SANS | GIAC CERTIFICATIONS

Supported by

CSA SINGAPORE
Cyber Security Agency of Singapore

IT Track: Practitioner Technical Programme (SANS): **Advanced Persistent Threat Detection and Response for IT Environment**

This Course Will Help You To:

- Analyse APT groups, understanding their geopolitical motivations, sector targeting, and campaign histories.
- Apply the MITRE ATT&CK framework to identify and map APT and other adversary tactics, techniques, and procedures.
- Execute hypothesis-driven threat hunting methodologies to proactively search for indicators of compromise.
- Design and evaluate secure network architectures using network segmentation, zero trust principles, and defence-in-depth strategies.
- Understand key preventive and detective controls and cyber hygiene for detecting and defeating advanced adversaries.
- Develop incident response procedures for organisations, including maintaining business continuity.
- Apply forensics techniques including memory analysis, log examination, and network traffic analysis.
- Establish IT recovery procedures prioritising critical business systems, and implement preventive hardening measures.

Course Overview

Sophisticated attackers know how to blend their activity into normal enterprise operations, making a compromise difficult to uncover through conventional monitoring alone. Evidence of an intrusion may be spread across endpoints, memory, event logs, file systems, authentication activity, and other data sources. Effective investigation requires more than finding individual indicators, it requires the ability to connect these traces, understand attacker behavior, reconstruct the intrusion, and determine the true extent of the compromise. This course provides a comprehensive, hands-on approach to Digital Forensics, Incident Response, and Threat Hunting across enterprise environments. Beginning with threat actor behavior, attack chains, Cyber Threat Intelligence, and MITRE ATT&CK, the six-day course progresses through malware persistence, evidence of execution, event log analysis, lateral movement, memory forensics, and timeline analysis. You will learn to connect individual artifacts, identify attacker techniques, reconstruct intrusions, and determine the scope and impact of a compromise.

Bringing these capabilities together, the course focuses on enterprise-wide threat hunting and intelligence-driven investigations. You will assess preventive and detective controls, develop threat hunts based on adversary behavior, investigate advanced malware and forensic evidence, and apply structured incident response techniques from initial discovery through recovery. AI-assisted approaches are also introduced to support investigative and response workflows. By the end of the course, you will have a practical methodology for hunting, investigating, and responding to sophisticated intrusions, and for turning lessons from each incident into stronger detection, better defenses, and more effective response. This course also equips participants with the knowledge and practical skills needed to prepare for GIAC Certified Forensic Analyst (GCFA).

SECTION 1: CYBER THREAT LANDSCAPE, THREAT INTELLIGENCE AND ACTIVE CYBER DEFENSE

We begin by examining the modern cyber threat landscape and attack chain, providing a foundation for understanding how threat actors operate, adapt and achieve their objectives. The session introduces Cyber Threat Intelligence (CTI) and the MITRE ATT&CK framework, demonstrating how to map the tactics and techniques of specific threat actors to better understand adversary behaviour and attack patterns. The course then moves into defensible security architecture, prevention versus detection, and the principles of advanced persistent defense. Practical exercises involve mapping preventive and detective controls to individual techniques and assessing an organization's ability to prevent and detect them. The role of Artificial Intelligence is also explored, including the generation of dynamic playbooks and support for incident response planning and exercises.

TOPICS:
Cyber Threat Landscape · Attack Chain · Cyber Threat Intelligence (CTI) · MITRE ATT&CK · Threat Actor Tactics and Techniques · Defensible Security Architecture · Prevention and Detection Controls · Advanced Persistent Defense · Defensive Capability Assessment · AI-Enabled Playbooks and Incident Response Planning

SANS | GIAC CERTIFICATIONS

Supported by CSA SINGAPORE Cyber Security Agency of Singapore

IT Track: Practitioner Technical Programme (SANS): **Advanced Persistent Threat Detection and Response for IT Environment**

SECTION 2: MALWARE ANALYSIS, PERSISTENCE AND ENTERPRISE THREAT HUNTING

We examine how malware operates within compromised environments, focusing on the identification of malicious activity, persistence mechanisms and evidence of execution. The session explores the ways forensic artifacts can reveal how malware establishes a foothold, maintains access and executes within a compromised system. These techniques are then extended to enterprise-wide threat hunting, providing practical approaches for identifying patterns, behaviours and indicators of compromise across multiple systems.

