يشمل هذا الكتيّب التعريفي قسمًا باللغة العربية أيضاً

MicroSmart
Corporate for Innovation and Recruitment

Applied Cybersecurity & SOC Operations

MicroSmart is a Private Limited Company (Ltd.), established in February 2019, specializing in competency-based training for individuals, capacity building for organizations, and the provision of IT and business solutions. The company operates with a strong focus on customer excellence and empowering entrepreneurship and business development.

Training Program 2026

THIS PROGRAM IS DESIGNED FOR THOSE WITH AMBITION, COMMITMENT, AND A DRIVE TO SHAPE THEIR FUTURE

MicroSmart Core Values:

turn ideas into action and challenges into opportunities.

Passion fuels our drive, inspires our creativity.

act with honesty, openness, and impartiality.

Our business is an open book, with every page reflecting transparency and credibility

Gaza – Omar Al-Mukhtar Street – opposite Gaza Municipality Park – Gardens Building – Sixth Floor.

Click here to contact us via WhatsApp

Click here to visit our website

Integrated training milestones to build your competence in Applied Cybersecurity & SOC Operations.

MicroSmart
Corporate for Innovation and Recruitment

Course Modules:

Module 1:
Foundations & Lab Setup (6 Hours)

- Cybersecurity fundamentals and threat landscape.
- Lab environment setup (virtual machines, tools).
- Basic Linux and networking for security.

Module 2:
Networking & Traffic Analysis (8 Hours)

- TCP/IP, DNS, HTTP/S fundamentals.
- Packet analysis using traffic capture tools.
- Detecting suspicious network behavior.

Incident Response

Module 3:
Operating Systems Security (9 Hours)

- Windows and Linux security fundamentals.
- System logs and event analysis.
- Basic system hardening practices.

Module 4:
Cyber Threats & Attack Techniques (10 Hours)

- Malware, phishing, brute-force, and DoS attacks.
- MITRE ATT&CK framework.
- Mapping real attacks to adversary techniques.

Threat Detection

Module 5:
SOC Operations & SIEM (12 Hours)

- SOC structure, roles, and workflows.
- SIEM concepts and alert lifecycle.
- Log ingestion, detection rules, and investigations.
- Incident documentation and reporting.

Vulnerability Assessment

Module 6:
Incident Response & Digital Forensics (8 Hours)

- Incident response lifecycle.
- Evidence collection and analysis.
- Timeline reconstruction and reporting.

Module 7:
Capstone Project – SOC Simulation (12 Hours)

- End-to-end SOC simulation.
- Attack detection, investigation, and response.
- Final technical report and presentation.

Compliance and Risk

The best time to start is always now.

Training Approach:
Competency-based, project-based, hands-on.

MicroSmart
Corporate for Innovation and Recruitment

The course adopts a hybrid methodology, combining:

- Hands-on Based Learning: Every session includes practical labs and exercises.
- Competency-Based Training: Each module is mapped to measurable cybersecurity skills.
- Project-Based Learning: A capstone project simulates real SOC operations from attack detection to incident reporting.

This approach ensures participants acquire applied skills, not just theoretical understanding.

Meet the Trainer

HAZEM EL BAZ

Accredited By MicroSmart

Assistant Professor Candidate – Cyber Security | LLM & Anomaly Detection Expert | Building AI-Driven SOC Automation Solutions

PhD, Computer and Network Security.
Master, Computer and Network Security – Cryptography

LinkedIn
For more details, click here

The course is designed for:

Primary Target Group:

- University students specializing in Cybersecurity, Computer Science, or Information Technology.
- Fresh graduates seeking practical cybersecurity experience.

Secondary Target Group:

- IT and Network professionals transitioning into cybersecurity.
- Individuals interested in starting a career in cybersecurity operations.

Prerequisites:

- Basic knowledge of networking and operating systems.
- No prior SOC experience required.

A future where creativity knows no limits, as technology empowers everyone with the strength tools. It's about enabling individuals to shape their surroundings.

MicroSmart
Corporate for Innovation and Recruitment

Training hours:
A total of (65) training hours, (4) hours per session, over (16) training sessions.

