Symantec™

Detect, Prevent and Remediate the Cyber attack

Nelson Yuen

Senior Systems Engineer

Symantec

ISTR20

INTERNET SECURITY THREAT REPORT

Overview of the Local Security Landscape

IP camera footages broadcasted live online

- In September, 2014, more than 1,000 IP cameras in Hong Kong were found vulnerable with private footages easily accessible online

東方日報

IP Cam預設密碼易破解 港人亦中招

家居「真人秀」全球任睇

更改密碼可防黑客入侵

明報

IP cam直播 電腦店懵然

拍攝不受管 私隱署籲改特別密碼

特稿

View camera online in Hong Kong

iCloud attack

- In October, 2014, Apple acknowledged a widespread man-in-the-middle attack targeting iCloud, which threatened user privacy

明報

假蘋果電郵 騙用戶帳戶密碼

除了政治敏感人物和傳媒機構，普通市民也會成爲黑客攻擊目標。根據香港電腦保安事故協調中心數據，市民舉報遭黑客攻擊的宗數，2012年、2013年分

封聲稱來自「蘋果公司」的郵件，內容是提醒用户iTunes帳户過期，或iCloud儲存已滿。記者查看郵件所附的鏈接，發現該鏈接地址用「appfe」魚目混珠

聲稱機構網址；一旦收到有應用程式附件的電郵，更要特別警惕，不要輕易打開附件；同時要做好事先防範，定期檢查防火牆，更新修補程式和防毒軟件。

成報

蘋果警告iCloud遭網絡攻擊

用家需小心被盜取個人資料

蘋果公司日前發布安全警告，提醒旗下雲端儲存服務iCloud的使用者正受到間歇性的網絡攻擊，小心被駭客入侵及盜取個人資料。香港早前曾掀起一股iPhone 6的熱潮，不少用家手持新手機，吸引全城關注，不過用家需要留意保安問題。早在本周一時有網絡安全監察組織表示，攻擊可能是由中國的駭客發動。而中國外交部發言人華春瑩強調，中國政府堅決反對和打擊任何形式的駭客攻擊活動。 本報港聞部報道

Former security chief fell victim to phishing scam

- Former security chief Regina Ip's email account was hacked after she opened an email. About HK$500,000 was transferred out of her bank account

