Cyber Defense
SOC Analyst Boot Camp

7739 | 185 Hours

המסלול שיחזיר אותך למעגל העבודה בתפקיד משודרג במהירות

JOHN BRYCE TALENT

JOHN BRYCE
תלמד הייטק. זה עובד!
a matrix company

רשות החדשנות
Israel Innovation
Authority

אודות הקורס:

אנליסט The Security Operations Center (SOC) עומד כקו הגנה קדמי מפני איומי הסייבר איתם מתמודדים ארגונים כיום. הראשונים לזהות אירוע הם האנליסטים ואנשי ה-SOC. צוות ה-SOC מבטיח שהנכסים הדיגיטליים של הארגון יישארו מאובטחים ומוגנים מפני גישה בלתי מורשית על ידי ניטור וניתוח של כמויות נתונים עצומים.

קורס זה מקנה את הכישורים והפרקטיקות הנדרשים להכשרת אנשי SOC להפעלה מקצועית ומוצלחת של מערכות SOC מודרניות. האימון מתחיל מתוך הבנה רחבה של הפונקציות השונות ב-SOC, הטכנולוגיות ועד לתרגול מעשי בזמן אמת בסביבת סימולציה וירטואלית. המטרה היא לפתח צוות אבטחה בעל ידע רב, מעשי ומיומן בארגון להתמודדות עם אבטחה ברשת על בסיס יום יומי.

ל- Analyst SOC צריך להיות כל מה שנדרש בכדי להגן על מערכות ה- IT המשתנות בתדירות גבוהה. SOC כולל מגוון עצום של טכנולוגיות איתור ומניעה מתוחכמות, דיווח מודיעין סייבר וגישה לכוח העבודה המתרחב במהירות של אנשי IT מוכשרים. מטרת המודול המתקדם בקורס היא יישום פתרון SOC ולספק הנחיה מלאה בנוגע לכישורים והנהלים הדרושים להפעלתו. הקורס יקנה למשתתפים את כל ההיבטים הדרושים לצוות SOC בכדי לשלב את כלל הידע והיכולות שנרכשו במהלך ההכשרה.

מסלול זה מקנה ידע בהגנה על תשתיות הארגון על ידי ניטור נתונים וזיהוי פעילויות חשודות על ידי שילוב של הבנה מעמיקה, תרגול והתמודדות עם תרחישים.

קהל יעד

- מועמדים המבקשים להשתלב בצוותי SOC ולהתמקצע בעולמות ההגנה כגון פורנזיקה וחקירת אירועי סייבר
- אנשי מחשבים בעלי רקע ברשתות תקשורת נתונים ואבטחת מידע אשר מעוניינים להרחיב את יכולותיהם.

תנאי קדם

- ראיון אישי / ייעוץ להכוונה מקצועית
- הכרות טובה עם עולם המחשבים והאינטרנט
- ידע בסיסי בתקשורת נתונים (TCP/IP) ותשתיות מחשוב (בסביבת Microsoft ו/או Linux/Unix)
- אנגלית טכנית ברמה טובה (קריאה והבנה)
- מעבר בחינת התאמה

היקף ומתכונת הקורס

- 185 שעות לימוד אקדמיות
- לימודי בוקר, 4 פעמים בשבוע 9:00-16:30 + מפגש שבועי של למידה/תרגול עצמאי וביצוע משימות.
- הלימודים אינם מתקיימים בחגים ומועדים
- חלק מהשיעורים בקורס יכול שיועברו במסגרת למידה מקוונת (live session). המכללה שומרת לעצמה את הזכות להעביר עד 10% משעות הלימוד בקורס במסגרת למידה מקוונת כאמור.

המכללה שומרת לעצמה את הזכות לערוך שינויים בתנאים הנוגעים לקורס על מנת להתאים את הלימודים לנסיבות שאינן בשליטתה. לרבות באמצעות שינוי מקום הלימוד, שינוי מועד פתיחת הקורס, החלפת מתכונת הלימוד ללימודים מקוונים, ו/או הקפאת הלימודים בקורס והמשכם לאחר חלוף הנסיבות שדרשו זאת ו/או כל שינוי אחר שיידרש לאור נסיבות שאינן בשליטת המכללה כאמור. בקרות נסיבות כאמור, המכללה תבחר ותיישם כל שינוי שידרש בהתאם למיטב שיקוליה המקצועיים.

