*Hosted by Amar Singh*



## DELEGATES WILL UNDERSTAND:

- Review the current threat landscape and cover the common attack vectors hackers are exploiting.
- Analyse recent known and some unknown attacks and dive into the technical details on how they avoided detection.
- Review the basic application of incident triage, OODA and the Diamond Methodology and deep dive into the Cyber Kill Chain.
- Help attendees understand the role log management plays in network based attacks followed by a review of the most common log types and log sources in an organisation.
- Review most common SIEM products and technologies including security analytic approaches to SIEM. We will also review NBAC – network behaviour anomaly detection approach to identifying attacks.
- Deep dive into some of the most relevant attack scenarios – analysing each attack with a technical and business focus.
- Help attendees understand the critical role that vulnerability management and penetration testing play in understanding network based attacks.
- Produce a profile of attackers and their motivations, and their capabilities.
- Identify and review results of current state of existing controls. This will include controls such as SIEM, Identity and access management, logging and monitoring and other relevant controls.

## MODULES

**Triage, Detection & Monitoring**
- OODA
- Triage
- Diamond Methodology
- Logging
- SIEM
- Log Management
- Log Types
- Deception Technology
- Visibility
- Cyber Kill Chain

**Attackers & Motivations**
- Types of Attackers
- Privileges Insider
- Types of Attack motivations
- Impact of Actions
- Attack Vectors

**Define Normal**
- Taxonomy
- Processes
- People
- Technology

**Attack Manifestation & Scenarios**
- Active Directory based attacks & the Privileged User
- LAN Based Attacks
- DDoS & DoS
- DNS
- Advanced Persistent Threats