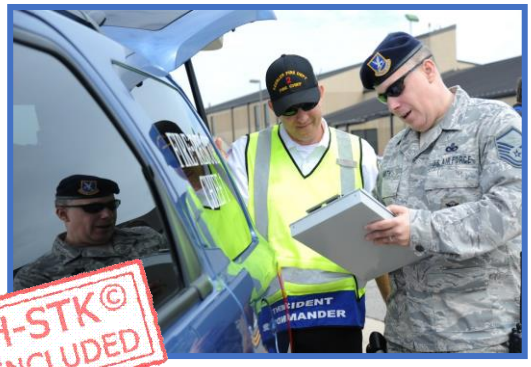
COURSE OVERVIEW DM0007
Security Incident Investigation and Management

Course Title
Security Incident Investigation and Management



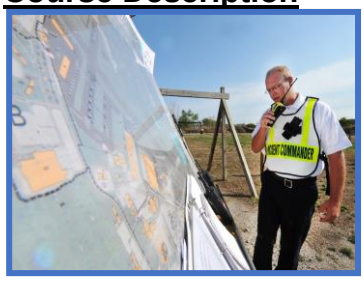
Course Date/Venue
Session 1: August 04-08, 2024/The Kooh Al Noor Meeting Room, The H Dubai Hotel, Sheikh Zayed Rd - Trade Centre, Dubai, UAE

Session 2: September 22-26, 2024/The Kooh Al Noor Meeting Room, The H Dubai Hotel, Sheikh Zayed Rd - Trade Centre, Dubai, UAE

Course Reference
DM0007

Course Duration/Credits
Five days/3.0 CEUs/30 PDHs

Course Description



This practical and highly-interactive course includes real-life case studies and exercises where participants will be engaged in a series of interactive small groups and class workshops.

This course is designed to provide participants with a detailed and up-to-date overview of Security Incident and Management Investigations. It covers the types of security incidents and the stages in incident management including preparation, identification, containment, eradication, recovery and lessons learned; the roles within an incident response team and their responsibilities; building a strong foundation for incident management through proactive measures; the tools and technologies used in incident response and legal and compliance aspects related to security incidents; and the various signs of security incidents and the techniques used for detection.

Further, the course will also discuss the threat intelligence to identifying potential threats and vulnerabilities; the importance of log files in incident detection and how to analyze them; monitoring and analyzing network traffic for signs of unauthorized activity; how to prioritize incidents based on their impact and severity; the effective strategies for initial response to a detected incident; developing and implementing an incident response plan; the proper techniques and best practices for containing an incident and the steps for removing

the threat from the environment; the forensic analysis in the context of incident response; and the proper documentation and evidence handling techniques during an incident.

During this interactive course, participants will learn the effective communication strategies with stakeholders during an incident; the strategies for system and data recovery post-incident; conducting a post-incident review to analyze the response and improving future procedures; extracting lessons and sharing knowledge within the organization for improvement; revising and updating incident response plans based on recent incidents and lessons learned; the role of cyber insurance and legal considerations post-incident; focusing on team wellbeing and stress management post-incident; the advanced persistent threats (APTs) and special considerations for incident response in cloud environments; the emerging threats and future trends in cybersecurity; and the alignment of incident response with business continuity and disaster recovery planning.

Course Objectives

Upon the successful completion of this course, each participant will be able to:-

- Apply and gain an in-depth knowledge on security incident management and investigations
- Recognize the types of security incidents and the stages in incident management including preparation, identification, containment, eradication, recovery and lessons learned
- Define the roles within an incident response team and their responsibilities
- Build a strong foundation for incident management through proactive measures
- Recognize the tools and technologies used in incident response and discuss the legal and compliance aspects related to security incidents
- Identify various signs of security incidents and the techniques used for detection
- Utilize threat intelligence to identify potential threats and vulnerabilities and discuss the importance of log files in incident detection and how to analyze them
- Monitor and analyze network traffic for signs of unauthorized activity and how to prioritize incidents based on their impact and severity
- Apply effective strategies for initial response to a detected incident and develop and implement an incident response plan
- Implement proper techniques and best practices for containing an incident and the steps for removing the threat from the environment
- Carryout forensic analysis in the context of incident response including proper documentation and evidence handling techniques during an incident
- Apply the effective communication strategies with stakeholders during an incident and the strategies for system and data recovery post-incident
- Conduct a post-incident review to analyze the response and improve future procedures
- Extract lessons and share knowledge within the organization for improvement
- Revise and update incident response plans based on recent incidents and lessons learned

- Discuss the role of cyber insurance and legal considerations post-incident and focus on team wellbeing and stress management post-incident

