SANS

IT 統括部 ASICS-CSIRT
リー アルビン 氏 / 村上 治 氏

IT 統括部セキュリティリード
谷本 重和 氏

株式会社アシックス 様

SANS 情報セキュリティトレーニング　導入事例

- SEC401 Security Essentials Bootcamp Style
- SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling
- SEC511 Continuous Monitoring and Security Operations

ユーザ企業においても、インシデント業務に柔軟に対応できるCSIRT 人材の育成は不可欠 グローバルで通用するカリキュラムで効果的に知識・スキルを習得

asics

1949年の創業以来、スポーツ総合メーカーとしてグローバルで躍進を続ける株式会社アシックス。世界で健康志向が高まる一方、購買チャネルと顧客の嗜好の大きな２つのトレンドの変化が同時に進んでおり、それに伴って情報化の推進やセキュリティの確保もますます重要視されている。それを担うASICS-CSIRTではSANSトレーニングを採用。短期間で効果的なスキルアップを図っている。

■ 企業概要

株式会社アシックス

アシックスグループは、創業者が1949年にスポーツによる青少年の育成を通じて社会の発展に貢献することを志して興された。「スポーツでつちかった知的技術により、質の高いライフスタイルを創造する」のビジョンの下、世界の人々が健康で幸せな生活を実現できる製品やサービスの提供を使命としている。

https://corp.asics.com/jp/about_asics

■導入背景

ユーザ企業としての情報セキュリティ人材の必要性を感じた

『ユーザ企業において、サイバーセキュリティのトップガン人材や情報セキュリティの専門家までは必要ない』ということには、多くの方が同意すると思う。その一方で、外部委託先のセキュリティエンジニアやアナリストとコミュニケーションをする際、その前提となる最低限の知識が必要であることにも、多くの方がうなずくはずだ。

「ユーザ企業においても、情報セキュリティを体系的に学習する機会やサイバーセキュリティ業務に従事するメンバーへのキャリアパスの明示は不可欠です。チームメンバーのキャリアアップと将来を見すえ、当社の情報セキュリティ人材の育成には、グローバルで通用する国際的な資格体系を有するようなカリキュラムが必要だと考えました。特に、インシデント業務に柔軟に対応できるCSIRT人材の育成には、SANSトレーニングが最も効果的な投資効果を生み出すと判断しました」(谷本氏)

■導入経路

各自の目的に合ったコースを選択しスキルを習得する

アシックスでは、ASICS-CSIRTを2017年10月に設立し、本格的なインシデント対応業務としてSOCやSIEMなどのログ監視システムの導入を推進してきた。

「このCSIRT機能の本格的な運用を目指し、情報セキュリティ業務を担当して2年あまりになる村上、リーの両氏に、CSIRT人材としてステップアップを図ってもらうことにしました。村上には『インシデント対応やログ監視分析の具体的な手法を習得すること』を、リーには『グローバル拠点を含むアシックスグループの全従業員を対象とした情報セキュリティ向上のための具体策の立案・推進を図るスキルを習得すること』を期待してコースを選定しました」(谷本氏)

こうして、村上氏が、SEC504 (Hacker Tools, Techniques, Exploits, and Incident Handling)とSEC511 (Continuous Monitoring and Security Operations) を、リー氏がSEC401 (Security Essentials Bootcamp Style)を受講した。

「SEC504は攻撃手法の技術的な理解とその対策、SEC511はセキュリティ監視技術に関する内容でしたが、その両方のトレーニングに参加したことは、大変有意義な経験となりました。受講したトレーニングの内容は、1日数百ページの分量の独自テキストに基づく講義と、教材として配付された仮想環境で行う多くのハンズオン(実務演習)でした。最終日はCTF (Capture The Flag)を体験しました。参加者がその場でチームを作り、前日までの５日間に学んだスキルを活用して課題に取り組むものです。SEC511のCTFでは、攻撃後に得られたログやイベ

ントを自分たちで解析しつつハッキングのプロセスを追うのはとても骨の折れる作業でしたが、攻撃者の行動や考え方を理解する上で重要な気づきとなりました」(村上氏)

一方、リー氏が受講したSEC401は、これから情報セキュリティ業務を本格的に行う方を対象として、あらゆるトピックを網羅する基礎的なコースである。『Bootcamp Style』と銘打っているとおり、座学での講義に加えてハンズオンも用意されている。セキュリティ業務に従事する多くの人が知っている(使っている)ツールやテクニックを体験してもらえるように設計されている。

「とにかくインストラクターの説明がとても分かりやすかったです。SEC401は情報セキュリティを学ぶ初学者に対して十分示唆に富んだ内容となっていて、実務にも活用できると感じました」(リー氏)

■導入効果

体系的な知識やスキルがほとんどない状態での研修受講

2016年からセキュリティ業務に従事してきた村上氏だが、ユーザ企業での経験しかないということもあってか、自身のサイバーセキュリティに関する技術や知識が十分ではないと感じていたという。

