SANS

デロイト トーマツ リスクサービス株式会社 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

グローバルスタンダードに照らした 自社のフォレンジック技術水準の検証と 最新のサイバーセキュリティ動向を探る

Deloitte. トーマツ

■ 会社概要

デロイト トーマツ リスクサービス株式会社(DTRS)

デロイト トウシュ トーマツ リミテッド(デロイト)の、日本におけるCyber Risk Services(CRS)チームとして、世界品質のリスクサービスを提供。技術革新やグローバリゼーション、そして規制の強化等で企業のビジネスリスクが拡大する中、デロイトのノウハウや最新のツールを活用し、従来型のリスク管理だけでなく、あらゆる分野でのリスクを想定した品質の高いリスク管理体制の構築・運用を支援している。

http://www.deloitte.com/jp/dtrs

デロイト トーマツ リスクサービス株式会社
マネジャー
岩井　博樹氏

「FOR508で学んだ手法の一つが、被害端末のPCの過去データをつぶさに検証する取り組みを通じて、今までは気づかなかったヒントを発見できるということです。これをトレーニングで体験した結果、インシデント対応では常に過去データを意識するようになりました」

世界の四大会計事務所の一角を占める、デロイト トウシュ トーマツ リミテッド(以下、デロイト)。その日本におけるサイバーセキュリティサービス拠点であるデロイト トーマツ リスクサービス株式会社は、幅広い分野にわたる総合的なITリスクマネジメント業務を提供しています。同社では2014年2月、わが国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」を導入。グローバル企業に求められる高度なインシデント対応力と、セキュリティマネジメントにおける先端ノウハウの習得を通じて、サイバーセキュリティ分野における存在感を一層確かなものにしています。

■ 導入背景

グローバルスタンダードに照らして 自社の技術レベルを確認する好機に

一口にフォレンジックといっても、その内容はさまざまです。一般に監査法人におけるフォレンジックはファイナンスにおける不正調査を指しますが、デロイト トーマツ リスクサービス株式会社(以下、DTRS)マネジャー 岩井博樹氏が担当するのは、サイバー犯罪やサイバー攻撃に対するインシデント対応であり、フォレンジックの中でもとりわけ高い緊急性と高度なセキュリティ技術が要求される分野です。

「デロイトの国際ネットワークの中で仕事に携わっていると、やはり品質とメソドロジーの両面においてグローバルスタンダードが要求されてきます。今回FOR508を受講してみようと思った背景には、サイバーセキュリティのフォレンジック技術に関して現在自分たちが提供しているものが、そうしたグローバルスタンダードに適っているかどうかを確認したいという考えがありました」。

加えてDTRSでは、サイバーセキュリティを自社のコア事業の1つと位置付けています。このため今回のFOR508導入も、いわゆる社内教育にとどまらない、重点事業分野への積極投資の一環として捉えていたことが、他社に先駆けての採用につながりました。

「最新の知見を得られるだけでなく、講師や参加者とのコミュニケーションを通じて、この分野のエキスパートとのコネクションを築くきっかけになればという期待もありました」。

■ 導入経緯

トレーニングの提案を受けて 自社の知りたい要件を満たすと判断

岩井氏が最初にNRIセキュアテクノロジーズからFOR508の提案を受けて、注目したトレーニングの内容としては、大きく3つのポイントがありました。

その筆頭は、トレーニング全体の最重要テーマのひとつでもあった「タイムライン分析」です。これはプログラムの実行やファイル作成などのシステムの挙動を時系列で整理して、インシデントの流れを分析するテクニックです。岩井氏は、これまではオープンソースソフトウェア(OSS)のツールを使ってタイムライン分析を実施してきましたが、これらの手法がグローバルスタンダードに照らして合っているかを確認できると考えたのです。

「実際に講師に質問してみた結果、これまで私たちが採用してきた手法が正しかったことが確認できました。加えて、過去のSANS受講者が開発したツールなども紹介していました」。

2番目の注目ポイントは、「メモリダンプの解析」です。これもDTRSではすでに手がけていま

したが、遠隔地から被害を受けた稼働中のシステムからメモリのダンプイメージを取得する手法について、アメリカの最新事情や技術動向を知りたかったと岩井氏は明かします。

「ユーザーからすると、今まさに被害に遭っている端末を止めずにどうするのかと思われますが、高度なマルウェアを悪用した侵害の場合は、攻撃者が侵入の痕跡を消していることが少なくありません。そういったシーンにおいて、メモリダンプの解析は不正箇所の特定が効率的に行えるメリットがあるため、注目度が高いのです。それだけに、セキュリティの本場であるアメリカの現在には大きな関心がありました」。

そして3つ目は、「エンタープライズ フォレンジックス」です。広大な国土を持つアメリカでは、インシデントのたびに現地に赴いていては間に合いません。このため、ネットワーク経由での解析が主流になっており、これについても最新の状況を知りたかったといいます。