זכאות לתעודת סיום:

על מנת להיות זכאי לקבלת תעודות גמר מטעם מכללת ג'ון ברייס יש לעמוד הדרישות הבאות:

- נוכחות ב 90% מן המפגשים לפחות
- הגשת כל המטלות הניתנות ע"י המדריך
- השתתפות ועמידה בבחינות פנימיות של המסלול

פרוט תכני הקורס

Module Title	Hours
Introduction • Introduction to Hardware • Introduction to Networking • Virtualization • Windows Operating System	35
Part 1 - Network Research • Introduction to Linux • Networking • Introduction to Network Forensics • Cyber Security	50
Part 2 - SOC Analyst • Case Investigation • Advanced Network Analysis • Intrusion Detection and Mitigation	50
Part 3 - SOC Analyst Advanced • Windows Domain • Setting Up the SOC Environment • Using the SIEM	50
Ongoing project	
Total	185

Module Title	Module Description
Part 1: Network Research	
Module 1: Introduction to Linux	Students will study the Linux OS fundamentals. This module uses Linux commands, manipulating text and command outputs, understanding terminal-emulators, permissions, and other security concepts. **Virtualization** • Introduction to Virtualization • About Linux Distro • Installing Linux • Working with VMWare • Bridged vs. NAT **Working with Linux** • Linux Directories • Linux Users • Packages • File Manipulation Commands • Text and File Manipulation Technics • Writing Linux Scripts
Module 2: Networking	During this module, participants will study network infrastructures, common network types, network Layers, communication between protocols, communication between network devices from different Layers, and network anonymity methods. **Protocols and Services** • TCP/IP and OSI Model • Network Routing Basics • DNS • DHCP • ARP • Remote Connection Protocols **Wireshark – Diving into Packets** • Non-Secure and Secure Packets • Filtering and Parsing • Extracting Objects and Files from PCAP Files

Module 3: Introduction to Network Forensics	Large organizations these days suffer greatly from network attacks and malicious intrusions. Those who manage the organization's network have an immense impact on ensuring its safety. This module will introduce participants to Network Forensics and learn how to locate and better understand various attacks. **Windows Tools** • NetworkMiner • Advanced Wireshark • OS-Fingerprinting • Detecting Suspicious Traffic • Sysinternals **Linux Tools** • Capture Packet Data from Live Network • Filter Packets from Live Network • Filter Packet from PCAP File • Traffic Statistics • File-Carving
Module 4: Cyber Security	This module's primary goal is to teach participants to embrace the attacker state-of-mind to recognize the necessary defense mechanisms. Participants will deal with several types of attacks. Students will learn about hash functions; furthermore, they will learn how wireless networks are attacked and how they are vulnerable to those attacks. Social engineering and honeypot techniques will also be demonstrated. **Cyber Security Vectors** • Anti-Viruses • DoS and DDoS • CNC Servers and Botnets • Steganography **Network Attacks** • Scanning Methods • MiTM • ARP Poisoning • DHCP Starvation • LLMNR Attacks • Offline Password Brute-Force • Working with Responder **Cyber Attack Practice** • Payloads: Reverse vs. Bind • Privilege Escalation

Part 2: SOC Analyst	
Module 1: Case Investigation	During this module, students will understand the challenges of investigating network-based cases. Students will practice using various tools and investigation methodologies to correlate data and collect evidence. **Advanced Wireshark** • Analyzing Domain Protocols • Working with SSL Traffic • Analyzing Wireless Connections • Enumerating Domain Network • Working with TShark **Investigation Process** • MiTM Attack • Find Network Anomalies • Flow Analysis • Network File Carving • NetworkMiner • File Carvers
Module 2: Advanced Network Analysis	During this module, participants will further explore data packets' study on a deeper level, learn to identify network anomalies, and understand system alerts. Students will master the use of well-known command-line-interface (CLI) and graphic-user-interface (GUI) tools to further specialize in the field. **Zeek** • Output Logs • Automating Process • Monitoring Data into Logs • Zeek-Cut Parsing
Module 3: Intrusion Detection and Mitigation	Students will learn how to deploy automatic data analyzers in this module, using preset rules or craft custom rulesets to alert and block suspicious traffic detection. **IPS and IDS** • Essential Intrusion Detection Tools and Methods • Installing and Configuration Sysmon • Network Events • IDS/IPS Operation Process • IDS/IPS Configuration • Snort

