シスコのサイバーセキュリティへの取組み

シスコシステムズ合同会社
最高技術責任者（CTO） 兼 最高セキュリティ責任者
濱田 義之

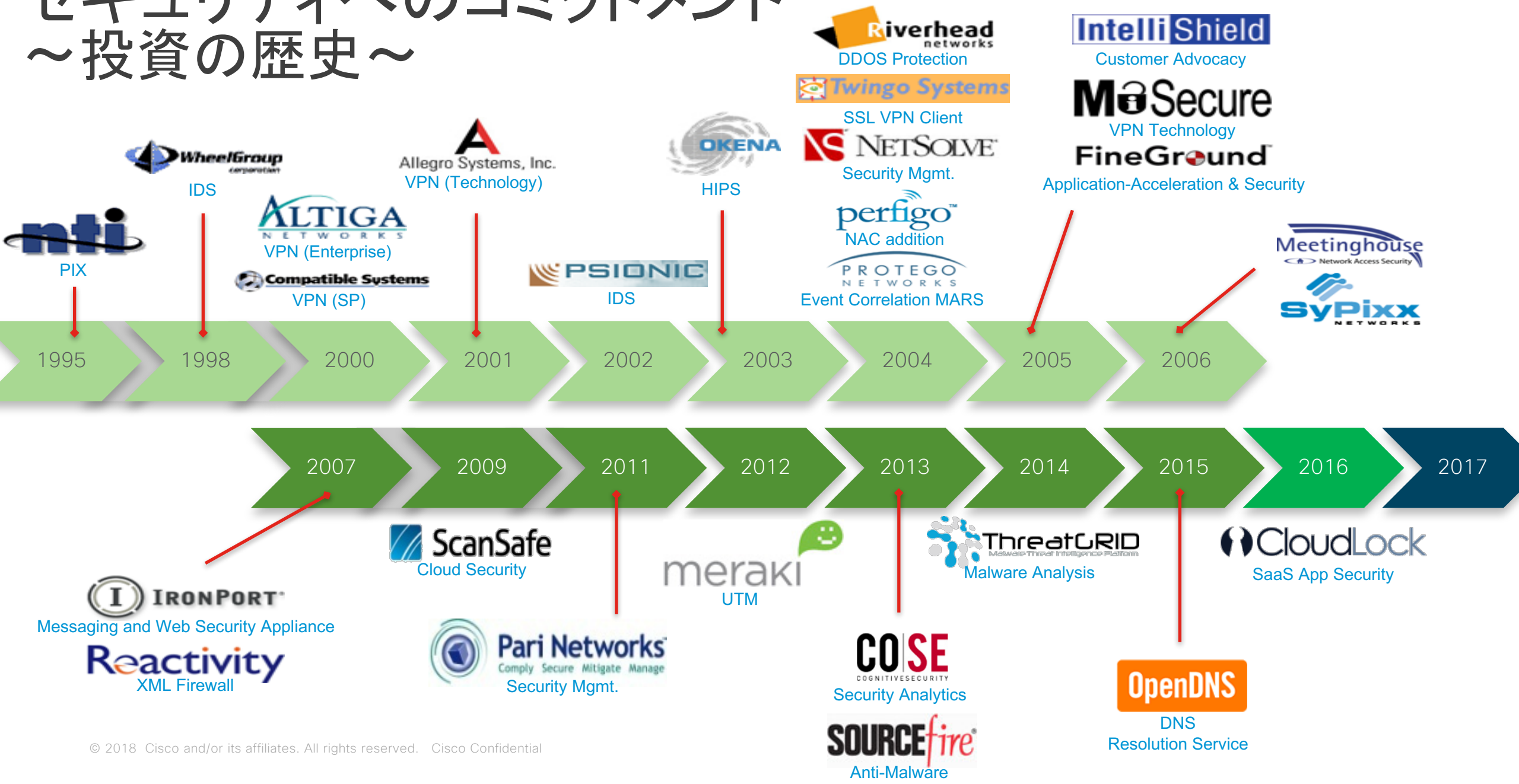
2018年5月16日

シスコ＝セキュリティ？

CISCO

=

セキュリティへのコミットメント ～投資の歴史～



シスコ　セキュリティポートフォリオ

脅威インテリジェンス- Talos

ネットワーク

- DNS
- Advanced malware
- NGFW/ NGIPS
- Network analytics
- ETA
- Network access
- Email security
- Web

エンドポイント

- DNS
- Advanced malware
- VPN
- Cloud access

クラウド

- DNS
- Advanced malware
- Email security
- Web
- Cloud access

サービス

- Sourcefire社の脆弱性リサーチチームがルーツ
- 2013年のSourcefire社買収時、Cisco Security Intelligence Operation (SIO) と合併し、新たにTALOSとして発足
- 主要拠点は、メリーランド州フルトン、テキサス州オースティン、カリフォルニア州サンノゼ
- 270名を越える担当者が、サイバーセキュリティ脅威分析に特化して活動中

TALOS チーム構成

Matt Watchinski

エンジン開発

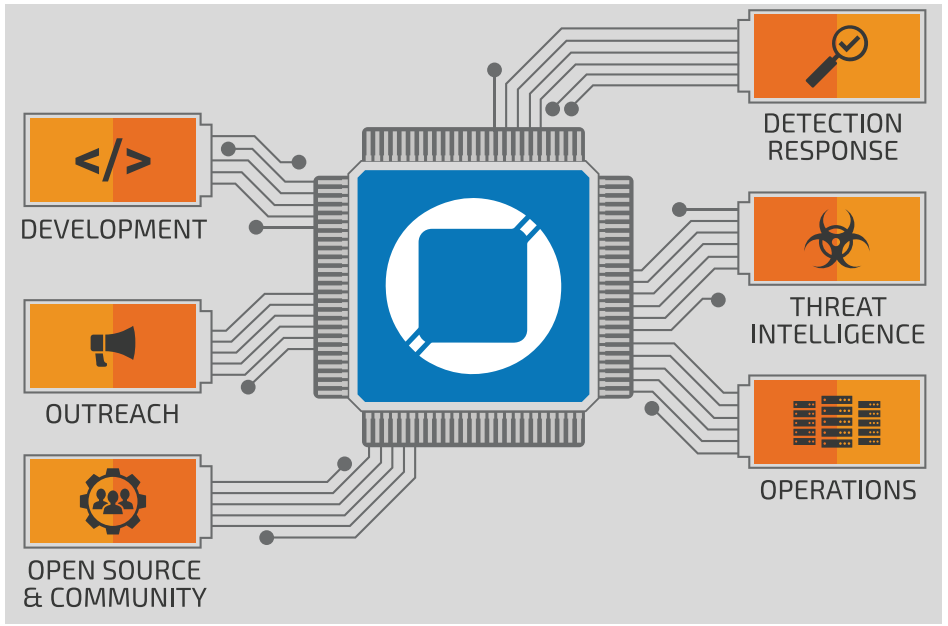
Luci Lagrimas

アウトリーチ
（情報発信・広報）

Craig Williams

オープンソース
コミュニティ連携

Joel Esler



Chris Marshall

マルウェア・スパム
分析・データ転換

Matt Olney

脅威インテリジェンス・
検出、攻撃者属性

Nigel Houghton

脆弱性R&D
ゼロデイ

数十万
顧客

数百万
ユーザ

100TB
1日あたりの
脅威テレメトリ

270+
リサーチャー

数百
脅威解析
エンジン

Software | Vulnerability Information | Reputation Center | Library | TALOS | Support Communities | About | Careers | Blog

http://blog.talosintelligence.com/

MONDAY, FEBRUARY 12, 2018

Olympic Destroyer Takes Aim At Winter Olympics

This blog post is authored by Warren Mercer and Paul Rascagneres. Ben Baker and Matthew Molyett contributed to this post.