「例えば自社のWebサイトのセキュリティ診断をする際にも、外部委託先の技術者から触りの部分を教えてもらいながらやったりするわけです。足手まといになるわけにはいきませんから、こちらとしてもその経験だけですべてをマスターするには限界がありました」(村上氏)

そうした中で研修に参加して印象的だったことが、テキストに書かれている内容が、実際の業務経験に基づいた実践的な内容であったことだと村上氏は言う。

「とても説得力があり、かつ示唆に富んだ内容でした。セキュリティアナリストの方であれば当然認識済みのことですが、例えば、ログ監視(モニタリング)においては、平常時の通信の状態を把握しておくことが重要で、それを把握するにはどうすればいいかを学びました。もし不審な通信があれば、その異常値にも自ずと気づくものだということをあらためて再認識しました。ハンズオンにおいても、『Windowsのパスワードはツールを利用することで、簡単に判明することができる』といった頭の中では理解していることを、実際に自分でクラッキングを行って確認できたこともよかったです」(村上氏)

SEC401のハンズオンでは、コマンドラインツールを体験するハンズオンも多数用意されている。毎回半数ほどの参加者の方々が、ほぼ初めてコマンドラインを体験するのがこのコースの平均だ。

「私もLinuxコマンドの知識がほとんどなかったため、ハンズオンのときには理解をするのに少し時間がかかりました。その際も、インストラクターの丁寧な説明にはとても感謝しています」(リー氏)

両氏はトレーニングの受講後も、個別にインストラクター陣から必要に応じてフォローアップしてもらっているそうだ。

■今後の展望

研修で得たテクニックを業務に活かし、さらなるスキルアップを目指す

村上氏は本社の情報セキュリティ担当者としてインシデント対応や脆弱性管理など、主にセキュリティアナリストの業務を担っている。

「具体的には、外部委託先のSOC(Security Operation Center)からのアラートを受け、社内デバイスのログ分析を行い、端末の特定や状況確認を行った後、感染端末をネットワークから隔離します。研修受講後は、今までわからなかったことも含めて知識が整理でき、習得したテクニックを使っています。現在は、事後対応活動に注力していますが、今後は、導入済みのSIEMやEDRを利活用し、早期にインシデントの予兆を把握するインテリジェンス機能を整備し、事前対応の課題にも取り組む予定です」(村上氏)

もちろんSANSのコースには、そうしたニーズを満たすものも多くラインナップされている。FOR508、FOR578などはその一例だ。

「私は、ASICS-CSIRTの海外POC(Point of Contact)として、海外販社のIT担当者とのコミュニケーションやインシデント発生時におけるコーディネーション業務を担当しています。最近は、海外販社を含むアシックスグループの従業員に対する情報セキュリティ意識向上のためのトレーニングの推進や啓蒙活動を実施していますが、研修で学んだトピックを参考にしながら自社の実情を加味したコンテンツを作成し、講師として教えるようにもなりました」(リー氏)

リー氏は社内向け研修のさらなる拡充を企画しつつ、さらに技術的なスキルも身につけていきたいということだ。

■メッセージ

同様の業務を行う他社の皆さんへ

最後に、両氏からユーザ企業のセキュリティ業務を担う皆さんに対してメッセージをもらった。

「SANSトレーニングには豊富なコースが用意されており、サイバーセキュリティのトップガンや専門家が『自身の技術や知見のレベルアップや自己研鑽に使うもの』と認識していましたが、各コースの中には、ユーザ企業のセキュリティ担当者としても十分に知っておくべき知識や内容が含まれています。例えば、私が受講したSEC504では、攻撃者が侵入に成功するまでのプロセスを一通り体験することができます。自社の情報資産をどのように守ればいいのかを考える上で、『攻撃者の手口を知るハンズオン学習は不可欠な機会である』と思います。全6日間のトレーニングは、実際、体力的にも知力的にもとてもハードなものですが、ぜひチャレンジすることをお勧めします。加えて、トレーニング期間に、共に受講するメンバーとの交流が、自分自身の交遊の幅を広げ、かつ、見聞を深めるきっかけにもなると思います」(村上氏)

「情報セキュリティチーム強化のために、SEC401はとてもいいコースだと思います。このコースを受講することによって、情報セキュリティ業務に必要なスキルや、業務対応のサポート範囲を広めることが可能になり、チームの成熟度を高めることができると思います」(リー氏)

『SANSトレーニグを選択したことは間違ってなかった』と、取材の最後にコメントしてくれた谷本氏の表情が印象的だった。

SANS Institute(日本オフィス)
〒100-0004
東京都千代田区大手町1-7-2 東京サンケイビル
Tel: 03-3242-6276
ホームページ　https://www.sans.org
メールアドレス　japan@sans.org

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: 03-7606-0606　Fax: 03-6706-0599
ホームページ　https://www.nri-secure.co.jp
メールアドレス　info@nri-secure.co.jp