Training Cost:

- Option 1: In-House Training (Face-to-Face) includes (65) training hours held in a physical training hall, at a fee of (385$). This covers refreshments, venue costs, and other operational expenses
- Option 2: Blended Training includes (40) hours of in-house training and (25) hours of online training, at a fee of (280$).
- Option 3: Online Training includes (65) hours of fully online training, at a fee of (155$).

Training Time and Location:
Time: Training sessions are scheduled based on the preferences of the trainees to ensure maximum engagement and benefit.

Place: The training venue is selected to best suit the geographical distribution of the trainees, aiming to accommodate the largest possible number based on their place of residence.

The priority will be given to early applicants.

SEATS LIMITED

Register now easily from here

Test & Performance Assessment:

- The trainer's observations of each trainee's performance and engagement with practical activities are taken into account.
- Practical lab performance.
- Scenario-based assessments.
- Incident investigation reports.
- Final capstone project presentation
- The trainee's commitment to attendance (based on the required percentage), active participation, and timely submission of assignments and the final project will impact the final evaluation.

Ready For the Competition?

Benefits and Privileges:

1. The trainee will be awarded a MicroSmart-certified certificate with a QR code for verification, indicating the final performance level (Excellent, Very Good, Good, Acceptable), based on commitment, participation, project quality, and assessments.
2. The top two trainees will be rewarded for their excellence: The first-place trainee will receive a full (100%) refund of the course fee, while the second-place trainee will receive a partial refund of (50%).
3. Outstanding trainees may be selected for paid freelance tasks with MicroSmart or be invited to join the team if relevant opportunities arise.

Click the icon to preview the certificate you will receive upon completion.

MicroSmart
Corporate for Innovation and Recruitment

Expected Training Outcomes (Competency-Based):

WE DON'T JUST TRAIN, WE UNLOCK YOUR POTENTIAL AND TURN IT INTO REAL-WORLD SUCCESS

Knowledge Level:

Participants will be able to:

1. Understand cybersecurity fundamentals, modern threats, and layered defense concepts.
2. Know the structure and roles of a Security Operations Center (SOC) and the incident management lifecycle.
3. Be familiar with essential cybersecurity tools such as SIEM systems, intrusion detection/prevention systems (IDS/IPS), and packet analysis tools.
4. Understand the MITRE ATT&CK framework and common attack techniques (e.g., phishing, malware, DoS attacks).
5. Know networking and operating system security fundamentals (Windows/Linux) for investigative purposes.
6. Understand digital forensics principles and proper legal methods of evidence collection.

Skill Level:

Participants will be able to:

1- Analyze Network Traffic:
- Use tools such as Wireshark to analyze packets and identify suspicious activities.

2- Monitor Logs and Alerts:
- Configure and use SIEM tools (e.g., Splunk, Elastic Stack) to monitor logs and create detection rules.

3- Investigate Security Incidents:
- Analyze alerts, trace attacker activity, and determine the scope and severity of incidents.

4- Respond to Common Attacks:
- Apply initial response procedures for phishing, malware, and DDoS attacks.

5- Document and Report:
- Prepare clear and detailed incident reports, including response steps and recommendations.

6- Simulate Full SOC Operations:
- Execute a practical project simulating a real SOC environment from detection to reporting.

Attitude & Behavior Level:

Participants will be able to:

1- Adhere to Professional Ethics and Integrity:
- Handle data and systems with confidentiality and responsibility during investigations.

2- Work in a Team and Communicate Effectively:
- Communicate clearly with security teams and management during incident response.

3- Apply Critical and Analytical Thinking:
- Analyze complex scenarios and make data-driven decisions quickly.

4- Commit to Continuous Learning:
- Keep up with emerging threats and new technologies in cybersecurity.