Update 2/13 08:30 We have updated the information regarding the use of stolen credentials

Update 2/12 12:00: We have updated the destructor section with action taken against mapped file shares

SUMMARY

The Winter Olympics this year is being held in Pyeongchang, South Korea. The Guardian, a UK Newspaper reported an article that suggested the Olympic computer systems suffered technical issues during the opening ceremony. Officials at the games confirmed some technical issues to non-critical systems and they completed recovery within around 12 hours. Sunday 11th February the Olympic games officials confirmed a cyber attack occurred but did not comment or speculate further.

Talos have identified the samples, with moderate confidence, used in this attack. The infection vector is currently unknown as we continue to investigate. The samples identified, however, are not from adversaries looking for information from the games but instead they are aimed to disrupt the games. The samples analysed appear to perform only destructive functionality. There does not appear to be any exfiltration of data. Analysis shows that actors are again favouring legitimate pieces of software as PsExec functionality is identified within the sample. The destructive nature of this malware aims to render the machine unusable by deleting shadow copies, event logs and trying to use PsExec & WMI to further move through the environment. This is something we have witnessed previously with BadRabbit and Nyetya.

OLYMPIC DESTROYER WORKFLOW

Search Blog

SUBSCRIBE TO OUR FEED

Posts

Comments

Subscribe

BLOG ARCHIVE

▼ 2018 (26)

▼ FEBRUARY

Threat Round

COINHOARDE Bitcoin Phis

Microsoft Patc

Olympic Destr Olympics

Threat Round

Targeted Attac

Beers with Tal Rob Joyce

Flash 0-Day In Controls...

► JANUARY

► 2017 (172)

► 2016 (98)

► 2015 (62)

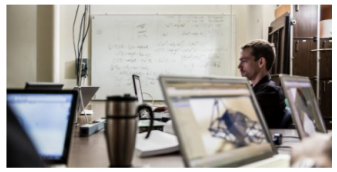
► 2014 (67)

► 2013 (30)

https://gblogs.cisco.com/jp/author/talosjapan

cisco Cisco Japan Blog

Cisco Japan Blog > セキュリティ



セキュリティ

冬季オリンピックを標的とする「オリンピック デストロイヤー」

TALOS Japan - 2018年2月15日 8:30 PM

執筆/投稿者：Warren Mercer、Paul Rascagneres

2 月12 日 12:00 時：マッピング済みファイル共有に対するアクションについて、「破壊目的のマルウェア」の項を更新

まとめ

今はちょうど冬季オリンピックが韓国の平昌で開催中ですが、英国のガーディアン紙の記事によると、オリンピックの開会式でコンピュータ システムに技術的な問題が発生したようです。大会関係者は、基幹システムを除く一部に技術的な問題が発生し、約 12 時間以内に復旧したことを公表しています。さらに 2 月 11 日（日）にはサイバー攻撃を受けたことも公表しましたが、それ以上のコメントや推測は控えています。

今回の攻撃で使用されたと（中程度の確率で）考えられるマルウェアについて、Talos はそのサンプルを特定しました。ただし調査中の現段階で感染ベクターは確認されていません。特定されたサンプルに

登録

メールアドレスを入力

登録する

フォローする

人気のコンテンツ

シスコ派遣記Season2

連載：アーキテクチャ考

Cisco Talos

シスコ派遣記

Cisco IOS フル活用への道

カテゴリー

Cisco Japan

エンタープライズ ネットワーク

Cisco DNA

Cisco IOS

ネットワーク管理

セキュリティ

モビリティ

ワイヤレス

データセンター/仮想化

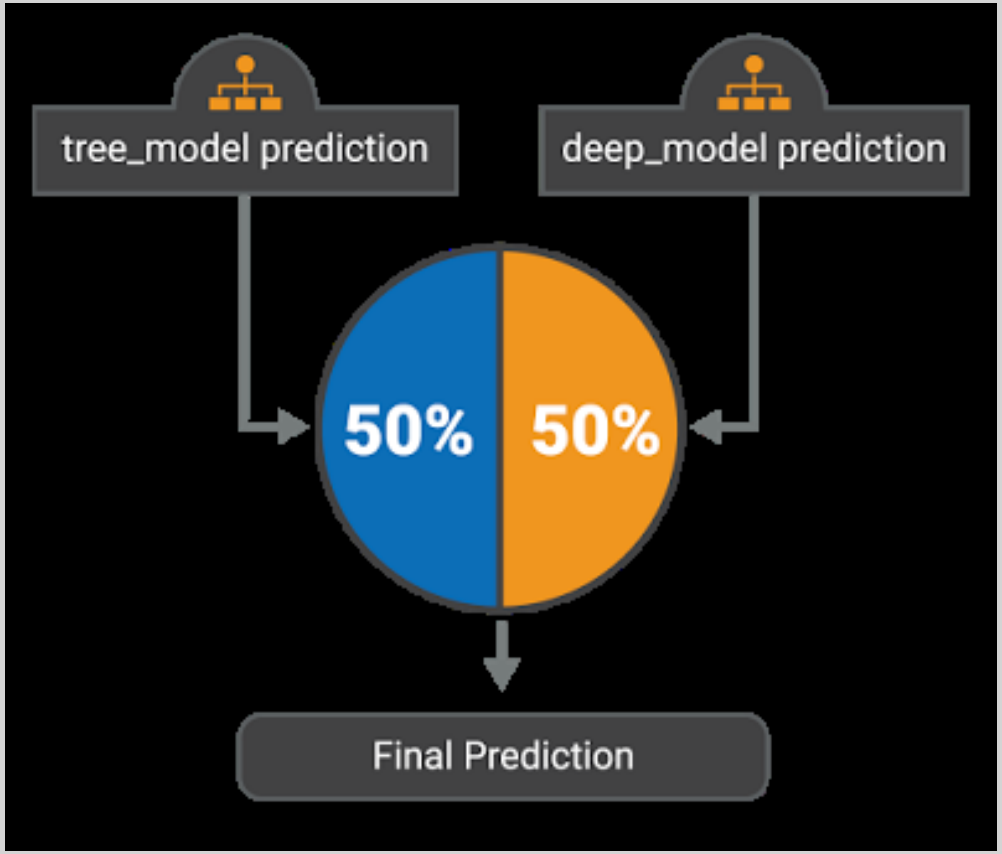
フェイクニュースチャレンジ

http://www.fakenewschallenge.org/

- フェイクニュースの問題への対処を目標に、学界や業界の研究者により“Fake News Challenge”が誕生
- ステージ1(FNC-1)： スタンス検出
  記事の見出し(主張)と本文が合致しているか、見出しについて議論しているかを見分けることによってフェイクニュースを識別する

