Cybersecurity Operations

Philipp Reinecke

ReineckeP@cardiff.ac.uk

Organisation of the module

Learning Outcomes

1. Reflect on the interplay between people and technology in securing organisations.
2. Justify the selection of and implement technical and organisational security measures.
3. Articulate the importance and requirements of situational awareness.
4. Articulate the purpose and operation of a Security Operations Centre (SOC).
5. Analyse and evaluate the current and evolving threat landscape.
6. Identify and analyse legal constraints and obligations in security operations.
7. Demonstrate knowledge of intrusion-detection and intrusion-prevention systems.
8. Articulate and analyse techniques and strategies used by Advanced Persistent Threats (APTs) and how they can be detected and mitigated.
9. Perform satisfactory peer review.

Teaching

- Mix of practical and theoretical
- Not just lectures – generally interactive
  - "Flipped classroom"
  - Present
  - Discuss
- Reading & research will be required
- Guest lectures

Assessments

1. Security Operations Portfolio – 50%
2. Computerised Class Test – 40%
3. Discussion contributions/presentation – 10%
4. Peer Review – 0%

Structure (tentative)

Week	Topic
1	**Introduction** Organisation – Challenges – Resources
2	**Understanding the Problem** Users - Advanced Persistent Threats - Threat Actors Modelling Attacker Behaviour: Kill Chains, ATT&CK, TTPs, Pyramid of Pain
3	**Prevention – Making Systems Secure** Security Architectures - Zero Trust, Defence in Depth, etc.
4	**Detection I** Data Collection - IDS/IPS – Threat Intelligence
5	**Detection II** SIEMs - Security Analytics – Situational Awareness
6	**Remediation and Recovery** Methods – Approaches – Impact
7	**Security Operation Centres (SOCs)** **Offensive Security – Testing, Evaluation, Impact & Trade-offs** Guest Lectures
8	**Legal Aspects**
9	**Practical & Revision**
10	**Computerised Class Test (1.5 hours)** **Emerging Challenges I** e.g. ICS, SCADA, IoT, Cloud, (Hyper-) Converged Systems, Containers
11	**Emerging Challenges II**

Earn marks quickly:
Present!
Lead a discussion!

Send me a short abstract of your topic by the end of the week.

Session Format

1. Everybody reads the material beforehand
2. 10-15 minute presentation on topic
3. Occasional guest lecture by an expert
4. 10-15 minute discussion of topic

Earn marks slowly:
Contribute to discussion

Security Operations?

- “Cyber security refers to the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.” (UK National Cyber Security Strategy)
- “An information security operations center (ISOC or SOC) is a facility where enterprise information systems (web sites, applications, databases, data centers and servers, networks, desktops and other endpoints) are monitored, assessed, and defended.[…]

  A SOC is related to the people, processes and technologies that provide situational awareness through the detection, containment, and remediation of IT threats. A SOC will handle, on behalf of an institution or company, any threatening IT incident, and will ensure that it is properly identified, analyzed, communicated, investigated and reported. The SOC also monitors applications to identify a possible cyber-attack or intrusion (event), and determines if it is a genuine malicious threat (incident), and if it could affect business.” (https://en.wikipedia.org/wiki/Information_security_operations_center)

- Goal of Security Operations: Keep an organisation secure
  - Prevent attacks
  - Detect attacks
  - Recover from attacks

Challenges

- Attackers only need to find one hole
- Insider threats – they are already inside
- Advanced Persistent Threats – they have time and resources
- Complexity of systems
  - Unknown interactions
  - Detecting and remediating attacks is complex
- Complexity of motives
  - Financial
  - Political
  - Sabotage
- Security is a human issue, not a technical one
- Attackers will attack the weakest link – so making systems secure is a paradoxical endeavour
- BYOD
- Security gets in the way
  - People are good at circumventing it

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➲	1. Malware	➲	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	➲	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	➲	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	➲	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	➲	10. Physical manipulation/ damage/ theft/loss	➲	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Legend: Trends: ↓ Declining, ➲ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Table 1- Overview and comparison of the current threat landscape 2018 with the one of 2017

ENISA Threat Landscape Report 2018, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

Resources

- The Cybersecurity Body of Knowledge – CyBOK
  https://www.cybok.org/media/downloads/cybok_version_1.0.pdf
- Government agencies and organisations funded by them, e.g.
  - European Agency for Cybersecurity – ENISA
  - National Cyber Security Centre – NCSC
  - Global Communications Headquarters – GCHQ
  - National Institute of Standards – NIST
  - MITRE, DARPA, DSTL, etc.
- Security Blogs – e.g. Krebs on Security
- Security vendor reports – e.g. FireEye, McAfee, Splunk, Palo Alto Networks, Kaspersky, LogRythm…
  - Especially the yearly reports
- Industry technical reports & talks
- Academic papers