4 月 16 日（火）

時間	セッション	説明
09:30 - 10:00	モーニングセッション	トレーニングの概要と 1 日のスケジュールの確認
10:00 - 11:00	サイバーセキュリティの概念	サイバーセキュリティの概念
11:00 - 11:45	アクティブディフェンスの概念	- 情報セキュリティの概念 - セキュリティシステムの 7 つのレイヤー - SIEMシステムの利点
11:45 - 12:00	休憩	休憩
12:00 - 12:30	Wiresharkの紹介	WireSharkの役割りと使用方法
12:30 - 12:45	Sysinternalsの概要	- Process Explorer, TCP View, Process Monitor, Autoruns - 兆候の把握
12:45 - 13:45	昼休憩	昼休憩
13:45 - 14:15	Wiresharkハンズオン	効率的かつ最適にWireSharkを使用する方法
14:15 - 15:30	基本的なフォレンジック - Kill Once	感染したワークステーションを分析し、収集したデータを解析した上で感染したワークステーションがどのように疑わしいかどうかを判断します
15:30 - 15:45	休憩	休憩
15:45 - 17:00	基本的なフォレンジック - Kill Once	感染したワークステーションを分析し、収集したデータを解析した上で感染したワークステーションがどのように疑わしいかどうかを判断します
17:00 - 17:30	デイリーサマリ	1 日の総括とフィードバック （質疑応答）

EXPECT THE UNEXPECTED

4 月 17 日（水）

時間	セッション	説明
09:30 - 09:45	モーニングセッション	トレーニングの概要と 1 日のスケジュールの確認
09:45 - 11:30	アリーナのインフラについて	トレーニングで使用するアリーナのセキュリティシステムとインフラを把握します
11:30 - 11:45	休憩	休憩
11:45 - 12:45	Desktop Dos [Malicious DOK]	攻撃者は組織を標的にし、すべてのユーザーにDoS攻撃を仕掛けます
12:45 - 13:45	昼休憩	昼休憩
13:45 - 17:00	Ransom [Nikto & XSS]	攻撃者は組織のコンピュータを標的にし、ランサムウェアでコンピュータのロックとデータの暗号化をします
17:00 - 17:30	トレーニングサマリ	トレーニング総括とフィードバック（質疑応答）