Talos：FNC-1 に挑戦

ツリーモデルの予測　　深層モデルの予測



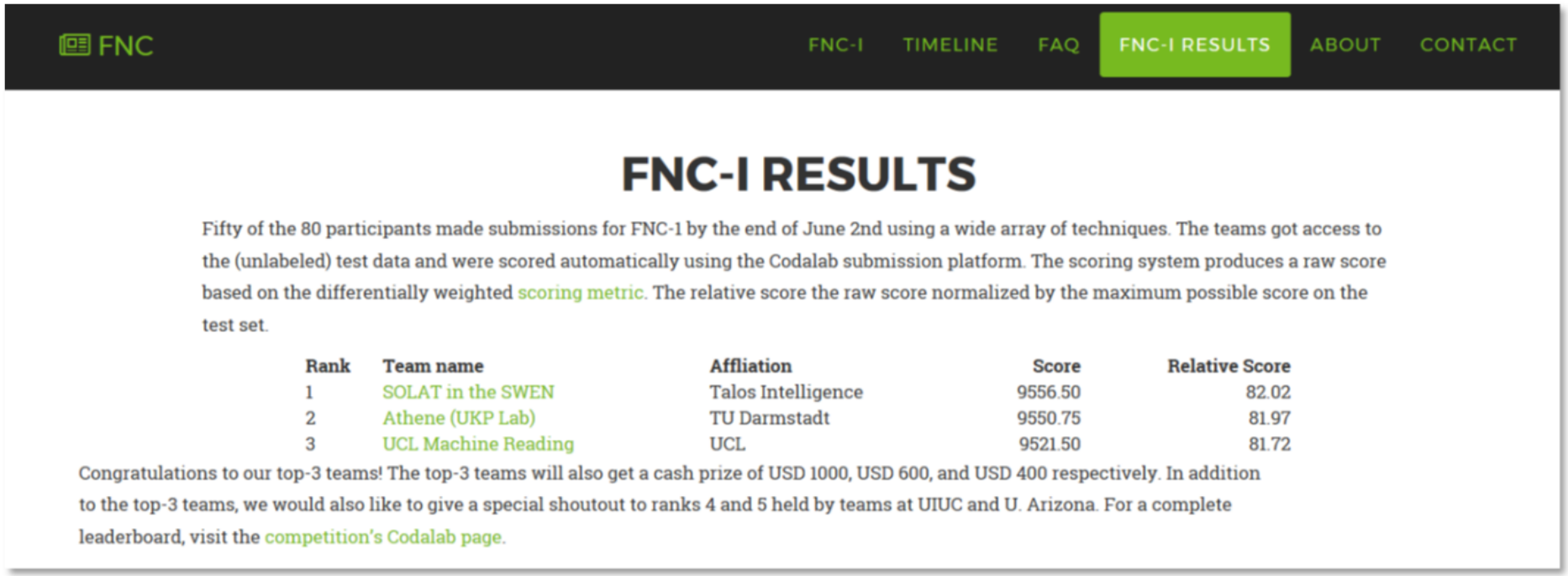
最終予測

SOLaT IN THE SWEN

勾配ブースティング意思決定ツリー（GBDT）と
深層畳み込みニューラル ネットワーク（CNN）を
50/50 の加重平均で組み合わせたもの

Talos GitHubにてコードを公開中
https://github.com/Cisco-Talos/fnc-1/

Talos：FNC-1で 1位に



FNC

FNC-I　TIMELINE　FAQ　FNC-I RESULTS　ABOUT　CONTACT

FNC-I RESULTS

Fifty of the 80 participants made submissions for FNC-1 by the end of June 2nd using a wide array of techniques. The teams got access to the (unlabeled) test data and were scored automatically using the Codalab submission platform. The scoring system produces a raw score based on the differentially weighted scoring metric. The relative score the raw score normalized by the maximum possible score on the test set.

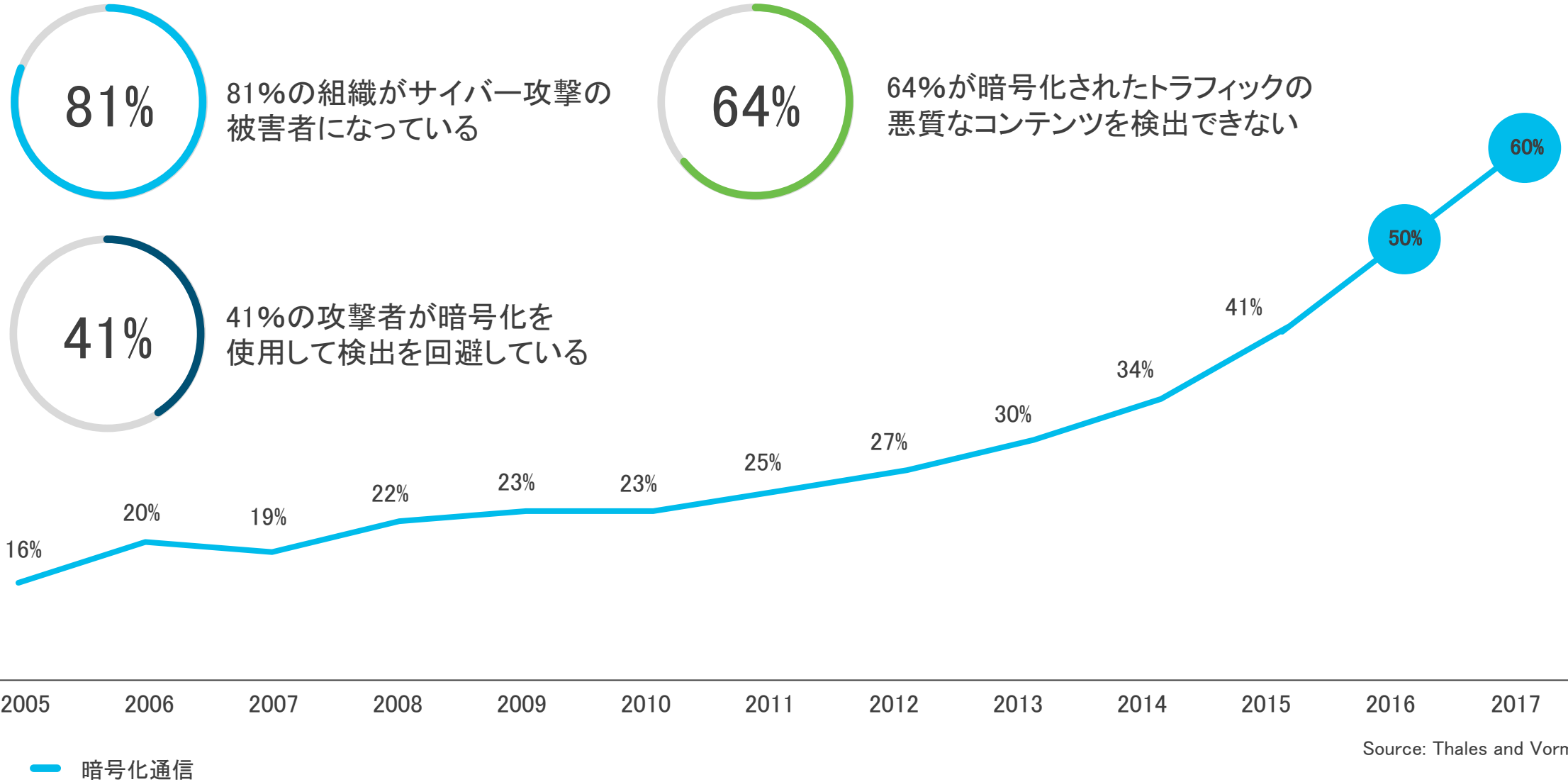
Rank	Team name	Affliation	Score	Relative Score
1	SOLAT in the SWEN	Talos Intelligence	9556.50	82.02
2	Athene (UKP Lab)	TU Darmstadt	9550.75	81.97
3	UCL Machine Reading	UCL	9521.50	81.72