■ 導入効果

迅速で高度な技術対応を求めるDTRSにお勧めのコンテンツ＆講師陣

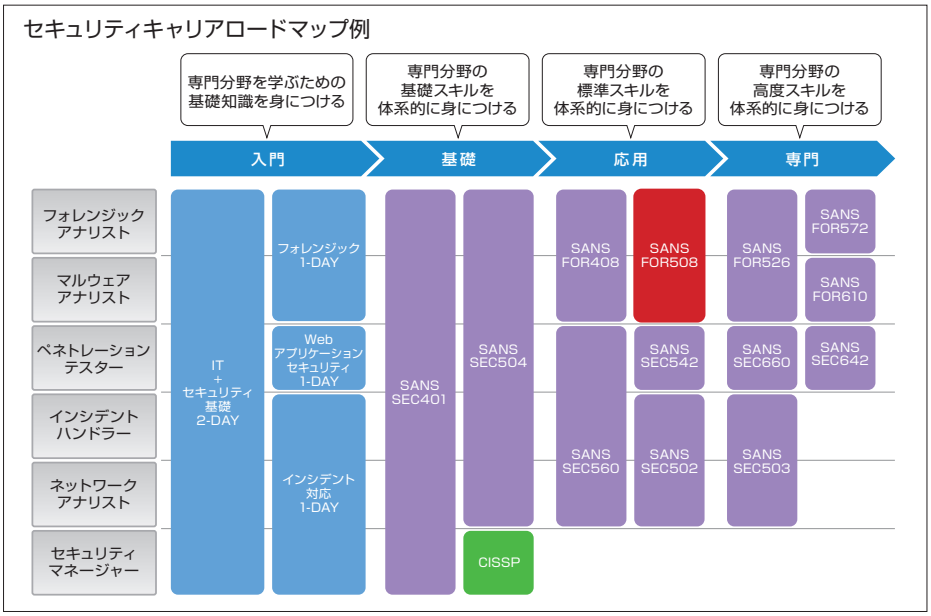
今回DTRSにFOR508をお勧めした理由について、NRIセキュアテクノロジーズ株式会社 事業開発部 担当部長 与儀大輔は、インシデント発生時に迅速かつ高度な技術的対応を要求される同社にふさわしい実践的な講義内容を挙げます。

「FOR508は、実際の問題対応を想定して、緊急事態発生から終熄までの具体的な手順をシナリオ化しています。いわゆる教科書的な座学ではなく、システム全体＝Active Directoryと被害端末であるPC3台という、あくまで実践に即したシチュエーションで組み立てられている点が、他のトレーニングにはない特長です。これも研究と実務の両面で高い知見を持つSANSの講師陣ならではです」。

このため、組織として現実に考えるべきリアルな緊急事態をベースとした学習が可能であり、FOR508で講師から聞いたなにげないテクニックが、実際のインシデント対応で思いがけなく役立ったという声も受講者から寄せられています。加えてSANSの講師は米国から第一線の専門家を招聘するため、岩井氏の大きな関心事である「グローバルスタンダードの確認」という点にも十分にお応えできると考えたと、与儀は振り返ります。

FOR508の最大の特長である「最新の技術動向にキャッチアップしたカリキュラム」も、提案の大きな理由でした。FOR508で想定するインシデント対応には、その時々にもっとも重要な脅威や主流となっているOSのバージョンに即したシナリオが盛り込まれ、随時ブラッシュアップされ続けています。

「つまり、フォレンジックの現場ですぐに活用できるテクニックや情報が、常に更新されながら盛り込まれているのです。この点でもDTRS様には必ずお役立ていただけると確信していました」（与儀）。



※本文中の組織名、職名、構成図は公開当時のものです。

■ 今後の展望

トレーニングでの実践体験が技術者自身のモチベーションをアップ

岩井氏は、サイバー攻撃被害へのダメージコントロールを十分に行う上で知っておくべき最新の基本知識と技術を、このトレーニングで習得できると指摘します。具体的な例を挙げると、たとえば10年前はインシデントが起こったらまずLANケーブルを抜くのが常識でした。しかし最近は、マルウェアが自己消滅したり、メモリ上から揮発性のデータが消えてしまうので、最初からむやみにLANケーブルを抜いてはならないという方向に変わってきています。

さらに岩井氏は、トレーニングを受講すること自体が、技術者自身のモチベーションを育てると語ります。誰かが受講したトレーニングの内容を社内にフィードバックすることも、組織全体のスキルを考える上では大切です。しかしそれ以上に、受講した本人がトレーニングによって刺激を受ける体験そのものに大きな効果があるというのです。

「ハンズオンで手を動かして成果を出し、それが自身のモチベーションを押し上げるという体験が、机上の勉強と大きく違うところです。またSANSのブランドはフォレンジック関係者にも信頼が厚く、大勢の解析技術者が集まってくるので、受講をきっかけに人的なネットワークができるのも大きなメリットです。」と語る岩井氏です。

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

9225-0032-02-1410