## Syllabus of Zero Trust Security

Zero Trust Security has rapidly emerged as a significant global trend for all types of organizations. Practically all enterprises have historically implemented some form of zero trust components without officially adopting the architecture. However, there is still quite a bit of confusion as to exactly what the initiative is and how to best implement it. In this live 4-hour crash course, security industry expert Michael J. Shannon demystifies the various architectures and offers real-world guidance for launching or continually improving your Zero Trust initiative while avoiding common pitfalls.

In this course the following topics are covered:

- **Session 1: Zero Trust Architectures**
    - Defining Zero Trust and related concepts
    - History and progression
    - Core principles
    - Expanded principles
    - Requirements for a platform
    - Components of a ZT architecture
    - The NIST Zero Trust Model (SP 800-207)
    - The Garbis/Chapman conceptual model
    - Resource-based model
    - Enclave-based model
    - Cloud-routed model
    - Microsegmentation model

*15 Minute Break*

- **Session 2: Zero Trust in Practice**
    - Google BeyondCorp
    - PagerDuty ZT Network
    - Software Defined Perimeters
    - IAM and Privileged Access Management
    - Network infrastructure and NAC
    - Next-generation IDS/IPS and Firewalls
    - VPNs
    - Security Operations
    - Data protection and DLP
    - Cloud services
    - IoT and Zero Trust

*15 Minute Break*

- **Session 3: Zero Trust Policies, Scenarios, and Strategies**
    - Common constraints and roadblocks
    - Zero Trust components
    - Applied policies and scenarios
    - VPN alternatives
    - Third parties using access controls
    - Migrating to the cloud
    - DevSecOps
    - Service-to-Service Access
    - Full Zero Trust network transformation
    - Mergers and acquisition considerations
    - Strategic top-down approach
    - Tactical bottom-up approach
    - Examples of Zero Trust deployments