Congratulations to our top-3 teams! The top-3 teams will also get a cash prize of USD 1000, USD 600, and USD 400 respectively. In addition to the top-3 teams, we would also like to give a special shoutout to ranks 4 and 5 held by teams at UIUC and U. Arizona. For a complete leaderboard, visit the competition's Codalab page.

80を超える参加チーム中、Talosが1位にランキング

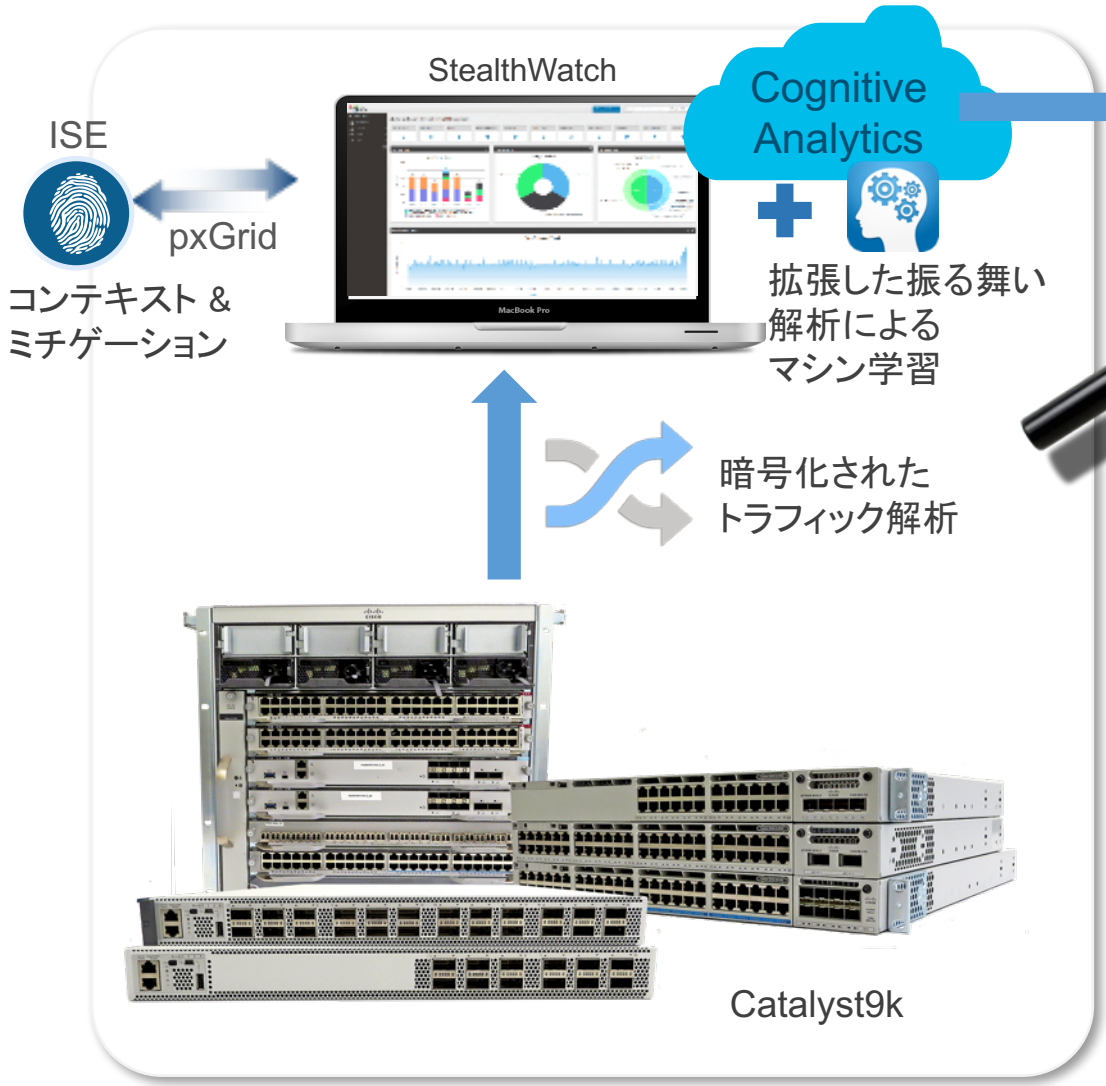
TALOS IN THE NEWS

増大する暗号化マルウェアの脅威



Source: Thales and Vormetric

Encrypted Traffic Analytics 概要



暗号化されたトラフィックにおいて
“マルウェア”と解析 → 99%以上の効果

ネットワーク
テレメトリーベース
(No Decryption)

