم 50% خلال فترة التسجيل الاولي  السعر يشمل الرخص اللازمة **بالإضافة إلى خصم 50% على رسوم الاختبار الدولي** | **رسوم البرنامج** |
| 14 يوما | **فترة السماح بالاسترداد** |
| شهادة حضور من مركز المبدعون  شهادة خبرة مهنية من انفوسيك | **شهادات البرنامج** |
| محاضر معتمد | **المحاضر** |
| أساسيات الشبكات (سيتم تخصيص أول أسبوعين في التدريب لدورة مكثفة في الأساسيات) | **المؤهلات اللازمة** |
| 15 | **عدد المعامل والسيناريوهات التي سيتم التدريب عليها** |

**Effective Security Operations: Techniques and Tools for Security Analysts**

**Module 1**: Security Data Collection

* Introduction to security telemetry
* Endpoint, network, and cloud-based sensors
* Best practices for collecting and analyzing security data

**Module 2:** Automation

* Identifying opportunities for SOAR platform and other script-based automation
* Building effective automation workflows for common SOC activities
* Freeing up time for better threat hunting and detection engineering

**Module 3**: Efficient Security Process

* Understanding the steps of a SOC or security operations team
* Keeping security operations tempo on track
* Tips and techniques for effective data generation, detection, triage, analysis, and incident response

**Module 4**: Quality Triage and Analysis

* Differentiating between typical commodity attack alerts and high-risk advanced attacks
* Conducting thorough and cognitive-bias free security incident analysis
* Tips and techniques for quickly identifying and separating true positives from false positives

**Module 5:** False Positive Reduction

* Detailed explanations, processes, and techniques to reduce false positives to a minimum
* Tips and techniques for improving alert accuracy and reducing noise

**Module 6**: SOC Tools

* Collecting, organizing, and using relevant threat data in a Threat Intelligence Platform (TIP)
* Endpoint security data collection with SIEM, EDR, or XDR
* Alert triage using data correlation and enrichment techniques
* Incident management systems for effective analysis, documentation, tracking, and metrics extraction
* Hands-on exercises for SOC tools

**Module 7:** Burnout and Turnover Reduction

* Understanding the causes and factors that lead to cyber security analyst burnout
* Tips and techniques for avoiding burnout and building a sustainable cyber defense career
* Building a long-term sustainable cyber defense career

**Module 8:** Certification

* Adding on the professional certification
* Demonstrating skill and retaining material over the long term