TOPICS:
Malware Analysis · Malware Persistence · Evidence of Execution · Compromise Identification · Enterprise-Wide Threat Hunting · Attacker Activity Reconstruction · Indicators of Compromise

SECTION 3: EVENT LOG ANALYSIS, LATERAL MOVEMENT AND ADVERSARY TACTICS

We explore the use of event logs and other telemetry to uncover malicious activity, investigate suspicious behaviour and reconstruct attacker actions. Attention is given to lateral movement and the techniques adversaries use to move through an environment while attempting to evade detection. The session develops practical skills in analyzing security events, malware-related activity, command-line execution and other relevant log sources, with a focus on correlating evidence to identify attack patterns and uncover previously overlooked activity across the enterprise.

TOPICS:
Event Log Analysis · Lateral Movement · Adversary Tactics · Malware Log Analysis · Command-Line Analysis

SECTION 4: MEMORY FORENSICS AND ADVANCED MALWARE INVESTIGATION

We examine memory forensics as a critical capability for uncovering advanced threats and malicious activity that may not be readily visible through traditional investigation. The session introduces memory acquisition and analysis techniques, showing how volatile memory can reveal running processes, malicious code, attacker activity and other evidence of compromise. Advanced investigative techniques are applied to identify code injection, rootkits and other sophisticated threats, while extracting relevant artifacts to support deeper malware and incident analysis.

TOPICS:
Memory Forensics · Memory Acquisition · Memory Analysis · Code Injection · Rootkits · Memory Artefact Extraction · Advanced Malware Investigation

SANS | GIAC CERTIFICATIONS

Supported by

CSA SINGAPORE
Cyber Security Agency of Singapore

IT Track: Practitioner Technical Programme (SANS): **Advanced Persistent Threat Detection and Response for IT Environment**

SECTION 5: TIMELINE ANALYSIS, THREAT HUNTING AND AI-ENABLED DFIR

We explore timeline analysis as a powerful method for reconstructing events and establishing the sequence of activity during a cyber incident. Beginning with filesystem timeline creation and analysis, the session progresses to the development and use of Super Timelines, including targeted timeline creation, filtering and reviewing to efficiently identify significant evidence and attacker activity. The application of Agentic AI is introduced, demonstrating how AI can enhance investigative workflows and support dynamic threat hunting. The session concludes by addressing post-exploitation considerations, including recovery, continuous improvement and lessons learned, with an emphasis on translating incident findings into stronger future defenses.

TOPICS:
Timeline Analysis · Targeted Timeline Analysis · Filesystem Timeline Creation · Super Timelines · Timeline Filtering and Review · Agentic AI for DFIR · CTI-Driven Threat Hunting · Recovery · Lessons Learned

SECTION 6: DFIR NETWARS

The course culminates in a DFIR NetWars which spans the full spectrum of digital investigations, from low-level forensic artefacts and technical evidence to high-level behavioural observations that reveal attacker activity, techniques and intent. The focus is on combining these to investigate incidents, validate findings, identify malicious behaviour and develop a comprehensive understanding of adversary activity across an environment.

TOPICS:
Digital Forensics · Incident Response · Threat Hunting · Malware Analysis · Behavioural Analysis · Adversary Activity Analysis

GCFA
Forensic Analyst
giac.org/gcfa

GIAC Certified Forensic Analyst

The GCFA certification focuses on core skills required to collect and analyze data computer systems. Candidates have the knowledge, skills, and ability to conduct formal incident investigations and handle advanced incident handling scenarios, including internal and external data breach intrusions, advanced persistent threats, anti-forensic techniques used by attackers, and complex digital forensic cases.

- Advanced Incident Response and Digital Forensics
- Memory Forensics, Timeline Analysis, and Anti-Forensics Detection
- Threat Hunting and APT Intrusion Incident Response

Strengthen detection. Accelerate response. Build resilience.
Contact **Singapore@sans.org** for registration, eligibility and GIAC certification details

Sign up today