ラインレート
パフォーマンス

投資の
最適化

管理の
シンプル化

グローバルレベル
による脅威情報と
の相関関係性

ISEおよびネットワークに
よるインシデント緩和

ERSPAN はディープな
解析を行うために
トラフィックを監視

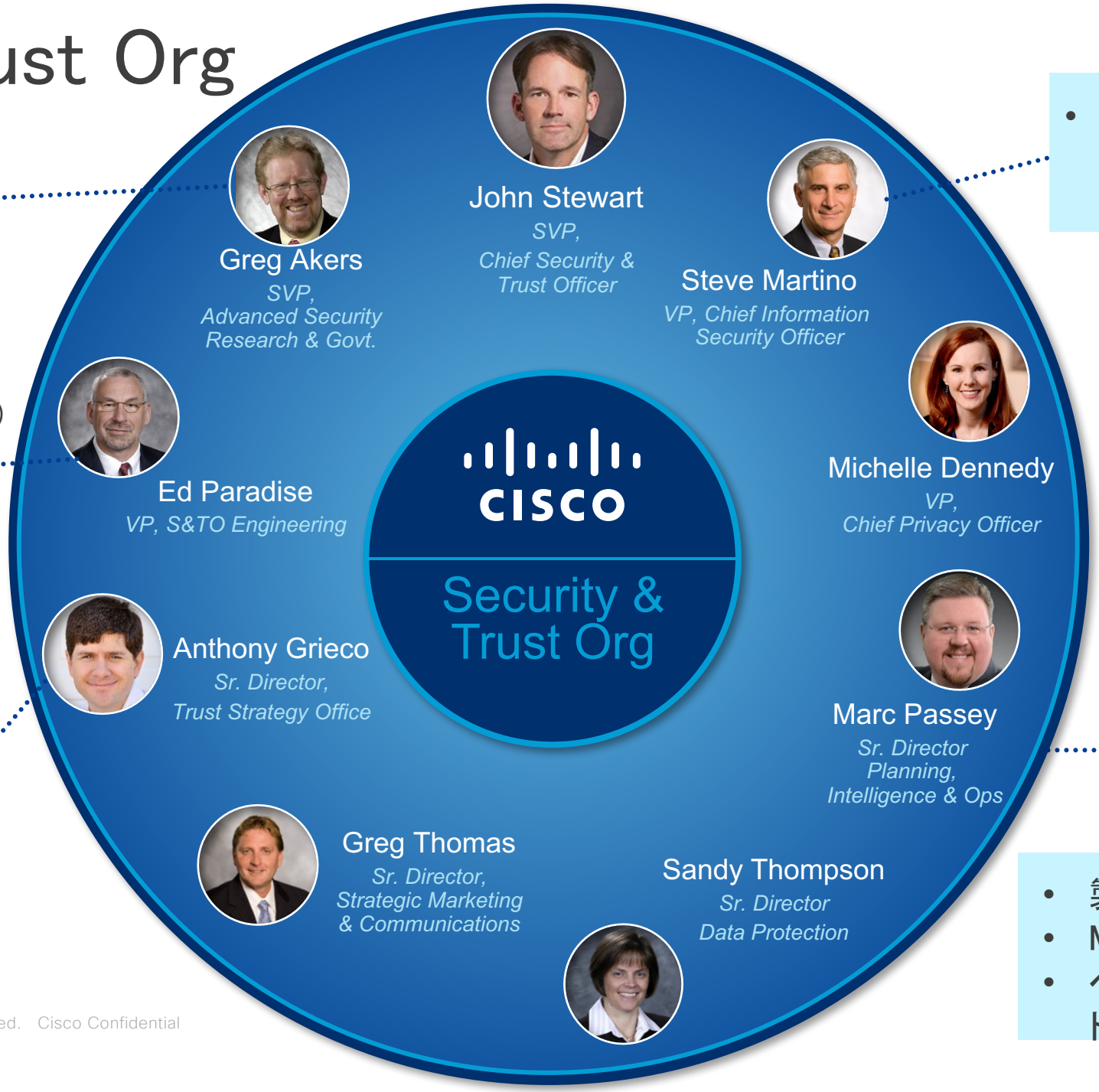
Security & Trust

Security & Trust Org

- セキュリティ先端研究
- 学術研究連携・投資

- 開発プロセス (CSDL: Cisco Secure Development Lifecycle)
- 信頼性技術開発 (Trustworthy technology)
- バリューチェーンリスク管理

- 最重要国・地域連携強化
- IoTセキュリティ、サイバー人材育成
- データ法令順守



- Infosec CSIRT (社内CISRT、脅威情報チームも所属)

- PSIRT
- Advanced Svc
- Security Prod Engineering

- 製品脆弱性調査
- MSSP/MDR
- ペンテスト、コンサル、トレーニング

IoTデバイスに対する懸念点

機器の増加

脆弱性

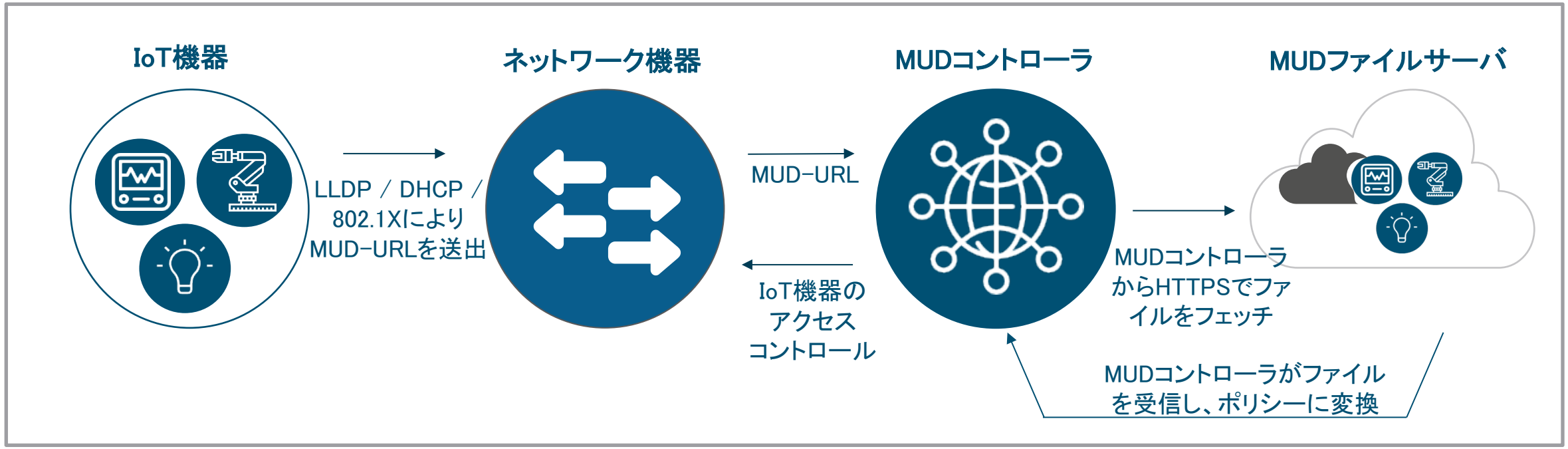
リソース不足

可視化

標準化

IoTセキュリティ標準化活動： MUDアーキテクチャ

MUDスタンダードはデバイスの可視化とセグメントの自動化を標準化する動きです。ネットワーク接続時にデバイス自ら可視化情報を流し、ベンダー予め用意したポリシーに沿ってネットワークで動作するフローをIETFで標準化。ITやセキュリティーアドミンの工数を大幅に軽減することを一番の目的としています。



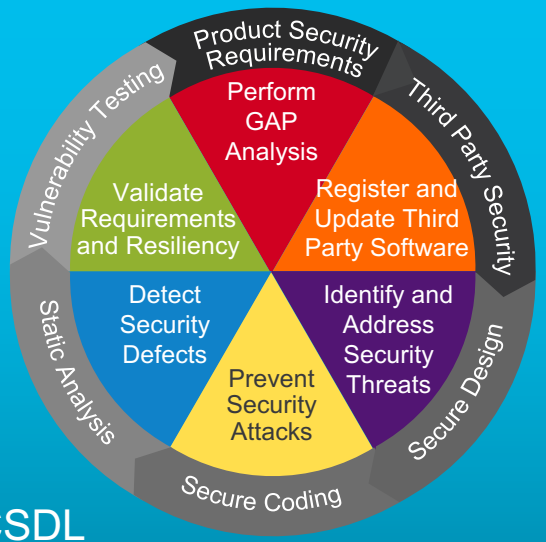
MUD: Manufacturer Usage Descriptions

信頼される製品開発への基礎

プロセス ---------- テクノロジー ---------- ポリシー

Secure Process

Lifecycle / Security Baseline



Trustworthy Systems Technology

Common Modules and Hardware

Visibility and Control

Secure Communications

Platform Integrity

Secure Standards

Information Assurance (IA)