- Recognize the advanced persistent threats (APTs) and special considerations for incident response in cloud environments
- Discus the emerging threats and future trends in cybersecurity as well as align incident response with business continuity and disaster recovery planning

Exclusive Smart Training Kit - H-STK®

*Participants of this course will receive the exclusive "Haward Smart Training Kit" (**H-STK®**). The **H-STK®** consists of a comprehensive set of technical content which includes **electronic version** of the course materials, sample video clips of the instructor's actual lectures & practical sessions during the course conveniently saved in a **Tablet PC**.*

Who Should Attend

This course provides an overview of all significant aspects and considerations of security incident and management investigations for law enforcement agents, digital forensics experts, military police officers, private investigators, information technology specialists and other technical staff who are tasked with responding to incidents of cybercrime.

Training Methodology

All our Courses are including **Hands-on Practical Sessions** using equipment, State-of-the-Art Simulators, Drawings, Case Studies, Videos and Exercises. The courses include the following training methodologies as a percentage of the total tuition hours:-

30% Lectures
20% Practical Workshops & Work Presentations
30% Hands-on Practical Exercises & Case Studies
20% Simulators (Hardware & Software) & Videos

In an unlikely event, the course instructor may modify the above training methodology before or during the course for technical reasons.

Course Fee

US$ 5,500 per Delegate + **VAT**. This rate includes H-STK® (Haward Smart Training Kit), buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Accommodation

Accommodation is not included in the course fees. However, any accommodation required can be arranged at the time of booking.

Course Certificate(s)

Internationally recognized certificates will be issued to all participants of the course who completed a minimum of 80% of the total tuition hours.

Certificate Accreditations

Certificates are accredited by the following international accreditation organizations: -

- The International Accreditors for Continuing Education and Training (IACET - USA)

  Haward Technology is an Authorized Training Provider by the International Accreditors for Continuing Education and Training (IACET), 2201 Cooperative Way, Suite 600, Herndon, VA 20171, USA. In obtaining this authority, Haward Technology has demonstrated that it complies with the **ANSI/IACET 2018-1 Standard** which is widely recognized as the standard of good practice internationally. As a result of our Authorized Provider membership status, Haward Technology is authorized to offer IACET CEUs for its programs that qualify under the **ANSI/IACET 2018-1 Standard**.

  Haward Technology's courses meet the professional certification and continuing education requirements for participants seeking **Continuing Education Units** (CEUs) in accordance with the rules & regulations of the International Accreditors for Continuing Education & Training (IACET). IACET is an international authority that evaluates programs according to strict, research-based criteria and guidelines. The CEU is an internationally accepted uniform unit of measurement in qualified courses of continuing education.

  Haward Technology Middle East will award **3.0 CEUs** (Continuing Education Units) or **30 PDHs** (Professional Development Hours) for participants who completed the total tuition hours of this program. One CEU is equivalent to ten Professional Development Hours (PDHs) or ten contact hours of the participation in and completion of Haward Technology programs. A permanent record of a participant's involvement and awarding of CEU will be maintained by Haward Technology. Haward Technology will provide a copy of the participant's CEU and PDH Transcript of Records upon request.

- British Accreditation Council (BAC)

  Haward Technology is accredited by the **British Accreditation Council** for **Independent Further and Higher Education** as an **International Centre**. BAC is the British accrediting body responsible for setting standards within independent further and higher education sector in the UK and overseas. As a BAC-accredited international centre, Haward Technology meets all of the international higher education criteria and standards set by BAC.

Course Instructor(s)

This course will be conducted by the following instructor(s). However, we have the right to change the course instructor(s) prior to the course date and inform participants accordingly:

Lieutenant Colonel Nayel Sarayreh is a **Senior Security Expert** in **Defence**, **Security & Military Management** with over **30 years** of extensive experience in **Accident/Incident Investigation** & **Root Cause** Analysis, Strategic **Security** Management, **Security Risk** Management, **Security Threat** Identification, **Risk Analysis** Evaluation & Management, **Security** Systems, **Security Inteligence**, **Security** Operations Management, **Investigation & Security Surveying**, **Security Crisis** Management, **Security Investigations & Criminal** Evidence, **Incident Investigation** Techniques, **Incident Root Cause** Analysis, **Root Cause Failure** Analysis, Effective Investigations, Administrative Investigations, **Emergency** Response & Preparedness, **Disaster** Management Strategies, **Emergency** Management Skills, **Disaster** Mitigation & Recovery, **Emergency** Communication & Response, **Corporate Security** Planning, **Safety** Protocols & Security Measures, **Disaster** Recovery, **Crisis** Management, **Risk** Management, **Risk Analysis** Evaluation & Management, **Investigation & Security Surveying**, **Security Crisis** Management, **Corporate Security** Planning, Advanced **Security**, **Strategic** Analysis, **Systems** Analysis & Design, **Strategy** Selection & Implementation, **Security** Policies & Procedures, Violence, Terrorism & Security, Counterterrorism, **Civil** Conflict, Anti-riot & Riot Control, **Rehabilitation & Correction**, **Corporate Legal Advising**, **Law**, **Mediation**, **Arbitration**, **Litigation & Legal** Risk, **Investigation**, **Prosecution & Execution** and **Human Rights** Etiquette & Protocol.

