INTSIGHTS
Defend Forward™

Security Advisory Services Overview

www.intsights.com

Introduction

IntSights Security Advisory Services offers a broad range of seminars and courses designed to provide actionable training for all employees, including hands-on analysts, executives, and board members. Seminars, add-on modules, and Cyber Threat Intelligence (CTI) courses are taught at your facility by seasoned cybersecurity professionals, including Etay Maor and Charity Wright. Pricing for these seminars and courses is available from your sales representative.

Etay Maor is Chief Security Officer at IntSights.
As CSO, Etay leads the Security Advisory Practice at IntSights, where he works with CISOs and other senior cybersecurity executives to develop risk management-based cybersecurity programs. Maor has extensive experience in cybersecurity, having worked at IBM (X-force Cyber Range Instructor and Executive Security Advisor), Trusteer, and RSA (Head of the Cyber Threats Research Lab). Maor holds a BA in Computer Science and an MA in Counter Terrorism and Cyber Terrorism, and is an adjunct professor at Boston College.

Charity Wright is a Cyber Threat Intelligence Analyst at IntSights with over fifteen years experience with the US Army and the National Security Agency, where she translated and analysed Mandarin Chinese communications. Wright now focuses her attention on dark web cyber threat intelligence. She enjoys the dynamic threat environment of cybercriminal communication and networks, and thrives on providing relevant, timely intel to her customers at IntSights. In her current role, she frequently serves as a security expert guest writer and speaker with news outlets and publications including NBC, SecurityWeek, Dark Reading, SC Magazine, C-SPAN, and more.

Seminars & Courses

Hands-On Cybersecurity Awareness Training

Target Audience: All employees
Duration: 4 hours

This half-day seminar covers the tools, tactics, and techniques used by adversaries (from script kiddies to sophisticated cybercrime groups). We dive into identifying and understanding phishing attacks, malware, proximity-based attacks, and more. In the second part of the course, we discuss mitigation strategies. Participants are also introduced to Open Source Intelligence and will witness, first hand, how easy it is to collect data on anyone from the clear web.

Thinking Like a Cyber Criminal

Target Audience: Managers, Executives, & Board members
Seminar Duration: 1.5 hours

A shorter version of the half-day Hands-On Cybersecurity Awareness Training seminar, this session focuses on how cybercriminals think and operate. Understanding the way attackers choose, analyze, and ultimately attack their targets is crucial for today's leaders. This session is designed for executives and board members who wish to understand online privacy issues as well as data collection and defensive strategies that can be applied both pre- and post-breach.

IntSights Cyber Intelligence Ltd, 155 W 19th Street, 5th Floor New York, NY 10011
Tel: +1 (212) 729-7104 | www.intsights.com

Cyber Threat Intel (CTI) 101 & 201

Target Audience: Threat intel, SOC teams, and security leadership personnel
Duration: 4 hours per course

Cyber Threat Intel 101 and 201 are designed to meet the needs of security and threat intel practitioners.

CTI 101

One person and a Threat Intelligence Platform (TIP) does not make a threat intelligence program. Learn how to build a successful CTI program from scratch by attending this comprehensive basic course. Participants will cover many areas that pose challenges to security organizations, including how to:

- Hire the right people, structure a CTI team, train your CTI professionals
- Determine your organization's Priority Intelligence Requirements (PIRs) in part by drafting mock PIRs in a live lab
- Learn how to talk to security stakeholders (CISOs, SOC leadership) about Cyber Threat Intelligence by encouraging their participation, and involving them in the creation of PIRs
- Determine who your internal clients are throughout your organization and what they can get from your CTI program
- Explore CTI tools, maximize the use of free OSINT tools, and learn how to utilize a Threat Intelligence Platform (TIP)
- Get started using the IntSights External Threat Protection platform and services and learn analyst tips on how to make the most from your subscription
- Analyze cyber threat intelligence through SIEM integration, aggregation, enrichment of indicators, and increase visibility into threats

CTI 201

focuses on maturing your CTI program. This course will guide your team through several steps needed to mature your program, including how to effectively analyze cyber intelligence for measurable impact on your organization. Choose from the following options to accommodate the needs of your team:

- Maximize your use of the IntSights Threat Intelligence Platform (TIP).
- Explore in-depth intelligence analysis tradecraft, including analysis processes, frameworks, bias awareness, and hypothesis generation.
- Discover new Open Source Intelligence (OSINT) tools and tricks for analysis and production.
- Implement Purple Team exercises to encourage teamwork across the organization.
- Create eye-catching, relevant CTI products for internal and external customers.
- Foster a peer review culture to encourage communication, teamwork, and collaboration, and to hone writing and speaking skills.
- Learn about existing intelligence analysis frameworks and determine which best suit your organization.

IntSights Cyber Intelligence Ltd, 155 W 19th Street, 5th Floor New York, NY 10011
Tel: +1 (212) 729-7104 | www.intsights.com

Additional Modules

Duration: 45-60 minutes per module

Tour of the Dark Web
- Online anonymity
- History and underlying architecture of TOR
- Live dark web tour

Intro to Cryptography
- Review of the RSA algorithm
- Diffie-Hellman, certificates, and PKI
- From Caesar to Enigma
- Steganography

OSINT in Depth
- Recon to collection to attack
- Social engineering
- OSINT tools
- Google hacking
- Shodan and CENSYS, targeting devices

Attacks 201
- SQLi, XSS, and API attacks; supply chain, data,and integrity attacks

Hacker's Backpack – Tools
- Malicious USBs/WiFi attacks
- AP attacks

Intro to Cybercrime and Security Frameworks
- LM killchain
- MITRE ATT&CK, usage and application
- The diamond model
- Basics of phishing and malware
- How to design a phishing site
- Malware modules, deployment and operation
- Financial malware and RATs
- Ransomware, cryptojacking

Bypassing Security Tools and Procedures
- Bypassing identification
- Bypassing authentication
- Bypassing two-factor authentication
- Bypassing Device ID
- Bypassing biometrics
- Attacking AI systems

IntSights Cyber Intelligence Ltd, 155 W 19th Street, 5th Floor New York, NY 10011
Tel: +1 (212) 729-7104 | www.intsights.com