星島日報 SING TAO DAILY

前保安局局長 墮電郵釣魚騙局

黑客化身錢果豐 「釣」走葉劉50萬

香港經濟日報 HONG KONG ECONOMIC TIMES www.hket.com

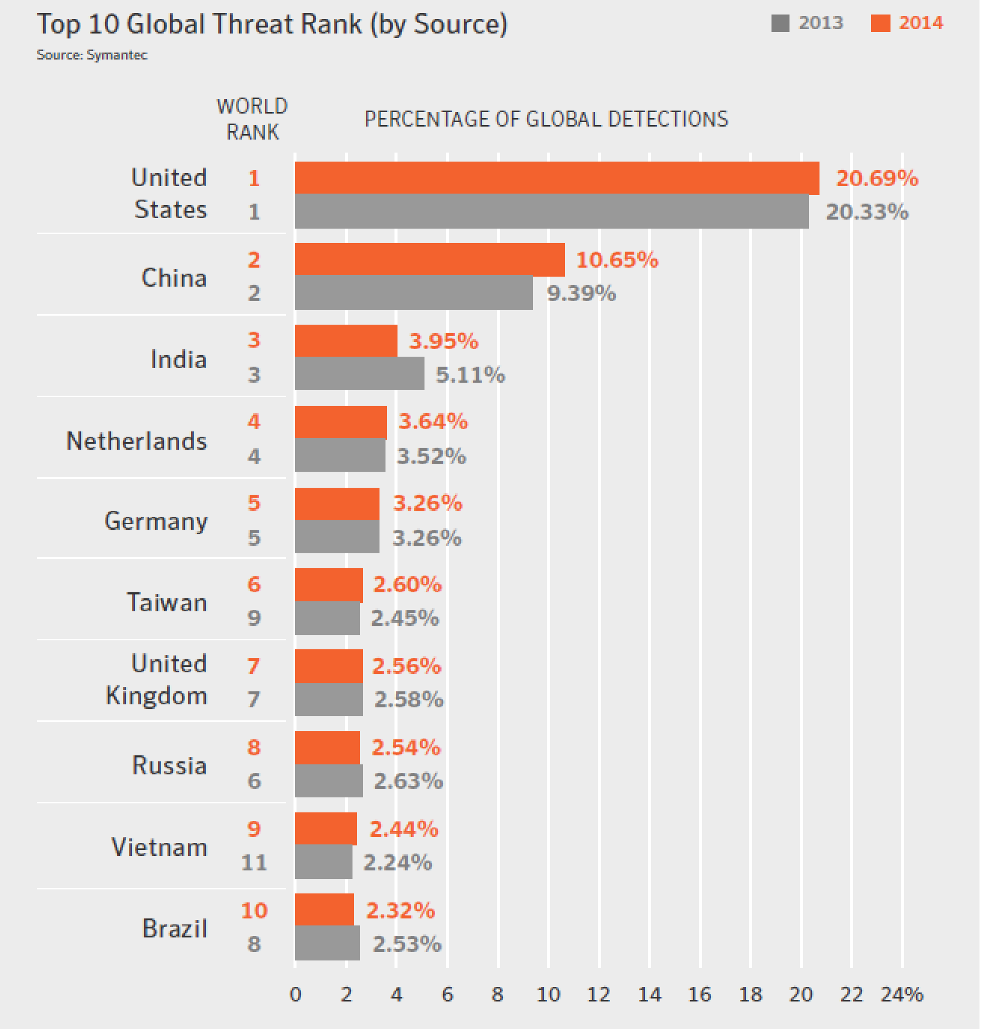
葉劉中招 遭「假錢果豐」騙50萬

忘改電郵密碼 黑客冒名滙款

科技罪案激增，連前保安局局長、行會兼立法會議員葉劉淑儀亦中招。葉太日前收到黑客以港鐵主席錢果豐名義發出的求助電郵，並打開相關附件，懷疑因而被黑客入侵電郵及冒名滙款50萬港元，她已報警求助。 ■本報記者

行會政府機密文件 親交收

Top 10 of Global Threat Rank



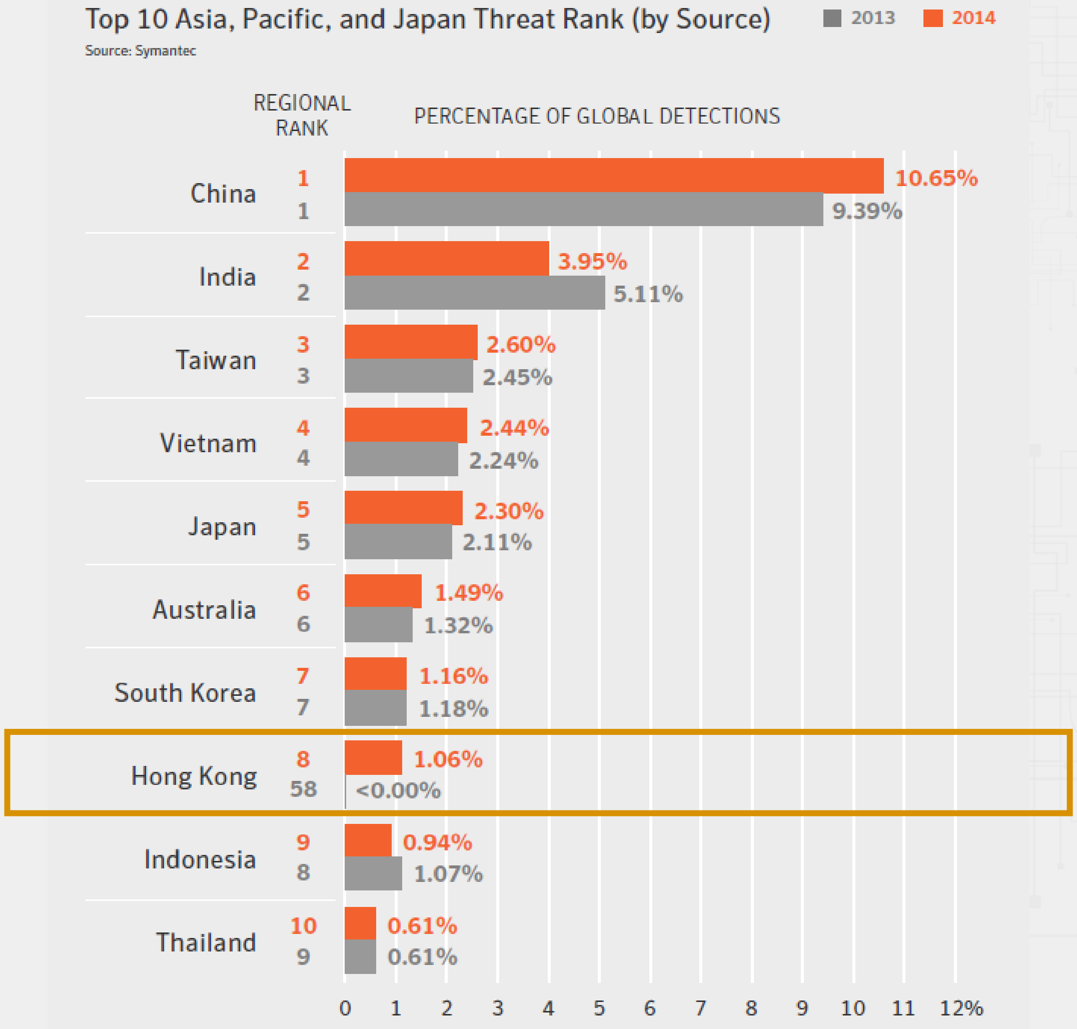
Top 10 Global Threat Rank (by Source)