During his service, Lieutenant Colonel Nayel had been served as the **General Prosecutor**, **Chief** of **Judicial Section**, **Chief** of **Security**, **Commander**, **Deputy Commander**, **Police Advisor**, **Civil Defense Officer**, **Police Officer**, **Intelligence Officer**, **Crisis Communication & Emergency Response Specialist**, **Internal Investigator**, **Security Specialist**, **Rehabilitation & Correction Officer**, **Investigation Officer**, **Security Expert**, **Security Management Consultant** and **Senior Instructor/Trainer** from the various international organizations such as the United Nations, UNHCR, Jordan Police and Diplomatic Security Unit which is responsible of all embassies, ambassadors and residences, just to name a few.

Lieutenant Colonel Nayel has a **Bachelor's** degree in **Law**. Further, he is a **Certified Instructor/Trainer**, a **Certified Trainer/Assessor** by the **Institute of Leadership & Management** (**ILM**) and has delivered numerous trainings, workshops and conferences and projects worldwide.

Course Program

The following program is planned for this course. However, the course instructor(s) may modify this program before or during the workshop for technical reasons with no prior notice to participants. Nevertheless, the course objectives will always be met:

Day 1

0730 – 0800	*Registration & Coffee*
0800 – 0815	*Welcome & Introduction*
0815 – 0830	***PRE-TEST***
0830 – 0930	***Introduction to Security Incidents:*** *What Constitutes a Security Incident, Types of Security Incidents (Cyberattacks, Data Breaches, Insider Threats, etc.)*
0930 – 0945	*Break*
0945 – 1030	***Incident Management Lifecycle:*** *The Stages in Incident Management (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned)*
1030 – 1130	***Roles & Responsibilities:*** *Defining the Roles Within an Incident Response Team and their Responsibilities*
1130 – 1215	***Preparation & Prevention Strategies:*** *Building a Strong Foundation for Incident Management Through Proactive Measures*
1215 – 1230	*Break*
1230 – 1330	***Key Incident Management Tools & Technologies:*** *Introduction to Tools & Technologies Used in Incident Response (SIEM, IDS/IPS, EDR, etc.)*
1330 – 1420	***Regulatory & Compliance Considerations:*** *The Legal & Compliance Aspects related to Security Incidents (GDPR, HIPAA, etc.)*
1420 – 1430	***Recap***
1430	*Lunch & End of Day One*

Day 2

0730 – 0830	***Incident Detection Techniques:*** *Identifying Various Signs of Security Incidents & the Techniques Used for Detection*
0830 – 0930	***Threat Intelligence:*** *Utilizing Threat Intelligence to Identify Potential Threats & Vulnerabilities*
0930 – 0945	*Break*
0945 – 1100	***Log Management & Analysis:*** *The Importance of Log Files in Incident Detection & How to Analyze Them*
1100 – 1215	***Network Traffic Analysis:*** *Techniques for Monitoring & Analyzing Network Traffic for Signs of Unauthorized Activity*
1215 – 1230	*Break*
1230 – 1330	***Incident Prioritization:*** *How to Prioritize Incidents Based on their Impact & Severity*
1330 – 1420	***Initial Response Strategies:*** *Effective Strategies for Initial Response to a Detected Incident*
1420 – 1430	***Recap***
1430	*Lunch & End of Day Two*

Day 3

0730 – 0830	***Incident Response Planning:*** *Developing & Implementing an Incident Response Plan*
0830 – 0930	***Containment Strategies:*** *Techniques and Best Practices for Containing an Incident*
0930 – 0945	*Break*

0945 – 1100	***Eradication Techniques:*** *Steps for Removing the Threat from the Environment*
1100 – 1215	***Forensic Analysis:*** *Introduction to Forensic Analysis in the Context of Incident Response*
1215 – 1230	*Break*
1230 – 1330	***Documentation & Evidence Handling:*** *Proper Documentation and Evidence Handling Techniques During an Incident*
1330 – 1420	***Communication During Incidents:*** *Effective Communication Strategies with Stakeholders During an Incident*
1420 – 1430	***Recap***
1430	*Lunch & End of Day Three*