Common Criteria

ISO 27034

FIPS/USGv6

TCG

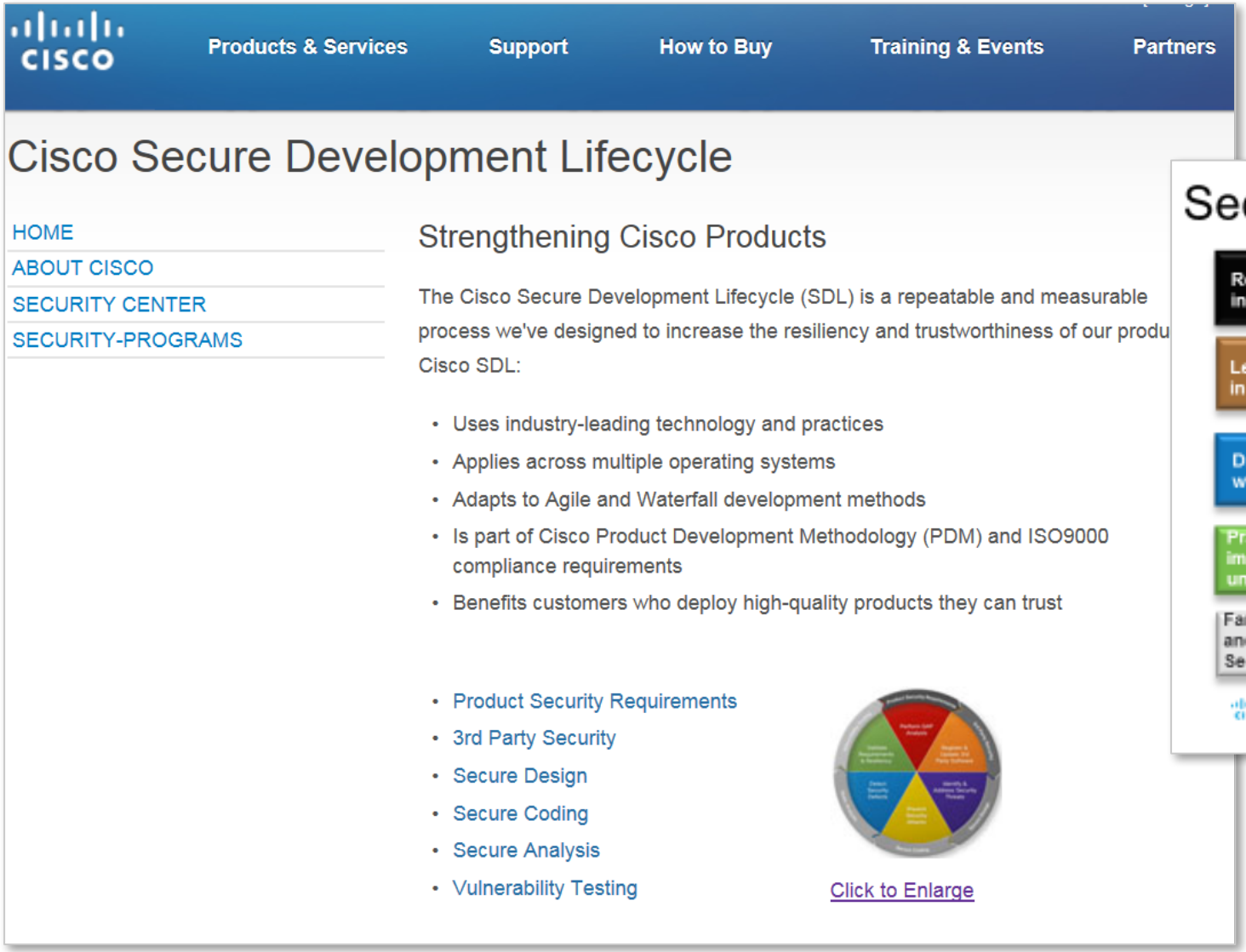
Prevention

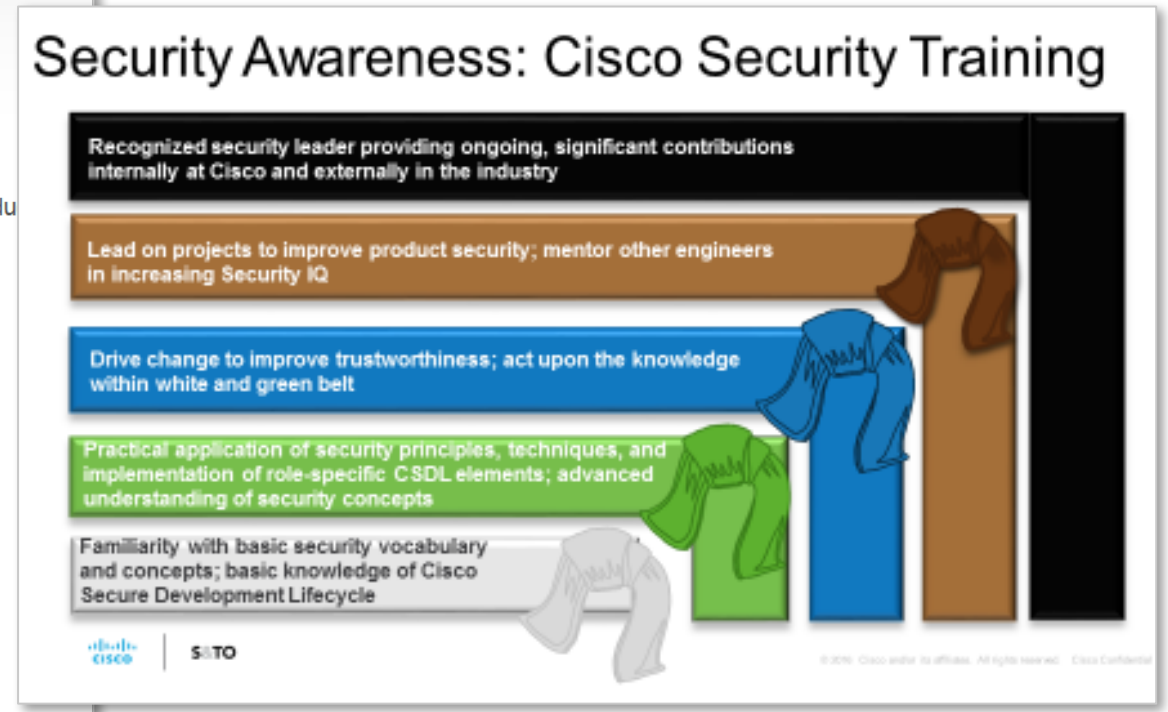
Detection

Recovery

Cisco Secure Development Lifecycle

https://www.cisco.com/c/en/us/about/security-center/security-programs/secure-development-lifecycle.html





