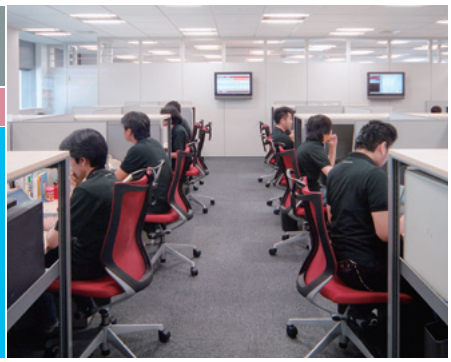
SANS



トレンドマイクロ株式会社 様

SANSセキュリティトレーニング　FOR508 (Advanced Computer Forensic Analysis and Incident Response)　導入事例

最高レベルのフォレンジック技術を実際の事案に即したシナリオで学習しセキュリティ現場の即戦力を育成

TREND MICRO
Securing Your Journey to the Cloud

■ 会社概要

トレンドマイクロ株式会社

1988年の創業以来、「デジタルインフォメーションを安全に交換できる社会」の実現に向けて、コンシューマー向け総合セキュリティ対策ソフト「ウイルスバスター」から、標的型サイバー攻撃対策をはじめとする各種エンタープライズセキュリティソリューションまでを幅広く提供。国境を超越した多国籍企業＝トランスナショナルカンパニーであると同時に、本社を日本に置くことで、国内ユーザーのニーズに対するきめ細かなサポートを実現している点も大きな特長となっている。

http://www.trendmicro.co.jp/

トレンドマイクロ株式会社
スレットディフェンスSE本部
エンタープライズSE部
サイバー攻撃レスポンスチーム1課　担当課長
新井　悠氏

「FOR508では、まったく新しいフォレンジック手法を学ぶことができました。従来とはアプローチをまったく変えて、個々のファイルではなくプロセス全体で見ていく新たな手法を採ることで、より迅速かつ効率的にマルウェアを回収できるようになったのです」

1988年の創業以来、世界的なセキュリティ製品ベンダーとして、コンシューマー向け製品「ウイルスバスター」をはじめ、多彩なソリューションを展開してきたトレンドマイクロ株式会社。エンタープライズ向け分野にも多大な実績を持ち、最近ではクラウドベースのセキュリティ対策ソリューションや、標的型サイバー攻撃対策など、常に最先端の技術を盛り込んだ製品やサービスを提供し続けています。同社では2014年2月、国内で初めて開催されたSANSトレーニングのコンピューターフォレンジック上級コース「FOR508」をいち早く導入。社内スタッフの技術力強化と顧客サービスのアジリティ向上に大きな成果を挙げています。

■ 導入背景

迅速なインシデント対応に向け常に技術向上への努力が求められる

トレンドマイクロ株式会社（以下、トレンドマイクロ）のエキスパート技術者の1人であり、今回FOR508を受講した同社 スレットディフェンスSE本部 エンタープライズSE部 サイバー攻撃レスポンスチーム1課 担当課長 新井 悠氏。同氏の所属チームは、不正アクセスやハッキングなどの脅威から企業システムを守るエンジニアの集団です。顧客のシステムにセキュリティ関連の事案が発生した場合、その問い合わせにいち早く対応し問題を解決する、まさに企業の情報セキュリティ防衛の最前線といえます。

「原因の究明から対処までのリードタイムをいかに短縮し、迅速で適確なインシデント対応を実現するかが私たちの至上課題です。それには常に最新の技術動向を把握し、不正アクセスを仕掛けてくる相手を上回る技術力を習得、維持、そして向上し続けることが要求されます」。

それだけに同社では社員一人ひとりの自己研鑽に積極的な支援体制を敷いており、各自の職制やポジションに応じた研修費用の補助が受けられるようになっています。

「社内教育メニューから学びたい科目を選び、ポータルサイトから申請するだけです。各人の自己研鑽に対する意欲を尊重し、モチベーションの高い人ほど、その意欲に応じた学習機会を得られる制度になっているのです」。

■ 導入経緯

フォレンジック上級コースの日本初開催に強い関心

今回、新井氏がFOR508に着目したきっかけは、「世界的な情報セキュリティトレーニングとして知られるSANSのアドバンストコースが日本でも開催されると聞いて、強い関心を持った」ことだと明かします。同氏は情報セキュリティのエキスパートとしてサイバー攻撃レスポンスチームの指導的立場にあり、かねてからSANSのトレーニングには高い評価を与えていました。

「私が情報セキュリティの仕事について間もない頃、米国ボルチモアでSANSトレーニングを受講したのです。とにかくすばらしい講師陣と講義内容で、ここでの教育が自分の基礎を作ってくれたと長らく感じていました。そのSANSのフォレンジック上級コースが日本で開催されると聞き、まずは自分で受けてみたいと考えたのです」。

フォレンジック技術は自分たちの担当業務で最も重要なテクノロジーの1つであり、トレーニングで習得した最新かつ世界水準の技術をチーム内に伝達・共有することで、チームの技術レベルアップにつながればという思いももちろんあったと、新井氏は付け加えます。

■ 導入効果

トレーニングで習得した実践的手法が現場での事案解決に大きく貢献

新井氏は実際にFOR508を受講した印象を、「全6日間のプログラムが、ひたすら最終日に向かって流れていく、その調和感がすばらしい」と表現します。FOR508では1～5日目までが各技術領域や手法の学習にあてられ、最終日となる6日目にはそれらを応用した実践的演習が行われます。そのため、最初の5日間も単なる知識の教科書的羅列ではなく、あくまで最終日の「お客様の問題発生から解決まで、実在の案件を想定し得るシナリオ」（新井氏）を解決する、実践的な視点に立ったトレーニングが大きな特長です。