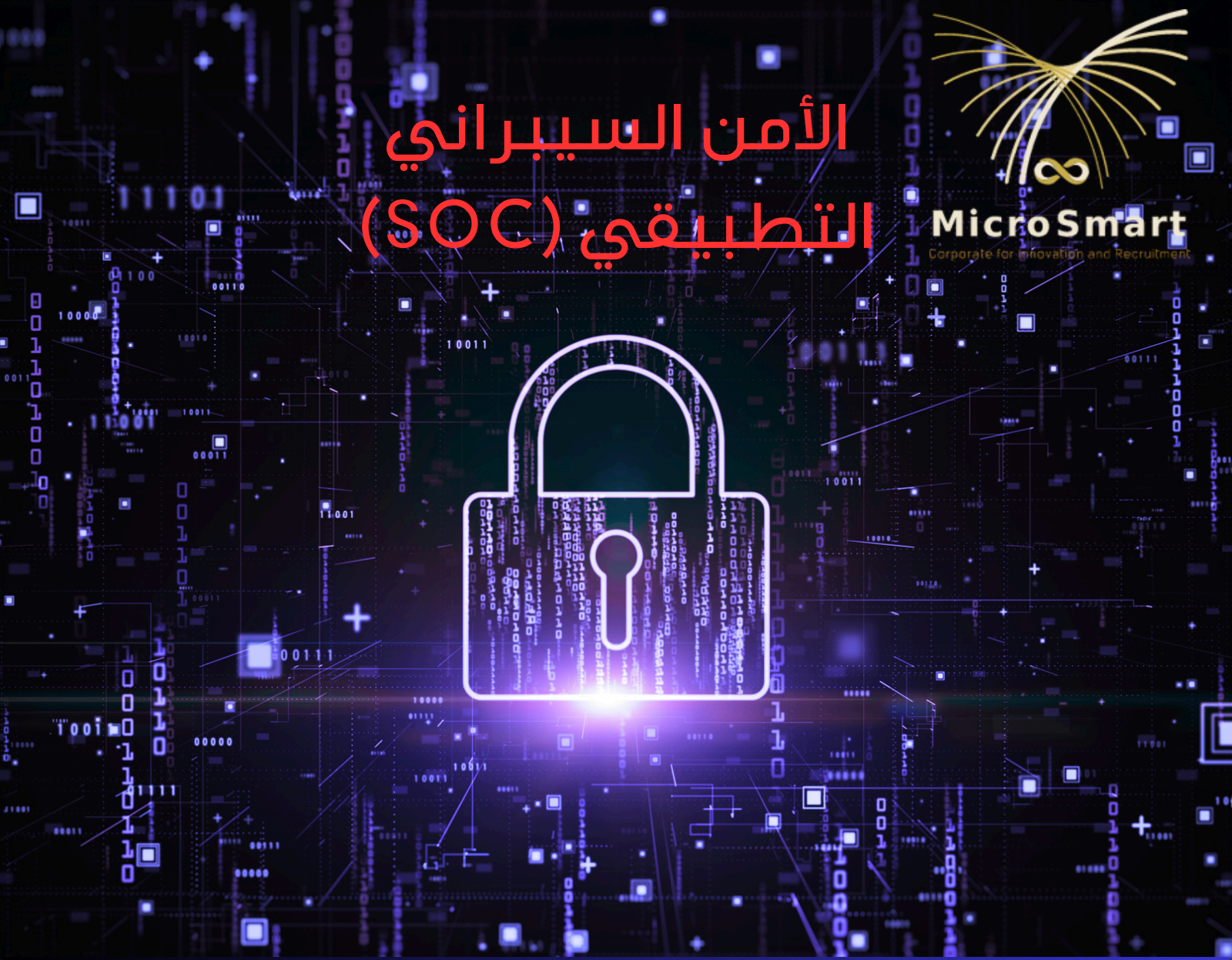
5- Remain Calm Under Pressure:
- Manage security incidents in an organized and calm manner, even in critical situations.

6- Take Responsibility and Be Transparent:
- Report errors, learn from them, and improve security processes.

Register now easily from here

MicroSmart's mission is to consistently create meaningful opportunities for those who truly deserve them

الأمن السيبراني التطبيقي (SOC)



ميكروسمارت شركة خصوصية محدودة، تأسست في فبراير 2019، متخصصة في التدريب القائم على الكفاءة للأفراد، وبناء قدرات المؤسسات، وتقديم حلول تقنية المعلومات والأعمال. تعمل الشركة برؤية تركز على التميز في خدمة العملاء، وتمكين ريادة الأعمال.

