PARTNERS IN KNOWLEDGE UK LTD
Suite No. 129
295 Chiswick High Road
LONDON W4 4HH



Strategic Security Operations Centre (SOC) Management and Cyber Defence for Judicial Institutions

PIK863-0927 UK-LDN-1

PARTNERS IN KNOWLEDGE UK LTD
Suite No. 129
295 Chiswick High Road
LONDON W4 4HH

Place	: London	**Venue**	: INDUSTRIOUS (1 and 2, 245 Hammersmith Road Floors, London W6 8PW) - TBC		
Start Date	: 06-09-2027	**End Date**	: 10-09-2027	**PPP**	: £4950

Strategic Security Operations Centre (SOC) Management and Cyber Defence for Judicial Institutions

PIK863-0927 UK-LDN-1

If you can't train them, you can't blame them!

Short Description:

This 5 days intensive training program is designed to equip IT professionals within the “Supreme Judiciary Council” with the knowledge and practical skills required to operate, manage and enhance a modern Security Operations Centre (SOC). The course balances strategic concepts, operational processes and hands-on methodologies, focusing on protecting sensitive judicial information, court systems and national digital assets from evolving cyber threats. The program progresses from SOC foundations and threat landscapes to advanced monitoring, incident response, digital forensics and governance. Emphasis is placed on real-world use cases, international best practices (NIST, ISO 27001, MITRE ATT&CK) and alignment with public sector and judicial requirements. By the end of the program, participants will be capable of contributing effectively to SOC operations, decision-making and continuous improvement.

Course Overview:

COURSE OBJECTIVES

- Understand the role and strategic value of a SOC within judicial and government institutions.
- Identify modern cyber threats targeting courts, legal systems and sensitive data.
- Develop skills in security monitoring, log analysis and threat detection.
- Apply structured incident response and escalation procedures.
- Integrate threat intelligence into SOC operations.
- Support digital forensics and evidence preservation processes.
- Align SOC operations with governance, compliance and national cybersecurity frameworks.

TARGET AUDIENCE

- IT Security Engineers and Analysts.
- Network and System Administrators.
- Cybersecurity Officers and SOC Team Members.
- IT Governance, Risk and Compliance Staff.
- Technical Managers responsible for security operations.

Program Outline:

DAY 1: Foundations of SOC & Cyber Threat Landscape

1. Role and Functions of a Security Operations Centre.
2. SOC Operating Models (In-House, Outsourced, Hybrid).
3. Cyber Threat Landscape for Government and Judiciary.

4. Types of Threat Actors (Cybercrime, APTs, Insider Threats).
5. SOC Roles, Skills and Maturity Models.

DAY 2: Security Monitoring, Detection & SIEM Operations

1. Log Management and Security Event Sources.
2. SIEM Architecture and Use Cases.
3. Correlation Rules and Alert Turning.
4. MITRE ATT&CK Framework for Threat Detection.
5. Reducing False Positives and Alert Fatigue.

DAY 3: Incident Response & SOC Workflows

1. Incident Response Lifecycle.
2. Incident Classification and Severity Levels.
3. SOC Playbooks and Standard Operating Procedures (SOPs).
4. Coordination with Legal, HR and Management.
5. Communication and Reporting During Cyber Incidents.

DAY 4: Threat Intelligence & Digital Forensics

1. Cyber Threat Intelligence (CTI) Sources and Feeds.
2. Integrating CTI into SOC Operations.
3. Basics of Digital Forensics for SOC Analysts.
4. Evidence Handling and Chain of Custody.
5. Supporting Legal and Judicial Investigations.

DAY 5: SOC Governance, Compliance & Continuous Improvement

1. SOC Governance and Performance Metrics (KPIs, SLAs).
2. Compliance with ISO 27001, NIST and National Regulations.
3. Risk Management and SOC Reporting to Leadership.
4. Automation and SOAR Technologies.
5. SOC Maturity Assessment and Improvement Roadmap.

CASE-STUDY: Equifax Data Breach (2017)

Equifax, a global credit reporting agency, suffered a massive data breach exposing personal data of over 147 million individuals. The breach highlighted critical failures in vulnerabilities management, monitoring and incident response, making it a vulnerable SOC learning case.

GROUPS DISCUSSION QUESTIONS:

- What was the primary SOC-related failure in the Equifax breach?
- Which SOC control could have detected the breach earlier?
- How could threat intelligence have helped prevent the incident?
- What incident response weakness worsened the impact?
- What key lesson is most relevant for judicial institutions?