



Cyber Security & Risk Management

Mastering Cyber Threat Identification in the Public Sector: Tactics, Techniques, and Procedures (TTP's)

TRAINING



Facilitated by
TOM BIGOS, CISSP
Certified Information Systems Security
Professional

Online

Modules 1 - 3: Tuesday, September 12, 2023

Modules 4 - 6: Tuesday, September 19, 2023



PUBLIC
SECTOR
NETWORK



Certified
B
Corporation

Cyber risks are now top of mind for the public sector, here digital has increased potential for sabotage. It is critical to have a thorough understanding of the tactics, methods, and procedures (TTPs) employed to defend against these threats.

Mastering Cyber Threat Identification: Tactics, Techniques, and Procedures (TTP's) has been designed to give public sector cyber professionals the practical advice and tools necessary to recognize and effectively neutralize cyber risks. This curriculum is comprised of six highly-intensive modules designed specifically for public sector employees to help them identify and mitigate cyber threats.

If you want to efficiently identify and mitigate cyber threats, with this course, you will be better prepared to defend against online threats, preserve vital infrastructure, and safeguard sensitive data.

REGISTRATION COMING SOON



Key Learning Objectives

- Gain knowledge and skills to identify and mitigate cyber threats in your organization
- Learn about the latest tactics, techniques, and procedures used by cyber attackers
- Play a crucial role in protecting your organization from cyber attacks
- Safeguard critical infrastructure and sensitive data
- Engage in hands-on exercises and case studies to reinforce learning
- Better equipped to handle incident response planning for cyber attacks

Who Should Attend

This training course is designed for employees of public sector organizations, including government agencies and critical infrastructure providers, who are responsible for cybersecurity and risk management.; including:

IT professionals, cybersecurity analysts, incident responders, risk managers, and other personnel involved in cybersecurity operations; compliance officers, policy makers, government officials, and data protection officers

Meet Your Facilitator



TOM BIGOS, CISSP
Certified Information Systems Security
Professional

Tom is a seasoned Cyber Security veteran with over 13 years of experience in the field and more than 20 years of experience in Information Technology. Throughout his career, Tom has worked with a diverse range of clients, including law enforcement, water and power utilities, local government, manufacturing, law firms, and other businesses in both Canada and the USA. His extensive knowledge stems from hands-on, in-the-field penetration engagements and testing, giving him a unique view into the world of Cyber Security from both an attacker and defender perspective.

In addition to his professional work, Tom is passionate about education and enjoys sharing his expertise with others. He has taught students, clients, and organizations how to detect, defend, and self-attack their infrastructure to better understand the methods used by threat actors in exploiting vulnerabilities. Most recently, Tom served as the primary instructor for a 13-week college-level course, where he trained the next generation of penetration testers and ethical hackers. With his unique educational approach and experience, Tom is sure to captivate and enlighten audiences at any speaking engagement.

Preparation

This training session is highly interactive with group activities about and discussions throughout. Come prepared with some current challenges you are facing in your organization.

To participate you'll need:

- Computer with a camera and microphone
- Strong internet connection
- Quiet, well-lit space
- An open mind and readiness to engage both internally and in groups



Explore the Agenda

DAY 1 | Tuesday, September 12, 2023, 10:00am - 2:30pm ET

10:00am ET Welcome from Public Sector

10:15am ET Training Overview, Objectives and Icebreaker

10:30am ET **Module 1: Introduction to Cyber Threats and TTPs**

- Overview of common cyber threats faced by the public sector
- Introduction to TTPs and their importance in identifying and mitigating cyber threats
- Examples of recent cyber attacks on public sector organizations

11:15am ET **Module 2: Understanding Attack Vectors and Techniques**

- Overview of common attack vectors used by cybercriminals
- Analysis of common attack techniques such as phishing, social engineering, and malware attacks
- Case studies of successful cyber attacks on public sector organizations

12:00pm ET Lunch

1:00pm ET **Module 3: Mastering Threat Intelligence Analysis for Cybersecurity**

- Understanding the importance of threat intelligence in identifying and mitigating cyber threats
- Gathering and analyzing threat intelligence data
- Techniques for monitoring threat intelligence sources and identifying potential threats

1:45pm ET Break

2:00pm ET Resources, Reflection and Feedback

2:30pm ET End of Day 1

DAY 2 | Tuesday, September 19, 2023, 10:00am - 2:30pm ET

10:00am ET Welcome from Public Sector and Recap

10:15am ET **Module 4: Effective Incident Response Planning**

- Importance of having an incident response plan in place
- Developing an incident response plan specific to the public sector organization
- Conducting regular incident response training and testing

11:00am ET Break

11:15am ET **Module 5: Mastering Cybersecurity Best Practices**

- Overview of cybersecurity best practices for the public sector
- Developing strong passwords and implementing multi-factor authentication
- Recognizing and reporting phishing attempts
- Protecting sensitive data and maintaining data privacy

12:30pm ET Lunch

1:30pm ET **Module 6: Anticipating Emerging Threats and Future Trends in Cybersecurity**

- Analysis of emerging cyber threats facing the public sector
- Understanding of the future trends in cyber threats and TTPs
- Strategies for staying up-to-date and continuously improving cybersecurity measures.

2:15pm ET Resources, Reflection and Feedback

2:30pm ET End of Day 2