Part 3: SOC Analyst Advanced	
Module 1: Windows Domain	During this module, participants will create a Windows server domain, configuring the different network protocols such as DNS, DHCP, and Group Policy. **Windows Server** • Installing Windows Server • Configuring Windows Server • Managing Features **Windows Domain** • Installing AD DS • Configuring AD DS • Managing Domain Protocols • Working with Group Policy
Module 2: Setting Up the SOC Environment	Companies regularly deploy various security technologies designed to prevent and detect threats and strengthen and protect assets. During this module, we will detail SOC environments and how they work. The student will know to build and properly configure his SOC environment and correlate it with other security products/assets. Having a SOC allows you to have dynamic security that acts as a real bastion of analysis, monitoring, prevention, and remediation. **Preparing the Framework** • Introduction to ELK • Deploying Beats • Identifying Threats • Aggregating Data • Real-Time Monitoring **Hands-on PfSense** • Setting and Configuring Rules • Passing Traffic using the NAT Feature • Configuring Firewall Rules • Managing Network Security • Snort

Module 3: Using the SIEM	Learning about the SIEM (Security Information and Event Management), the primary system used by SOC analysts for monitoring the network. Participants will install a freely available open-source SIEM platform and simulate different scenarios through a pre-prepared virtual environment, mimicking an organization. **Building SIEM Environment** • Configuring Your Domain • Setting-Up an Open Source SIEM • Deploying Security-Onion • Network and Host DLP Monitoring and Logging **Monitoring using the Virtual Environment** • Firewall Monitoring and Management • Email and Spam Gateway and Web Gateway Filtering • Vulnerability Assessment and Monitoring • Setting your Rules for Cyber Threats

John Bryce Online Academy

האקדמיה המקוונת של ג'ון ברייס מציעה לתלמידים מגוון רחב של קורסי Online בלמידה עצמית כהשלמה ממוקדת לתחום הנלמד. בנוסף לשעות הלימוד בכיתה, התלמידים יקבלו גישה לקורסים מקוונים הממוקדים לחיזוק והעמקת הידע בהתאם להמלצותיו של המנהל המקצועי של המסלול.

ג'ון ברייס טאלנט

יחידת השירות המנוהל (Outsourcing) של ג'ון ברייס הדרכה, מכשירה, משלבת ומנהלת עובדים רבים בחברות המובילות במשק בכלל ובחברות הייטק בפרט.

בפעילות הטאלנט אנו בונים Boot Camps ייעודיים על פי צרכי השוק וצרכי הלקוחות השונים.
לפעילות זו באמצעות מבחני סינון ומיון קפדניים אנו מאתרים את התלמידים המוכשרים ביותר ובעלי המוטיבציה הגבוהה ביותר להשתלב בשוק העבודה.
יכולת הליבה שלנו היא לזקק את התלמידים הטובים ביותר ולהקנות להם ידע בכל תחומי הפיתוח, אבטחת מידע, סייבר, תשתיות, בדיקות ועוד, כך שיתאימו כמו כפפה לארגון בו יתחילו לעבוד.
בזכות תוכנית זו ג'ון ברייס מעמידה בוגרים מצוינים אשר מספקים תמורות ותפוקות איכותיות בצורה מהירה ובהצלחה.
חשוב לנו לתמוך ככל האפשר ולכן בהמשך הדרך אנו דואגים לחניכה , הכשרות נוספות, מעקב ובקרה צמודים, כל זאת ועוד במטרה להוריד את עקומת הלימוד, הגדלת התפוקות ואיכותן ושילוב המועמד במסגרת העבודה שלו בזמן הקצר ביותר.

הריני מאשר שניתנה לי ההזדמנות לעיין במסמך זה

שם:_____ ת.ז:_____
חתימה:_____ תאריך:_____

עדכון אחרון בסילבוס בוצע בתאריך 10/10/2021

*6460

www.johnbryce.co.il

עקבו אחרינו

JOHN BRYCE TALENT

JOHN BRYCE
תלמד הייטק. זה עובד!
a matrix company

רשות החדשנות
Israel Innovation Authority