Advanced Cybersecurity Threat Management for Government Institutions Training Course



07 - 11 Dec 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #SM5862_4011

Course Introduction / Overview:

Government institutions are increasingly targeted by sophisticated cyber threats, from nation-state actors to organized crime syndicates. This training course is designed to provide public sector professionals with the advanced skills needed to protect critical data and systems. We will cover a range of topics, including threat intelligence, incident response, and vulnerability management, all with a focus on the unique challenges and regulatory requirements of the government sector. The program will equip participants with the knowledge to build a robust cyber defense framework and manage a security team. We will explore academic work by authors like Dorothy E. Denning, whose book Information Warfare and Security provides a foundational framework for understanding the national security implications of cybersecurity. The curriculum is designed to help professionals develop a strategic approach to cyber threat management, looking at cybersecurity, physical security, and risk management as an integrated whole. The BIG BEN Training Center is committed to providing a program that helps participants become the cybersecurity leaders of tomorrow, making a significant impact on their organization's resilience and success.

Target Audience / This training course is suitable for:

- Government cybersecurity managers.
- IT and network administrators.
- Public sector security analysts.
- Risk management and compliance officers.
- Senior government executives.
- Data protection officers.
- Law enforcement personnel.

Target Sectors and Industries:

- Government and public administration.
- Defense and military.
- Public utilities and infrastructure.
- Healthcare.
- Education.
- Law enforcement.
- Government agencies and their equivalents.

Target Organizations Departments:

- Information Technology (IT) and Cybersecurity.
- Internal Audit.
- Risk Management.
- Legal and Compliance.
- Public Affairs.
- Operations.
- Executive Leadership.

Course Offerings:

By the end of this course, the participants will have able to:

- Develop a comprehensive cybersecurity strategy for a government institution.
- Use threat intelligence to proactively identify and mitigate risks.
- Lead and manage a cybersecurity incident response team.
- Conduct a detailed vulnerability assessment and penetration test.
- Understand the legal and ethical aspects of government cybersecurity.
- Implement a continuous monitoring program to detect threats.
- Communicate complex cyber risks to senior management and the public.
- Ensure regulatory compliance with government mandates.

Course Methodology:

This training course uses a highly practical and immersive methodology to make sure that participants can apply what they learn in the real world. The program starts with instructor-led sessions that provide a clear understanding of the core principles of advanced cybersecurity threat management. A key component of our approach is the use of real-world case studies and simulations of major cyberattacks on government institutions. Participants will work through complex scenarios, making strategic decisions under pressure and analyzing the results. We will also use interactive workshops and group exercises where participants work together to develop a threat response plan or a mock vulnerability assessment. This collaborative model encourages teamwork and allows participants to practice their leadership skills. Instructors at BIG BEN Training Center are experienced professionals who provide personalized feedback and guidance throughout the course. Our goal is to prepare professionals to face the complex challenges of government cybersecurity. By focusing on advanced skills and a strategic mindset, we are making sure that every participant leaves the course ready to make a significant impact on their organization's resilience.

Course Agenda (Course Units):

Unit One: The Foundation of Government Cybersecurity.

- The unique threat landscape for government institutions.
- The principles of a strategic cyber defense framework.
- The role of threat intelligence and information sharing.
- The legal and ethical aspects of cybersecurity in the public sector.
- Aligning cybersecurity strategy with national security goals.

Unit Two: Threat Intelligence and Risk Assessment.

- Using threat intelligence to anticipate attacks.
- Conducting a risk assessment for government systems.
- The process of threat modeling.
- Quantifying cyber risk and its impact.
- Presenting risk findings to executive leadership.

Unit Three: Incident Response and Crisis Management.

- The stages of a cybersecurity incident response plan.
- Leading a crisis team during an attack.
- The role of forensic analysis.
- Post-incident recovery and learning.
- Communication with the media and public during a crisis.

Unit Four: Vulnerability Management and Defense.

- Conducting vulnerability assessments and penetration testing.
- The role of security hardening and patch management.
- Implementing advanced network security controls.
- The use of security information and event management (SIEM).
- Protecting sensitive data and access control.

Unit Five: Policy, Governance, and the Future.

- Developing and implementing effective cybersecurity policies.
- Ensuring regulatory compliance with government mandates.
- The future of cyber threats and countermeasures.
- The role of emerging technologies in cyber defense.
- Creating a long-term cybersecurity roadmap.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

Given the increasing sophistication of cyber threats and the need for public trust, how can a government institution build a cybersecurity program that is both highly secure and transparent to its citizens?

What unique qualities does this course offer compared to other courses?

This training course is unique because it provides an advanced and strategic approach to cybersecurity that is specifically designed for government institutions. While many courses focus on technical skills, our program places a strong emphasis on threat intelligence, incident response, and strategic management. We move beyond technical details and teach participants how to think like a security leader, making sure that cybersecurity is seen as a key component of national security and public trust. The curriculum is designed to be highly practical, with a strong emphasis on case studies and simulations that reflect real-world government challenges. We also address the legal, ethical, and public relations aspects of a cyber crisis. BIG BEN Training Center is committed to providing a program that gives professionals the knowledge and skills they need to protect their organizations and their citizens.