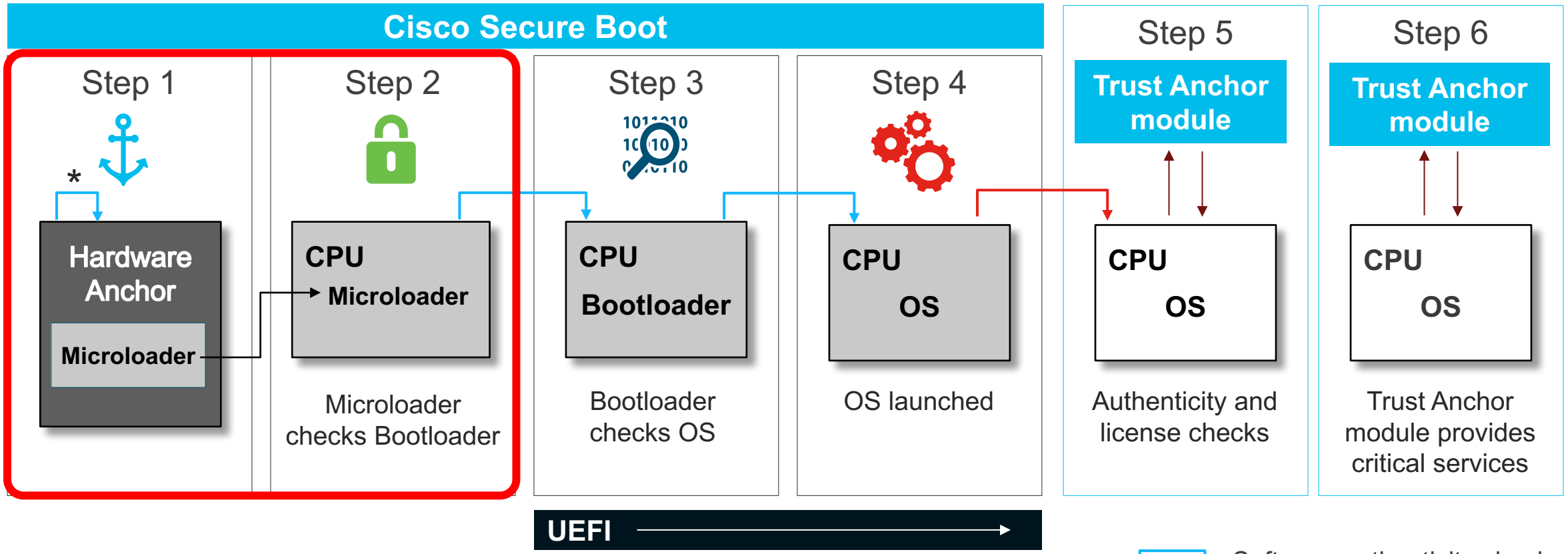
セキュリティ社内トレーニング：NINJA Program

※日本語化および外部公開検討中

Trustworthy Technology: 堅牢なプラットフォームへ

Microloader: 起動プロセス（Bootloader/BIOS）のチェック機能をハードウェアレベルに組み込むことによって、ソフトウェアの整合性・完全性を担保

Trust Anchor Module: 正規のハードウェア情報が刻印されたチップを搭載。OSが確認し、正規のハードウェアであることを担保（正規のものでない場合にはコンソール画面にアラート表示）



バリューチェーンセキュリティ

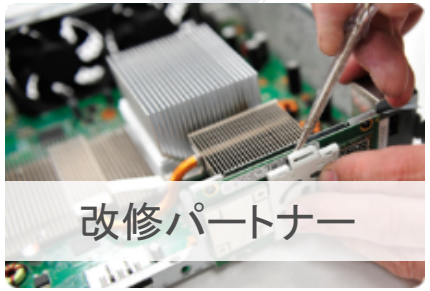
74% 過去3年、少なくとも1件のサードパーティ関連インシデントを経験*[1]

72% 最大80%のセキュリティを、サードパーティに依存している*[2]

75-80% 過去7年間のサードパーティに関係するセキュリティインシデント*[3]

1: 2017 Deloitte Third Party Risk Management Global Survey
2: 2017 Cisco Annual Cybersecurity Report
3: 2017 Verizon Data Breach Investigation Report

シスコにおけるサードパーティエコシステム



シスコのバリューチェーンセキュリティプログラム

ゆりかごから墓場まで、妥協しないソリューションライフサイクル

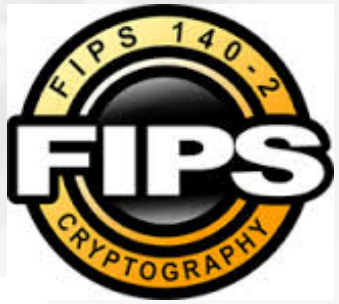
階層化アプローチ

- 論理的セキュリティ
- ネットワークセキュリティ
- 行動(規律)セキュリティ
- 技術的セキュリティ
- 物理的セキュリティ

https://www.cisco.com/c/en/us/about/trust-center/global-value-chain-security.html

Global Certification: 認証関連

- Common Criteria
- FIPS 140-2
- DoD UC APL
- USGv6
- IPv6 Ready Logo
- FedRAMP
- Commercial Solutions for Classified (CSfC)
- GDPR, CBPR etc



認証プログラム要約

	FIPS 140-2	Common Criteria	DoD UC APL	USGv6	CSfC	FedRAMP
概要	暗号モジュールのセキュリティ要件の適合性検証	製品のセキュリティ機能のシステムテスト（認証：2年更新）	国防・軍の固有および相互運用にかかる機能の検証（認証：3年更新）	IPv6対応製品のコンプライアンス評価	COTSの機密情報取り扱いの適合認定	クラウドサービスのセキュリティ認証
対象製品	•暗号化製品	•現在: 主要なセキュリティ製品 •将来: すべての製品	•UC •LAN •WLAN •Security	•すべて	•IA製品	•クラウド関連製品およびサービス
関連性	•国ごと •FIPS for US, UK, Canada	•26か国	•US DoD	•USG •ReadyLogo	• USG	•USG, some US state and local
証明機関	•NIST/CSEC	•国ごと •NIAP in US	•US DoD	•NIST	NSA	JAB or Govt Agency

日本国内での取り組み

サイバーセキュリティ関連機関との連携を強化

JC3 日本サイバー犯罪対策センター

Financials ISAC Japan Information Sharing and Analysis Center

NICT

CSSC 技術研究組合 制御システムセキュリティセンター Control System Security Center

JPCERT CC®

InterNational Cyber Security Center of Excellence (INCS-CoE)