Day 4

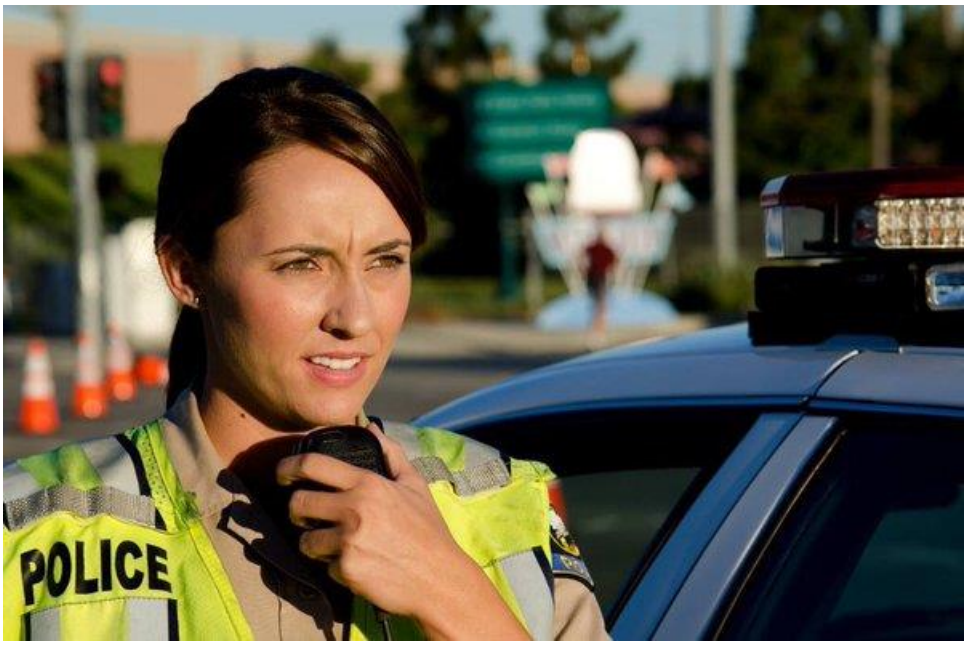
0730 – 0830	***Recovery Processes:*** *Strategies for System and Data Recovery Post-Incident*
0830 – 0930	***Post-Incident Review:*** *Conducting a Post-Incident Review to Analyze the Response and Improve Future Procedures*
0930 – 0945	*Break*
0945 – 1100	***Lessons Learned & Knowledge Sharing:*** *Extracting Lessons & Sharing Knowledge within the Organization for Improvement*
1100 – 1215	***Updating Incident Response Plans:*** *Revising & Updating Incident Response Plans Based on Recent Incidents & Lessons Learned*
1215 – 1230	*Break*
1230 – 1330	***Cyber Insurance & Legal Considerations:*** *The Role of Cyber Insurance & Legal Considerations Post-Incident*
1330 – 1420	***Stress Management & Team Wellbeing:*** *Focusing on Team Wellbeing & Stress Management Post-Incident*
1420 – 1430	***Recap***
1430	*Lunch & End of Day Four*

Day 5

0730 – 0830	***Advanced Persistent Threats (APTs):*** *Understanding & Responding to APTs*
0830 – 0930	***Tabletop Exercises:*** *Conducting Tabletop Exercises for Simulated Incident Response Scenarios*
0930 – 0945	*Break*
0945 – 1100	***Incident Response in Cloud Environments:*** *Special Considerations for Incident Response in Cloud Environments*
1100 – 1230	***Emerging Threats & Future Trends:*** *Discussion on Emerging Threats and Future Trends in Cybersecurity*
1230 – 1245	*Break*
1245 – 1300	***Integration with Business Continuity Planning:*** *Aligning Incident Response with Business Continuity and Disaster Recovery Planning*
1300 - 1345	***Live Simulation Exercise:*** *Conducting a Live Simulation Exercise to Apply Learned Skills in a Real-World Scenario*
1345 – 1400	***Course Conclusion***
1400 – 1415	***POST-TEST***
1415 – 1430	*Presentation of Course Certificates*
1430	*Lunch & End of Course*

Practical Sessions

This practical and highly-interactive course includes real-life case studies and exercises:-



Course Coordinator

Mari Nakintu, Tel: +971 2 30 91 714, Email: mari1@haward.org