Masterclass: Implementing and Managing Microsoft Advanced Threat Analytics

Duration: 5 Days **Course Code: ATA** **Delivery Method: Company Event**

Overview:

200+ days. That's the average amount of time that attackers reside within your network until they are detected, gathering classified data and information, waiting to strike at just the right moment. The Microsoft Advanced Threat Analytics (ATA) helps to identify breaches and threats using behavioral analysis and provides a clear, actionable report on a simple attack timeline. Customers that want to proactively monitor the environment should be more aware about which activities are malicious, which are good. This is a great challenge when this relates to the hundred-servers environment.

Target Audience:

Infrastructure architects, security professionals, systems engineers, network administrators, IT professionals, security consultants and other people responsible for implementing network and perimeter security.

Objectives:

- Module 1: Threat landscape
- Module 2: ATA Architecture
- Module 3: Prerequisites
- Module 4: Installation
- Module 5: Detection module
- Module 6: Analytics module
- Module 7: Management
- Module 8: Troubleshooting
- Module 9: Further steps

Prerequisites:

An ideal candidate for this course should have attended Masterclass: Hacking and Securing Windows Infrastructure. You should alternatively have good knowledge on Windows authentication mechanisms and protocols. You should have good understanding of PTH and PTT attacks. Experience in Active Directory Domain Services is highly recommended.

Content:

Module 1: Threat landscape

- Risks for cloud and on-premise infrastructure
- Modern threats
- Incident response flaws

Module 2: ATA Architecture

- ATA Center
- ATA Gateway
- ATA Console
- Multi-segment networks

Module 3: Prerequisites

- Active Directory requirements
- Networking requirements
- Database requirements
- Capacity planning
- Port and protocols

Module 4: Installation

- Port monitoring
- Event collection
- Mobility support
- Integration to SIEM/Syslog
- Virtualization issues

Module 5: Detection module

- Incident responding
- Short-term lease subnets
- Honeytokens

Module 6: Analytics module

- Suspicious Activities Time Line
- Filtering Suspicious Activities
- Self-learning

Module 7: Management

- ATA Console
- ATA Configuration
- Alerts
- Health Center
- Database management
- Telemetry

Module 8: Troubleshooting

- Backup and Restore
- Logs
- Performance counters
- Database

Module 9: Further steps

- Advanced monitoring techniques
- Incident response plans

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/