SEC699.1: Adversary Emulation for Breach Prevention & Detection

Topics
• Introduction
• Course objectives
• Purple teaming using MITRE ATT&CK
• Purple team planning and follow-up
• Automation
• Ansible automation
• Building an emulation and detection pipeline
• Building a stack for detection
• Rule-based versus anomaly-based detection
• Building a stack for adversary emulation
• Automated emulation using MITRE Caldera

SEC699.2: Advanced Initial Execution Techniques - Threat Actor APT-28

Topics
• Topic for the day - Advanced initial execution
o Bypassing application whitelisting and ASR
• Threat actor for the day - APT-28
o APT-28 Ã¢ÂÂ Introduction and common techniques
o Definition of the APT-28 emulation plan
• Implement detection use cases
o Review opportunities for detection
• Execute adversary emulation plan - automated
• Conclusion
o Debrief - Emulation plan conclusions and lessons learned

SEC699.3: Advanced Active Directory Attacks - Threat Actor APT-34

Topics
• Topic for the day - Advanced AD attacks
o Advanced Active Directory attacks
• Threat actor for the day - APT-34
o APT-34 - Introduction and common techniques
o Definition of the APT-34 emulation plan
• Implement detection use cases
o Review opportunities for detection
• Execute adversary emulation plan - automated
• Conclusion
o Debrief - Emulation plan conclusions and lessons learned

SEC699.4: Stealth Persistence Strategies & Turla

Topics
• Topic for the day - Stealth persistence
o Obtaining stealth persistence
• Threat actor for the day - Turla
o Turla - Introduction and common techniques
o Definition of the Turla emulation plan
• Implement detection use cases
o Review opportunities for detection
• Execute adversary emulation plan - automated
• Conclusion
o Debrief - Emulation plan conclusions and lessons learned

SEC699.5: Azure AD Attacks

Topics
• Topic for the day - Azure AD attacks
o Azure AD attacks
• Threat actor for the day - APT-30
o APT-30 - introduction and common techniques
o Definition of the APT30 emulation plan
• Implement detection use cases
o Review opportunities for detection
• Execute adversary emulation plan - automated
• Conclusion
o Debrief - Emulation plan conclusions and lessons learned

SEC699.6: Adversary Emulation Capstone