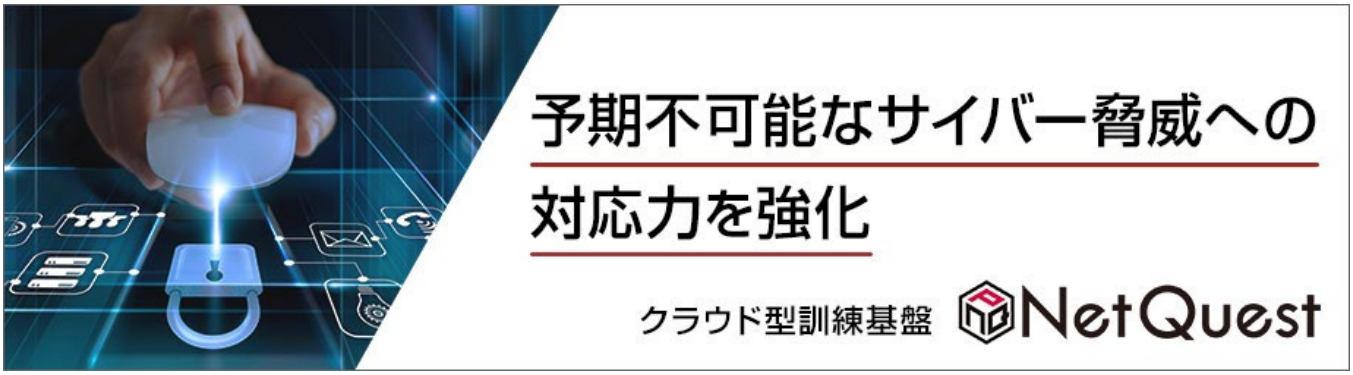
NEWS RELEASE

報道関係各位

2024 年 8 月 1 日

サイバー攻撃を疑似体験し、リアルな行動と判断で CISO／CSIRT 要員の対応力・意思決定力の向上を支援！ ～クラウド型インシデントレスポンス訓練基盤に新機能を追加～

アライドテレシス株式会社（本社 東京都品川区、代表取締役社長 サチエ オオシマ）は、組織全体でサイバー攻撃に迅速かつ適切に対応するための訓練をクラウドで提供する「NetQuest Platform」に新機能の追加および機能拡張を実施したことをお知らせいたします。



日々巧妙化するサイバー攻撃による被害は深刻化し組織全体の対応が求められる中、アライドテレシスは事前の準備や調整の時間・コストを抑えながら、企業の実環境に即した組織全体の訓練を可能とするクラウド型インシデントレスポンス訓練基盤「NetQuest Platform」の提供を開始しました。CISO・CSIRT の育成とともにインシデント対応を必要とする部門に同一のシナリオ状況を付与することで組織全体の訓練を同時に実施すること、また、一連のインシデント対処を経験することができるため、内閣サイバーセキュリティセンター（NISC）をはじめ様々な企業にも採用されています。

この度、「NetQuest Platform」に新機能「ダイナミックシナリオ」の追加と既存機能のエンハンスを行いました。これにより、よりリアルな環境・状況に即した訓練が可能となり、CISO や CSIRT 要員などの訓練者の判断力や対応力、さらには意思決定力の向上を支援いたします。

■予測不可能なサイバー攻撃への対応力を強化

現実のインシデントレスポンスには、予測不可能な状況が多く存在するため、フォレンジック調査を含め、試験のような選択肢の提示は無く的確な判断力と対応力が求められます。

当社は、これまで選択肢問題の回答によって自動的にシナリオが分岐する訓練のみを提供していましたが、新機能「ダイナミックシナリオ」では、記述式問題を追加し、ファシリテータが参加者の回答をもとにその場でシナリオを構築します。