Open Government Consortium Open Platform Sharing

INTERPOL

INTERPOL Global Complex for Innovation

情報セキュリティワークショップin越後湯沢2017

サイバーセキュリティシンポジウム道後 2018 Cyber Security Symposium in Dogo

PAC SEC Tokyo November 2017

Nov.7 (Tue) - 10 (Fri), 2017 CODE BLUE @TOKYO

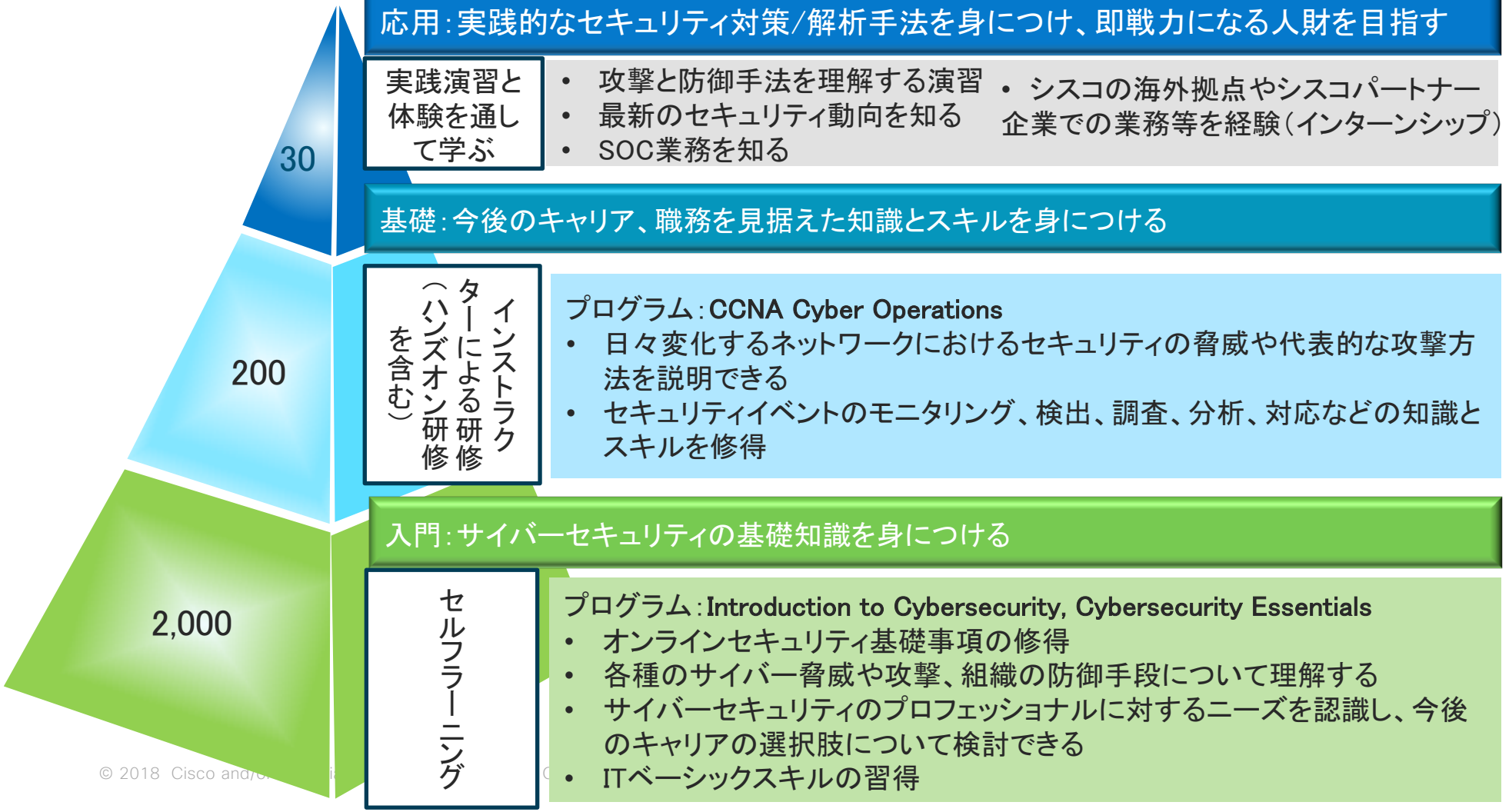
SHIRAHAMA CYBER CRIME SYMPOSIUM

International Cybersecurity Symposium

人材育成：サイバーセキュリティスカラーシップ導入

目指す職種（例）

- ネットワーク セキュリティスペシャリスト
- セキュリティ管理者
- インストラクター
- SOCオペレータ



応用：実践的なセキュリティ対策/解析手法を身につけ、即戦力になる人財を目指す

実践演習と体験を通して学ぶ

- 攻撃と防御手法を理解する演習
- 最新のセキュリティ動向を知る
- SOC業務を知る
- シスコの海外拠点やシスコパートナー企業での業務等を経験（インターンシップ）

基礎：今後のキャリア、職務を見据えた知識とスキルを身につける

インストラクターによる研修（ハンズオン研修を含む）

プログラム：CCNA Cyber Operations

- 日々変化するネットワークにおけるセキュリティの脅威や代表的な攻撃方法を説明できる
- セキュリティイベントのモニタリング、検出、調査、分析、対応などの知識とスキルを修得

入門：サイバーセキュリティの基礎知識を身につける

セルフラーニング

プログラム：Introduction to Cybersecurity, Cybersecurity Essentials

- オンラインセキュリティ基礎事項の修得
- 各種のサイバー脅威や攻撃、組織の防御手段について理解する
- サイバーセキュリティのプロフェッショナルに対するニーズを認識し、今後のキャリアの選択肢について検討できる
- ITベーシックスキルの習得

国内の育成事業との連携

enpit Security

KOSEN 国立高等専門学校機構

AITAC

2017年秋より
オンライン受付開始

サイバーセキュリティスカラーシップ進捗状況

CCNA Cyber Ops トライアル
26名修了

オンライントレーニング受講生
700名以上

- 一部高専にて今秋よりカリキュラム提供開始
- enPIT securityにて、19年春より先進演習科目として開講予定

社会人向け無料オンライントレーニングプログラム

Cisco Networking Academy

https://www.netacad.com/campaign/486851

Introduction to Cybersecurity
サイバーセキュリティ入門

サイバーセキュリティにおけるキャリア機会について触れながら、オンラインやソーシャルメディアから自分自身を保護する方法について学びましょう。

開始時点　時間: 15 時間

コースのまとめ

「サイバーセキュリティ入門」コースでは、サイバーセキュリティに関する幅広いトピックを各自にピッタリの方法で学習できます。オンラインおよびソーシャル メディア上の個人データおよびプライバシーを保護する方法や、サイバー セキュリティの見識と理解を必要とする IT 業務が増えている理由について学習します。

- サイバーセキュリティとは何か、またそれが自分自身や自分のキャリアにとって何を意味するのかについても学べます。
- 最も一般的な脅威、攻撃、脆弱性を理解し、オンラインで安全性を強化する方法を学びましょう。
- 企業がサイバー攻撃から事業を守る方法や、セキュリティ人材への需要が増えている理由をご紹介します。

今すぐ登録

電子メール

送信

入門編：全職種の方々へのリテラシー教育

Cisco Networking Academy

https://www.netacad.com/campaign/598101/

Cybersecurity Essentials

情報とネットワークのセキュリティの基本原則、手順、および実践を学びましょう。

中級　30時間　セルフ スタディ

コースのまとめ

Cybersecurity Essentialsコースは、サイバーセキュリティの基礎、ならびに情報セキュリティとネットワークセキュリティとどのように関係しているかを学習することができます。また、サイバー犯罪の特徴、セキュリティ原則、技術、ネットワークを守るための手順を紹介します。インタラクティブなマルチメディアコンテンツ、ラボ活動、マルチインダストリーのケーススタディを通じて、サイバーセキュリティにおけるキャリアを追求するための技術的で専門的なスキルを身につけることができます。

- データの機密性、整合性、可用性、およびセキュリティ制御をネットワーク、サーバー、アプリケーションに実装する手順を学びます。

今すぐ登録

電子メール

送信

基礎編：IT・情報セキュリティ担当者向け教育


CISCO