Source: Symantec

Top 10 Asia, Pacific, and Japan Threat Rank

Top 10 Asia, Pacific, and Japan Threat Rank (by Source)

Source: Symantec



Attack Methods

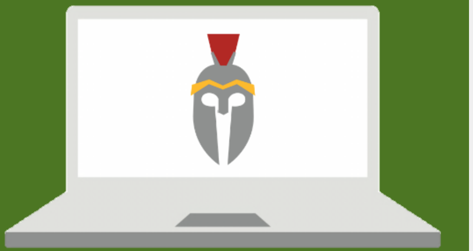
Spear Phishing

Send an email to a person of interest

Watering Hole Attack

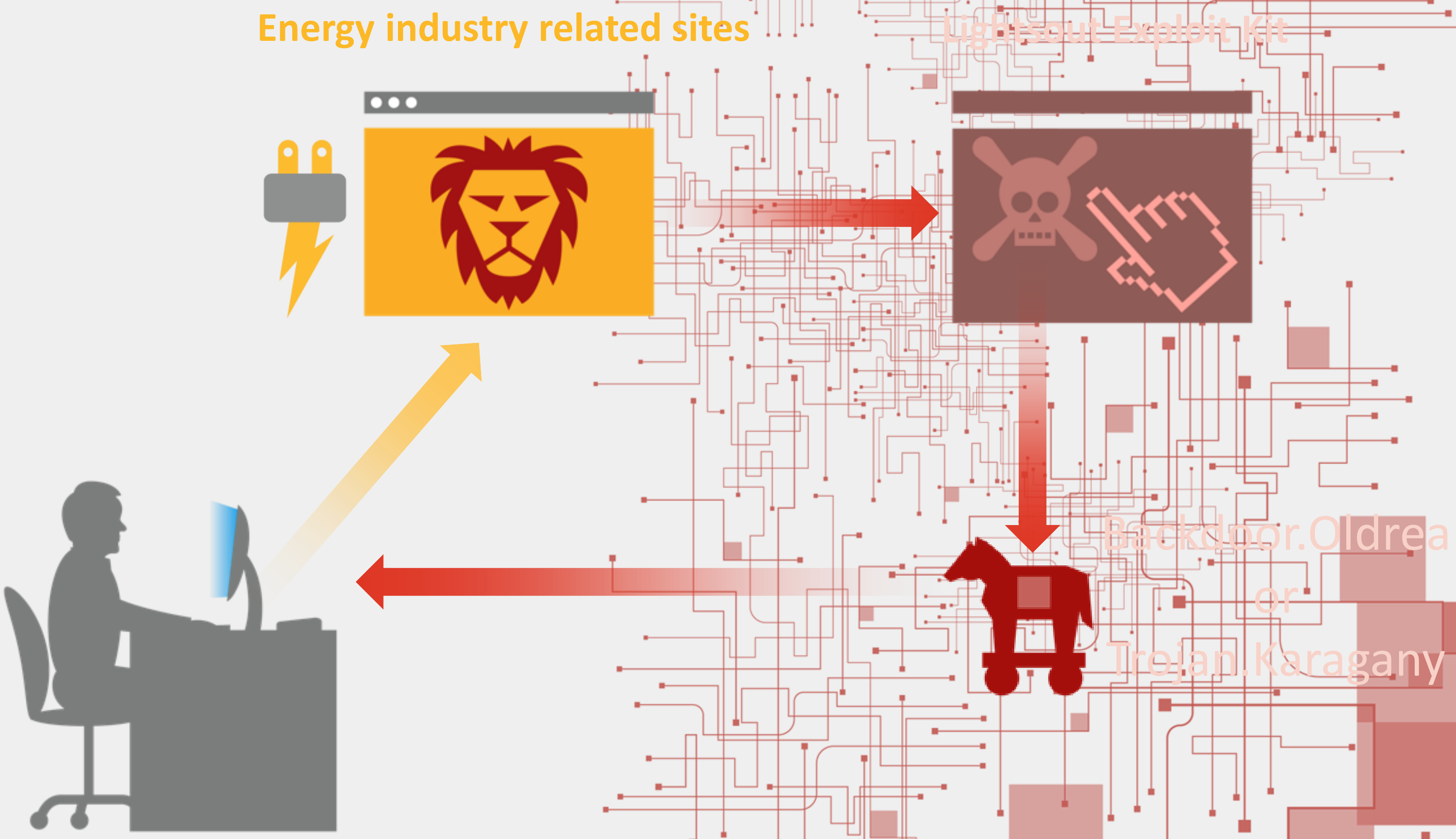
Infect a website and lie in wait for them