برنامج التدريب 2026

هذا البرنامج مخصّص لأولئك الذين يملكون الطموح والالتزام والعزيمة لصنع مستقبلهم

القيم الأساسية لميكروسمارت:

نحوّل الأفكار إلى إنجاز، والتحديات إلى فرص.

الشغف يُشعل دافعنا ويُلهم إبداعنا.

نتصرّف بأمانة وشفافية وحيادية.

أعمالنا كتاب مفتوح، تعكس كل صفحة منه الشفافية والمصداقية.

اضغط هنا لزيارة موقعنا الإلكتروني

اضغط هنا للتواصل عبر واتساب

غزة - شارع عمر المختار - مقابل منتزة بلدية غزة - عمارة الجاردنز - الطابق السادس

MicroSmart
Corporate for Innovation and Recruitment

محطات تدريبية متكاملة لبناء كفاءتك في الأمن السيبراني التطبيقي (SOC)

وحدات الدورة التدريبية:

Incident Response

الوحدة 1: الأساسيات وإعداد المعمل (6 ساعات)
- أساسيات الأمن السيبراني ومشهد التهديدات.
- إعداد بيئة المعمل (الآلات الافتراضية، الأدوات).
- أساسيات لينكس والشبكات للأغراض الأمنية.

الوحدة 2: الشبكات وتحليل حركة المرور (8 ساعات)
- أساسيات بروتوكولات TCP/IP و DNS و HTTP/S.
- تحليل الحُزم باستخدام أدوات التقاط حركة المرور.
- كشف السلوك المشبوه على الشبكة.

الوحدة 3: أمن أنظمة التشغيل (9 ساعات)
- أساسيات أمن ويندوز ولينكس.
- تحليل سجّلات الأنظمة والأحداث.
- ممارسات أساسية لتأمين وتحصين الأنظمة.

- الوحدة 4: التهديدات السيبرانية وتقنيات الهجوم (10 ساعات)

Threat Detection

- هجمات البرمجيات الخبيثة، التصيد، القوة الغاشمة، وحرمان الخدمة (DoS).
- إطار عمل MITRE ATT&CK.
- ربط الهجمات الحقيقية بتقنيات المهاجمين.

الوحدة 5: عمليات مركز العمليات الأمنية (SOC) وأدوات SIEM (12 ساعة)
- هيكل مركز العمليات الأمنية، الأدوار، وسير العمل.
- مفاهيم SIEM ودورة حياة التنبيهات.
- استيعاب السجّلات، قواعد الكشف، والتحقيقات.
- توثيق الحوادث وإعداد التقارير.

Vulnerability Assessment

الوحدة 6: الاستجابة للحوادث والتحقيق الرقمي (8 ساعات)
- دورة حياة الاستجابة للحوادث.
- جمع الأدلة وتحليلها.
- إعادة بناء الخط الزمني وإعداد التقارير.

الوحدة 7: المشروع النهائي – محاكاة مركز العمليات الأمنية (12 ساعة)
- محاكاة شاملة لمركز العمليات الأمنية من البداية للنهاية.
- كشف الهجمات والتحقيق فيها والاستجابة لها.
- التقرير الفني النهائي والعرض التقديمي.

Compliance and Risk

أفضل وقت للبدء هو الآن

MicroSmart
Corporate for Innovation and Recruitment

منهجية التدريب: قائم على الكفاءة، ومبني على المشاريع، ويعتمد على التطبيق العملي.

التعلم القائم على التطبيق العملي: حيث تتضمن كل جلسة معامل عملية وتمارين تطبيقية.

التدريب القائم على الكفاءة: حيث يتم ربط كل وحدة بمهارات قابلة للقياس في مجال الأمن السيبراني.

التعلم القائم على المشاريع: من خلال مشروع نهائي يتيح محاكاة عمليات مركز العمليات الأمنية الحقيقية بدءاً من اكتشاف الهجوم ووصولاً إلى إعداد تقارير الحوادث.