「トレーニングはハンズオン中心で行われるので、自分の手で実際に操作してみて理解する。つまり『わかると、できるようになる』のを受講者に自ら経験させることに時間を割いています。この成功体験の繰り返しが、習得への強いモチベーションになるのです」。

新井氏自身も今回のFOR508受講では、「捨てていく」手法を新たに学ぶことができたと振り返ります。一口にフォレンジック作業といっても、OSが標準で持っている数十万のファイルの中からたった1つのマルウェアを探し出すのは至難の技です。そこで可能性の薄いものをどんどん削ぎ落としていき、怪しい部分だけに絞り込んでいくのです。

「それも従来のフォレンジック手法の延長ではなく、アプローチそのものがまったく変わりました。個々のファイルを見るのではなくプロセス全体で見ていくことで、より迅速かつ効率的にマルウェアを回収できるようになりました」。

FOR508で得られた知識や手法は、チーム内にも着実に伝達・共有されています。新井氏が講師役となって勉強会を開催したり、チームのスタッフが担当する顧客で発生した事案に、新井氏がトレーニングで習得した手法をアドバイスして無事解決に至ったという成果もすでに挙がっています。

■ 今後の展望

さらに高度な内容と幅広い分野のSANSトレーニングの展開に期待

ところで、本事例を見た企業のセキュリティ担当者がこれからFOR508を受講してみたいと考えた場合、フォレンジックトレーニングの最高レベルの内容とあって、あらかじめ新井氏のようなエキスパートのレベルに達している必要があるのでしょうか。

「FOR508では基本的に『SIFT Workstation』というツールのセットを渡されて、そのツールの使い方を学びながら事案を解決していくというカリキュラムが中心です。使いながら理解していけるので、ウイルス事案などを手がける情報セキュリティ担当者ならば、予備知識の有無はあまり気にせずに、まず受講されるのがよいでしょう」。

6日間にわたってのツールを利用したトレーニングとあって、費用もある程度まとまったものになります。

「多くの企業経営者は、サイバー攻撃などの報道を聞いて、『うちの備えはどうなっているのか』と情報システム担当者に尋ねます。しかし本来は、いざそうしたニュースに接してもあわてないよう、ふだんから人材を育成しておくことが、何よりの自社の情報セキュリティ防衛につながるのです」。

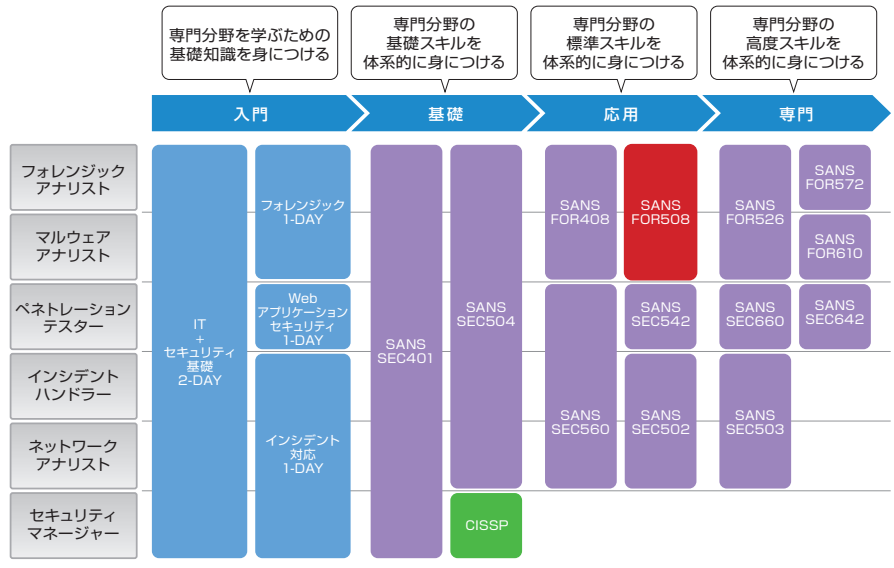
そうした意味でも、FOR508に限らず、SANSトレーニングを活用して人材育成することは、有効なセキュリティ投資と捉えることができるのではないかと新井氏は示唆します。

また、SANSの講師の高度な知識とユーモアあふれる魅力的な講義に強い感銘を受けたと語る新井氏は、今後さらに高度な内容のトレーニングを幅広く展開してほしいと要望を語ります。

「自分で社内のスタッフに指導をしていても、内容が高度になればなるほど、どうやって教えていいのか悩むケースがしばしばです。SANSトレーニングの講師のように、『難しいことを解りやすく伝える』ノウハウを知る意味でも、今後のプログラム展開には期待しています」。

情報セキュリティの世界最先端を走るトレンドマイクロの技術力を、FOR508をはじめとしたSANSトレーニングのプログラム群がこれからも力強くサポートしていきます。

セキュリティキャリアロードマップ例



※本文中の組織名、職名、構成図は公開当時のものです。

NRIセキュアテクノロジーズ株式会社
〒100-0004　東京都千代田区大手町1-7-2　東京サンケイビル
Tel：03-6706-0500　Fax：03-6706-0599
ホームページ　http://www.nri-secure.co.jp/
メールアドレス　info@nri-secure.co.jp

9225-0032-01-1409