学校法人 岩崎学園 情報科学専門学校　様
職場体験レポート

アイルミッション

CYBERGYM横浜

サイバーセキュリティトレーニング

APT攻撃を実体験

攻撃調査＋初期分析の実践

CYBERGYM横浜に関して

ホワイトハッカーによる最新技術のサイバーアタックを体感

模擬環境を持つトレーニングルームで、ホワイトハッカーによる巧妙なサイバーアタックを体験。何が起きているか分からない緊迫感のある異常事態で、対応マニュアルや対応チームのアクションが機能するか、改善点がどこにあるのかを実践的に理解できます。

受講トレーニング　Cyber-Threats and Defense Essentials

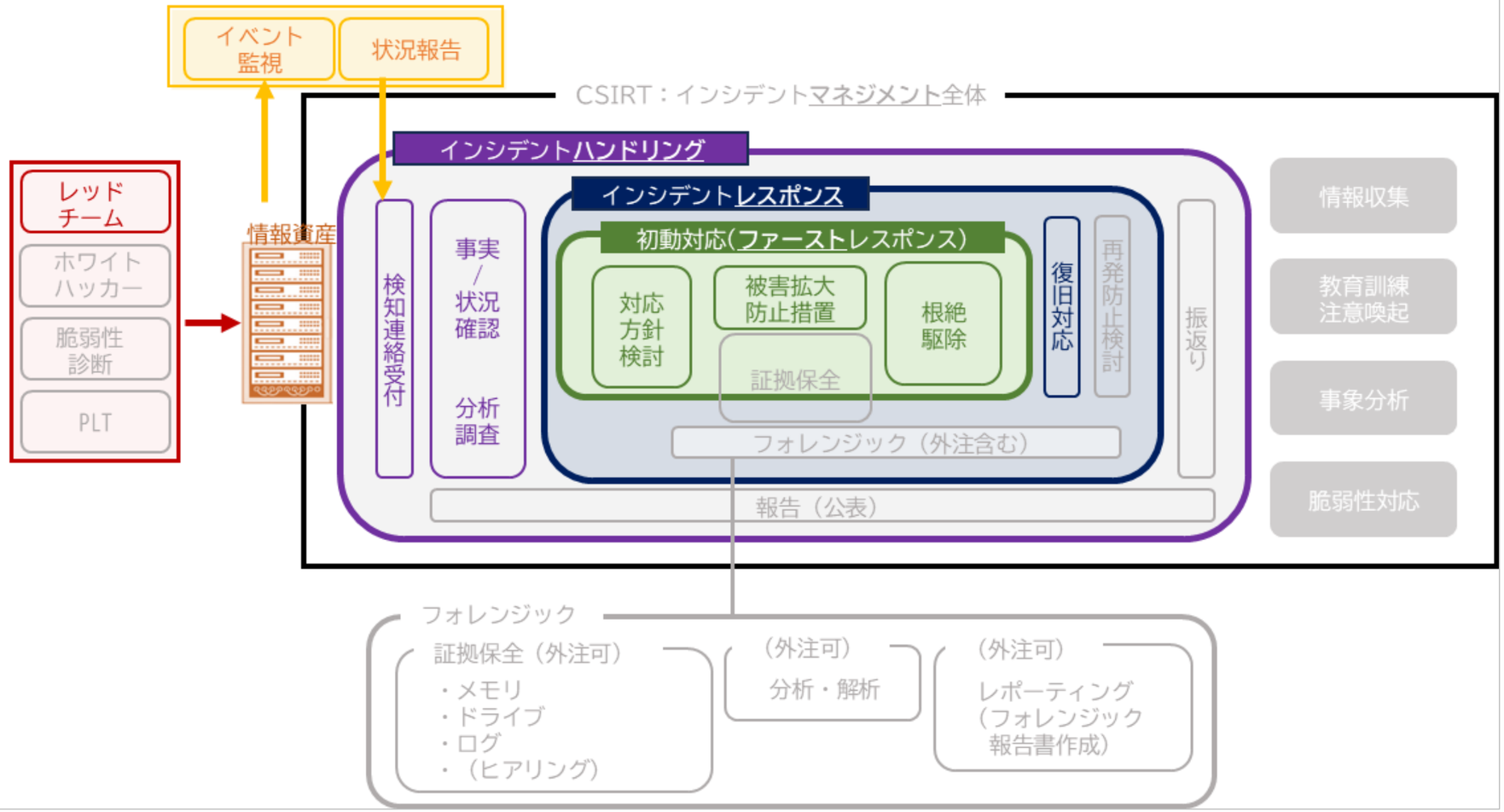
内容
・ホワイトハッカーが行う実際のAPTを体験
・サイバー攻撃防御の基礎
・各種ツールを用いた攻撃調査＆初期分析