●ダイナミックシナリオの特長

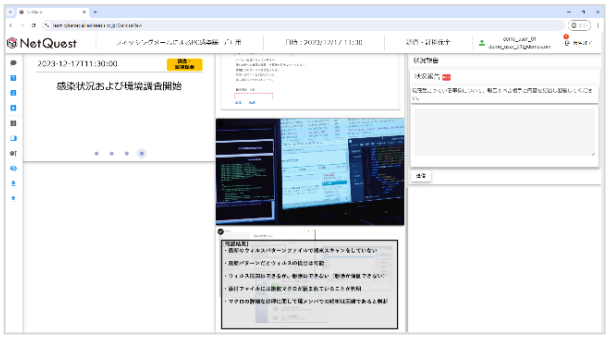
＜想定するシチュエーションが増え、実体験に近い環境を提供＞

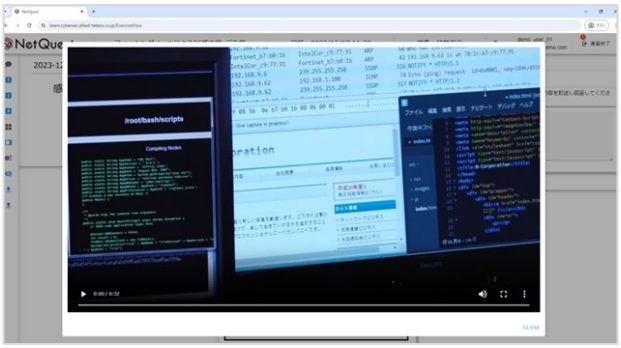
分岐したシナリオの内容に応じて記述式問題を利用することで、分岐シナリオの幅は広がり、想定されるシチュエーションが増えます。また、ファシリテータがその場でシナリオを構築するため、企業に合わせて個別化・細分化された内容となり、より実体験に近い環境で訓練を提供します。

＜記述式問題により参加者の的確な判断力・対応力を養う＞
記述形式の問題では、用意された回答が無い中、参加者の考えを言語化してアウトプットすることで、深い理解と応用力、さらには的確な判断力、対応力を養うことができます。また、インシデントが発症すると報告書の提出などのドキュメントワークも必要となるため、訓練参加者が実際に利用するドキュメント・フォーマットで情報共有を行うトレーニングにもご活用いただけます。

CISO や CSIRT に加え、サイバー攻撃について充分な知識を持つ情報セキュリティやインシデント関連部門の責任者・担当者に適した訓練となります。サイバー攻撃をリアルに体験することができ、実態に沿った改善策を得られます。

■動画視聴でインシデント状況を直感的に把握、参加者の理解度が向上
今回の機能拡張により、インシデント状況が動画ファイルでも付与できるようになりました。
これにより、シチュエーションに合わせて画像や文書ファイルだけでなく、動画ファイルも活用できるため、直感的な訓練が可能となり、参加者の理解度を大幅に向上させることができます。また、組織全体の同時訓練のスムーズな進行を支援します。
＜動画ファイルによるインシデント状況の付与＞





■複数人での同時シミュレーション訓練で、迅速かつ効果的な対応力を育成
今回の機能拡張により、回答者（1 名）に加え「部門参加アカウント」として複数の訓練参加者が訓練状況の参照とチャット機能を利用できるようになりました。

例えば、インシデント対応の中心的な役割を担う CISO や CSIRT が回答者である場合、情報システム部の複数の訓練参加者が「部門参加アカウント」を利用します。それぞれ同時並行で、付与されたシナリオへの対応方法を検討しチャット機能でエスカレーションを行うことで、回答者の迅速な意思決定をサポートします。また、回答者は、「部門参加アカウント」を利用する訓練参加者にログ調査などの指示を適切なタイミングで出すことをシミュレーションでき、迅速なインシデント対応力とリーダーシップスキルの向上にお役立ていただけます。
他にも、部門間の連携・情報共有などのコミュニケーション強化を目的とした訓練にもご活用いただけます。

●サービスの詳細はこちらよりご確認ください。https://www.allied-telesis.co.jp/security/training/

サイバー攻撃の被害を最小限に抑えるには、個々の的確な判断力と迅速な対応力を養い、部門間の連携を強化し組織全体でのインシデントレスポンス能力を向上させることが重要です。日々進化するサイバー攻撃への対策として、「NetQuest Platform」をはじめ当社のセキュリティソリューション・サービスをご活用ください。

＜＜製品に関するお問い合わせ＞＞
E-Mail: info@allied-telesis.co.jp
https://www.allied-telesis.co.jp

＜＜ニュースリリースに対するお問い合わせ＞＞
マーケティングコミュニケーション部
Tel: 03-5437-6042 E-Mail: pr_mktg@allied-telesis.co.jp

アライドテレシス株式会社　　東京都品川区西五反田 7-21-11 第 2 TOC ビル