تعرف على المدرب

حازم الباز

محرب معتمد من قبل ميكروسمارت

مرشح أستاذ مساعد – الأمن السيبراني | خبير في نماذج اللغة الكبيرة والكشف عن الشذوذ | بناء حلول أتمتة مراكز العمليات الأمنية المعتمدة على الذكاء الاصطناعي

.الدكتوراه، أمن الحاسوب والشبكات
الماجستير، أمن الحاسوب والشبكات
– التخصص في التشفير.

Linked in

لمزيد من التفاصيل اضغط هنا

الدورة موجهة إلى

الفئة الأساسية:

- طلاب الجامعات المتخصصون في الأمن السيبراني، علوم الحاسوب، أو تكنولوجيا المعلومات.
- الخريجون الجدد الباحثون عن خبرة عملية في مجال الأمن السيبراني.

الفئة الثانوية:

- المتخصصون في تقنية المعلومات والشبكات الراغبون في التحول إلى مجال الأمن السيبراني.
- الأفراد المهتمون ببدء مسار مهني في عمليات الأمن السيبراني.

المتطلبات المسبقة:

- معرفة أساسية بالشبكات وأنظمة التشغيل.
- لا يشترط وجود خبرة سابقة في مركز العمليات الأمنية (SOC).

خطوة واحدة اليوم قد تغيّر مستقبلك بالكامل... لا تنتظر، ابدأ الآن

MicroSmart
Corporate for Innovation and Recruitment

ساعات التدريب:

(65) ساعة تدريبية، بواقع (4) ساعات للجلسة الواحدة، على مدار (16) جلسة تدريبية.

سعر الدورة:

- الخيار الأول: تدريب وجاهي داخل قاعة التتدريب، يتضمن (65) ساعة تدريبية في قاعة التدريب، بسعر (385$)، يشمل الضيافة، القاعة، التكاليف التشغيلية الاخرى.
- الخيار الثاني: تدريب مدمج يتضمن (40) ساعة وجاهي، و(25) ساعة عن بُعد، بسعر (280$).
- الخيار الثالث: تدريب عن بُعد يتضمن (65) ساعة تدريبية عبر الانترنت، بسعر (155$).

وقت ومكان التدريب:

الوقت: يتم تحديد مواعيد التدريب بما يتناسب مع تفضيلات المتدربين لضمان أعلى درجات التفاعل والاستفادة.

المكان: يُختار موقع التدريب بما يتناسب مع التوزيع الجغرافي للمتدربين، وذلك لتسهيل الوصول وخدمة أكبر عدد ممكن وفقاً لمناطق سكنهم.

SEATS LIMITED

المقاعد محدودة، وستُمنح الأولوية حسب أسبقية تقديم طلب التسجيل.

سجّل الآن بسهولة من هنا

اختبار وتقييم الأداء:

- ملاحظات المدرب: تقييم أداء كل متدرب ومدى تفاعله مع الأنشطة العملية.
- الأداء في المعامل العملية: تقييم المهارات التطبيقية أثناء الجلسات العملية.
- تقييمات قائمة على السيناريوهات: اختبار قدرة المتدرب على التعامل مع حالات مشابهة للواقع.
- تقارير تحقيقات الحوادث: تقييم منهجية التحليل والتوثيق في تقارير الحوادث.
- عرض المشروع النهائي: تقييم العرض التقديمي للمشروع التطبيقي الشامل (Capstone Project).
- العوامل المؤثرة في التقييم النهائي: التزام المتدرب بالحضور (وفقًا للنسبة المطلوبة)، المشاركة الفعالة أثناء الجلسات، التسليم في الموعد المحدد للواجبات والمشروع النهائي.

جاهز للمنافسة؟

الفوائد والامتيازات

1. يُمنح المتدرب شهادة معتمدة من ميكروسمارت مزوّدة برمز QR للتحقق، توضح مستوى الأداء النهائي (ممتاز، جيد جدًا، جيد، مقبول)، بناءً على الالتزام، المشاركة، جودة المشروع والتقييمات.
2. يُمنَحُ أَفْضَلُ مُتَدَرِّبَيْنِ مكافأةً على تميّزِهما، حيثُ يَحصُلُ الأَوَّلُ على استردادٍ كامِلٍ (100٪) من رَسْمِ الدَّوْرَةِ، بينما يَحصُلُ الثّاني على استردادٍ جُزْئِيٍّ (50٪).
3. قد يتم اختيار المتدربين المتميزين لأداء مهام عمل مدفوعة الأجر مع ميكروسمارت، أو يتم دعوتهم للانضمام إلى الفريق إذا توفرت الفرص المناسبة.