習得スキル
・複数の検出・監視ツールを駆使して
サイバーインシデント攻撃を検出
・検出したサイバー攻撃インシデントの初期分析

PROGRAM

★はオンラインで実施

- サイバーセキュリティの概念 ★
- アクティブディフェンスの概念 ★
- WireShark概要 ★
- WireShark演習
- Sysinternals概要 ★
- マルウェアフォレンジック演習
- SIEM概論 ★
- アリーナインフラについて
- APT攻撃演習
- 演習レビュー



受講者インタビュー

Q：学校での専攻や将来の夢は？
A：将来の夢は、セキュリティテクノロジーの法的リスクを解決しその能力を十分に発揮して堅牢で信頼できるデジタル環境を構築し、個人や組織を守ることです。

Q：ズバリ！「実際のマルウェア感染体験」を受けて見て、感想はいかがでしたか？
A:マルウェアに感染することは初めての体験でしたが、sysinternalsを利用しどのような振る舞いが見られ、QRaderを使用してどのログが重要かを理解することができ、セキュリティの観点から多くの知見とスキルを得ることができました。

大森さん

学校法人 岩崎学園 情報科学専門学校
情報セキュリティ学科
サイバーセキュリティコース

受講者インタビュー

Q：これまで学校で学んで来た事で活かせた部分は？
A：学校で習得した知識や、スキルが情報処理安全確保支援士の午後試験の対策に有効だったことです。

Q：学校での学びに加え「実体験してみて」学べた事、理解が深まった事は？
A：マルウェアに感染した後の対応は授業や資格勉強で学びましたが、感染後PC内でマルウェアがどのような振る舞いをとるのかまた、ログではどのように表示されるのかを実際に体験して理解が深まりました。

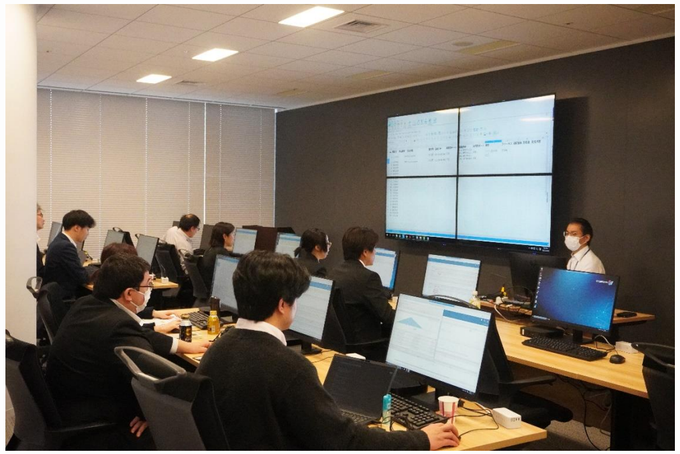
サイバー攻撃の裏で何が起こっているのか、真剣にログを見つめる。

受講者インタビュー

Q：トレーニングを受けて、今後更にチャレンジしていきたいと感じた事は？（学校での学習や将来の夢に対して）

A：自分の夢に近付けるよう、授業や資格勉強に活用すること、また自分以外の学生にもQRaderやsysinternalsの使用方法を広報して、マルウェアを検知する際の技術的な側面を広めていきたいと考えています。

講師の解説や“種明かし”で、知らなかった学びを得る。



受講者インタビュー

Q：学校での専攻や将来の夢は？
A：サーバの構築を通してセキュリティを学んでいます。

Q：ズバリ！「実際のマルウェア感染体験」を受けて見て、感想はいかがでしたか？
A：大変勉強になり、面白かったです。セキュリティ面白いなと改めて感じることができました。レッドチームからの攻撃の状況が最初はよく分からなかったのですが、講師の方々から状況を整理をしていただく中で、「今はこういった攻撃がされているんだな」「前の攻撃はこの段階で、今度はさらに侵入してきたんだな」としっかり理解しながら講習を進められたことが嬉しかったです。

永吉さん

学校法人　岩崎学園　情報科学専門学校
情報セキュリティ学科
ITスペシャリストコース

受講者インタビュー

Q：これまで学校で学んで来た事で活かせた部分は？
A：QRadarが検知した攻撃の内容について理解できました。上がってきたアラームについて、具体的にどこから、どのような手段で攻撃されたのかが全く分からなくなることはありませんでした。

