

Interactive Group Activities

- Breach notification Templates
- Before the Incident Mind Map
- After the Incident Mind Map
- Checklists
- Crown Jewels
- Process Workflows
- The Cyber Kill Chain
- Go Destroy
- Log Data Analysis
- Press Interview Scenarios
- Crisis Comms Plan
- Client and PR Communication Templates

Understanding Threat Actors

- Threat Actors in Detail
- Threat Agents Intent & Attributes
- Detection and Response Strategies

Automating Incident Management & Response

- What is incident orchestration
- Using incident orchestration to significantly reduce time to - respond to data breaches
- How to semi-automate and fully automate incident management
- Using incident orchestration to empower and up skill existing staff
- Incident orchestration as Force Multiplier
- Using orchestration to increase compliance to regulations like GDPR

Defining Normal

- Identifying Critical Systems and Assets
- Understanding and Building the Organisational Baseline
- Interactive session on applying these principles
- Strategies in understanding operational weaknesses
- Defining high level cyber response process workflows

COURSE CREATOR AND TRAINER AMAR SINGH

- UK Government GCHQ certified trainer and creator of GCHQ certified courses.
- Experienced cyber, information security and data privacy practitioner.
- Global Chief Information Security Officer, expert in information risk management.
- Mentor and trusted advisor to FTSE 100 Firms.

The Technologies

- Understanding the technologies that underpin an effective breach ready organisation.
- Analysis of core technology requirements

The Cyber Kill Chain

- Methods of Attack
- Analysis of the Cyber Kill Chain
- Review of Recent High Profile Attacks
- Strategies to counter the Cyber Kill Chain

Triage, Detection & Monitoring

- OODA Loop
- The Golden Hour
- Log Management

The Checklist

- Creating/ adopting the checklist
- Incident management checklist
- Using the check list to beat the hackers!

Intelligence Led Incident Response

- Detailed why and how
- Actionable Threat intelligence

Forensics & Investigations

- Integrity
- Forensic Principles
- Seizing Evidence

Public Relations

- Crisis Comms Plan Management
- Social Media & PR Key Steps
- PR Case Study
- Breach notification

Building the Team

- Stakeholders - Who are they?
- Legal, Compliance and Notifications



Free Download - our incident response mind map
<http://hubs.ly/H01VWvt0>

“ A really good session, the trainer is really knowledgeable and presents it in a really understandable format that the participants really enjoyed. ”

Wayne Parkes
Head of ICT, West Mercia & Warwickshire Police

“ I have to say I was very impressed with the course and its content. The day was packed full of information, examples and there was plenty of interaction between the group. ”

DCI Vanessa Smith
Yorkshire and Humberside Region Cyber Crime Team