أضغط على الأيقونة لمعاينة الشهادة التي ستتسلمها بعد إتمام الدورة التدريبية.

MicroSmart
Corporate for Innovation and Recruitment

المخرجات التدريبية المتوقعة (المبنية على الكفاءة):

نحن لا نقدم تدريبًا فحسب، بل نطلق العنان لقدراتك ونحولها إلى نجاح حقيقي في العالم الواقعي.

مستوى المعرفة:

سيتمكن المشاركون من:

1. فهم أساسيات الأمن السيبراني، التهديدات الحديثة، ومفاهيم الدفاع متعدد الطبقات.
2. معرفة هيكل وأدوار مركز العمليات الأمنية (SOC) ودورة حياة إدارة الحوادث.
3. الإلمام بأدوات الأمن السيبراني الأساسية مثل أنظمة SIEM، وأنظمة كشف ومنع التسلل (IDS/IPS)، وأدوات تحليل الحزم.
4. فهم إطار عمل MITRE ATT&CK وتقنيات الهجوم الشائعة (مثل التصيد الاحتيالي، البرمجيات الضارة، هجمات حجب الخدمة DoS).
5. معرفة أساسيات أمن الشبكات وأنظمة التشغيل (Windows/Linux) لأغراض التحقيق.
6. فهم مبادئ التحقيق الجنائي الرقمي والطرق القانونية السليمة لجمع الأدلة.

مستوى المهارات:

سيتمكن المشاركون من:

1. تحليل حركة مرور الشبكة:
   - استخدام أدوات مثل Wireshark لتحليل الحزم وتحديد الأنشطة المشبوهة.
2. مراقبة السجلات والتنبيهات:
   - تكوين واستخدام أدوات SIEM (مثل Splunk، Elastic Stack) لمراقبة السجلات وإنشاء قواعد الكشف.
3. التحقيق في الحوادث الأمنية:
   - تحليل التنبيهات، وتتبع أنشطة المهاجم، وتحديد نطاق وشدة الحوادث.
4. الاستجابة للهجمات الشائعة:
   - تطبيق إجراءات الاستجابة الأولية لهجمات التصيد الاحتيالي والبرمجيات الضارة وهجمات حجب الخدمة الموزع (DDoS).
5. التوثيق وإعداد التقارير:
   - إعداد تقارير حوادث واضحة ومفصلة تتضمن خطوات الاستجابة والتوصيات.
6. محاكاة عمليات SOC كاملة:
   - تنفيذ مشروع عملي يحاكي بيئة SOC حقيقية بدءاً من الاكتشاف وحتى الإبلاغ.

مستوى السلوك والموقف:

سيتمكن المشاركون من:

1. الالتزام بأخلاقيات المهنة والنزاهة:
   - التعامل مع البيانات والأنظمة بسرية ومسؤولية أثناء التحقيقات.
2. العمل ضمن فريق والتواصل بفعالية:
   - التواصل بوضوح مع فرق الأمن والإدارة أثناء الاستجابة للحوادث.
3. تطبيق التفكير النقدي والتحليلي:
   - تحليل السيناريوهات المعقدة واتخاذ قرارات سريعة مدعومة بالبيانات.
4. الالتزام بالتعلم المستمر:
   - مواكبة التهديدات الناشئة والتقنيات الجديدة في مجال الأمن السيبراني.
5. الحفاظ على الهدوء تحت الضغط:
   - إدارة الحوادث الأمنية بطريقة منظمة وهادئة حتى في الظروف الحرجة.
6. تحمل المسؤولية والشفافية:
   - الإبلاغ عن الأخطاء والتعلم منها لتحسين العمليات الأمنية.

رسالة ميكروسمارت الاستمرار في خلق فرص ذات معنى لأولئك الذين يستحقونها حقًا

سجّل الآن بسهولة من هنا