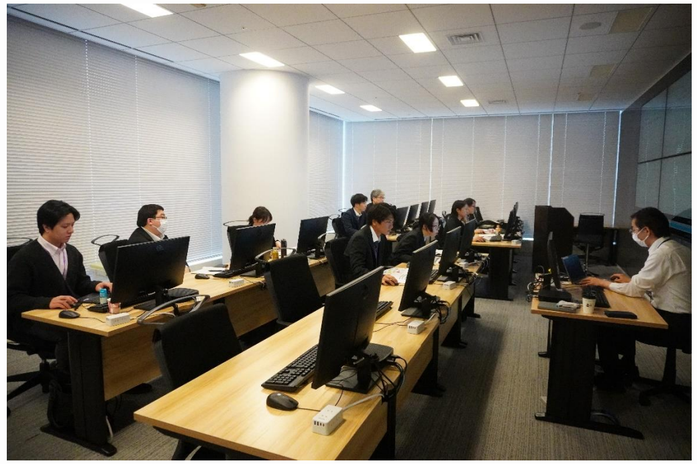
Q：学校での学びに加え「実体験してみて」学べた事、理解が深まった事は？
A：どのようにマルウェアが侵入してくるのかは今回初めて体験しました。クロスサイトスクリプティングやSQLインジェクションなどの攻撃はある程度体験したことがありますが、そこからマルウェアがコンピュータに入ってしまった状況と、それをどのように確認するか、実態がどこにあるかをSysinternalsの使い方とあわせて学ぶことができました。

受講者インタビュー

Q：トレーニングを受けて、今後更にチャレンジしていきたいと感じた事は？（学校での学習や将来の夢に対して）

A：フォレンジックの役割でマルウェア感染体験をしましたが、現在の力不足を感じました。マルウェアが侵入してきたことはわかっているのに、どこにいるか、どこで悪さをしているのか見当がつかない、それによって次の段階まで侵入を許してしまうことがありました。講師の方々にアドバイスを受けながら理解はできましたが、この先自分である程度の対応ができるようになりたいと思いました。

IT企業の情シス部門も参加。
実際に仕事で携わる人たちの取り組みに刺激を受ける。

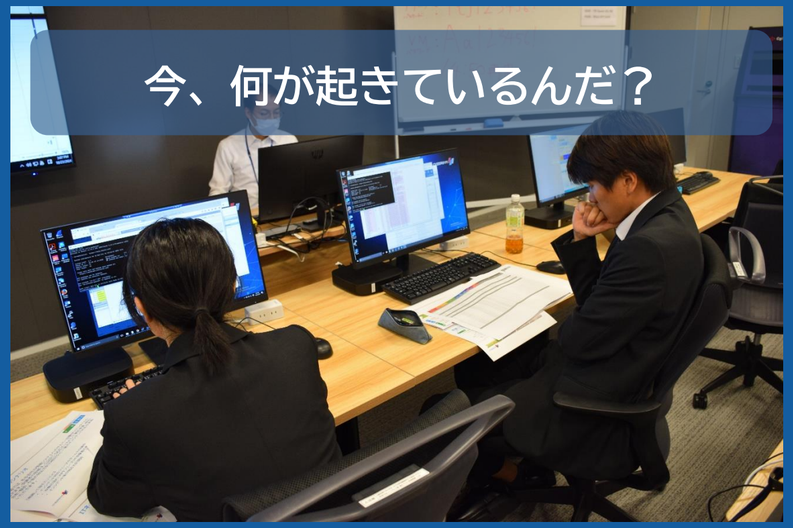


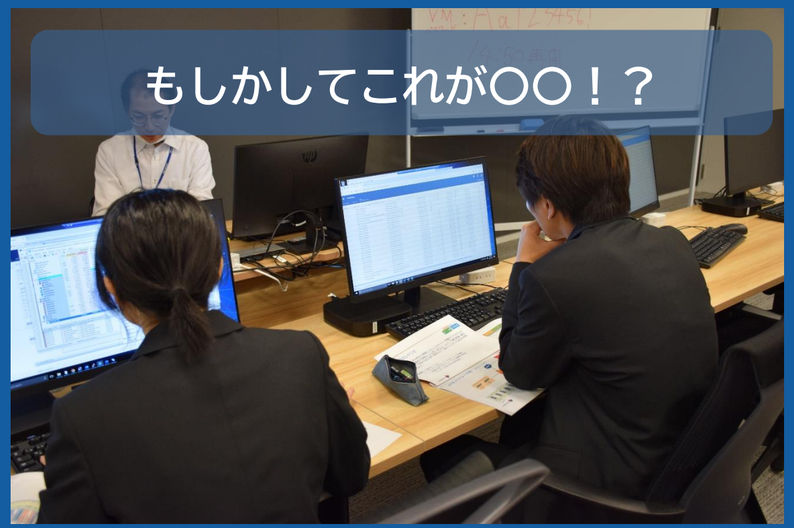
フォトギャラリー


いざ！サイバー攻撃体験へ！


監視ツールの使い方をおさらい


さあ、攻撃が始まった！


今、何が起きているんだ？


もしかしてこれが〇〇！？


ヘトヘトになって終了！

THANK YOU!

心地よい疲れと共に、受講を終えて講師と記念撮影

大森さん・永吉さん
受講お疲れ様でした！

将来の夢に向かって、
少しでも刺激になっていれば嬉しいです！

岩崎学園様、
ありがとうございました。

アイルミッション