Trojanized Update



Infect software update victim downloads

How It Works: Watering Hole Attack



Energy industry related sites

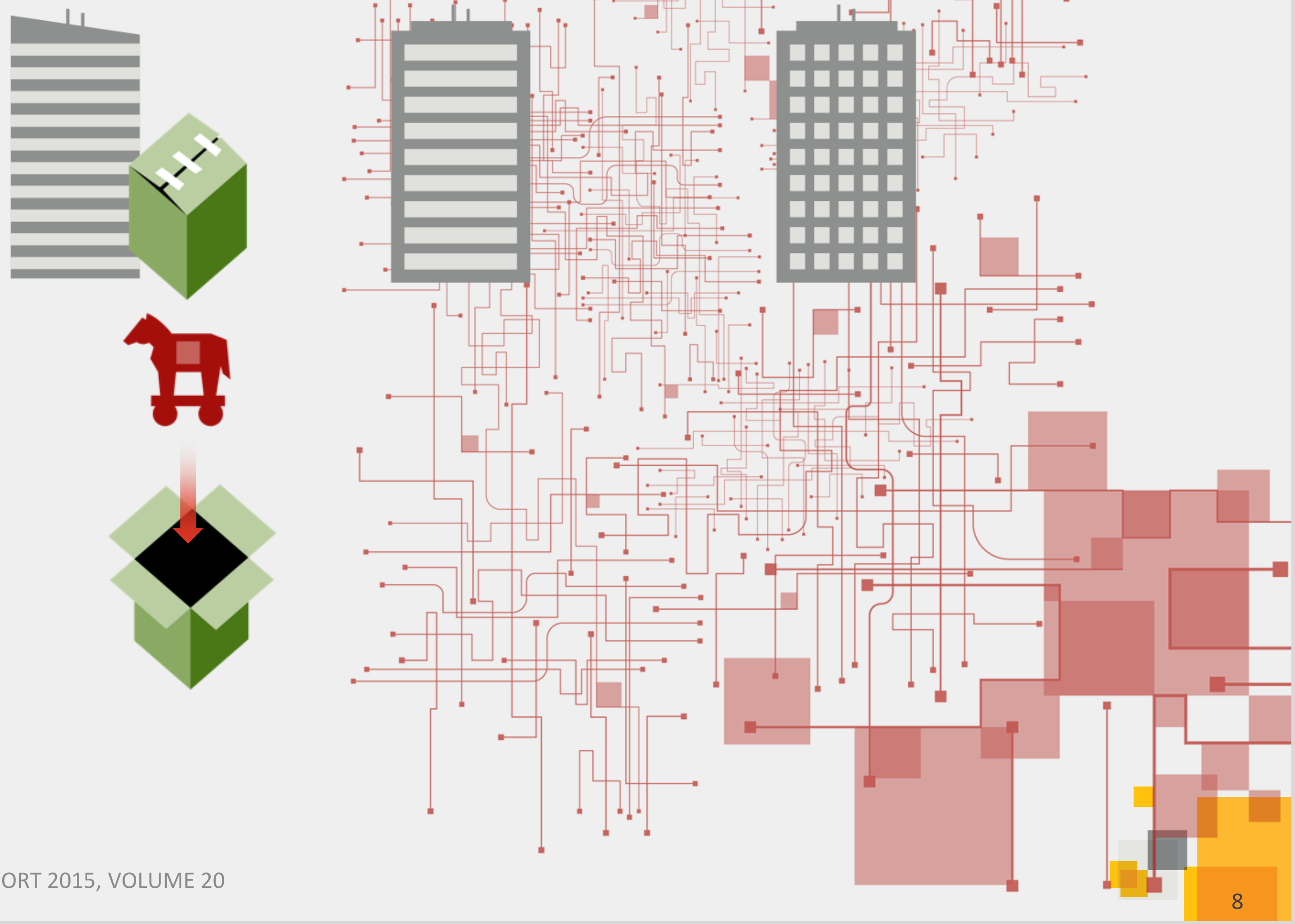
Lightsout Exploit Kit

Backdoor.Oldrea

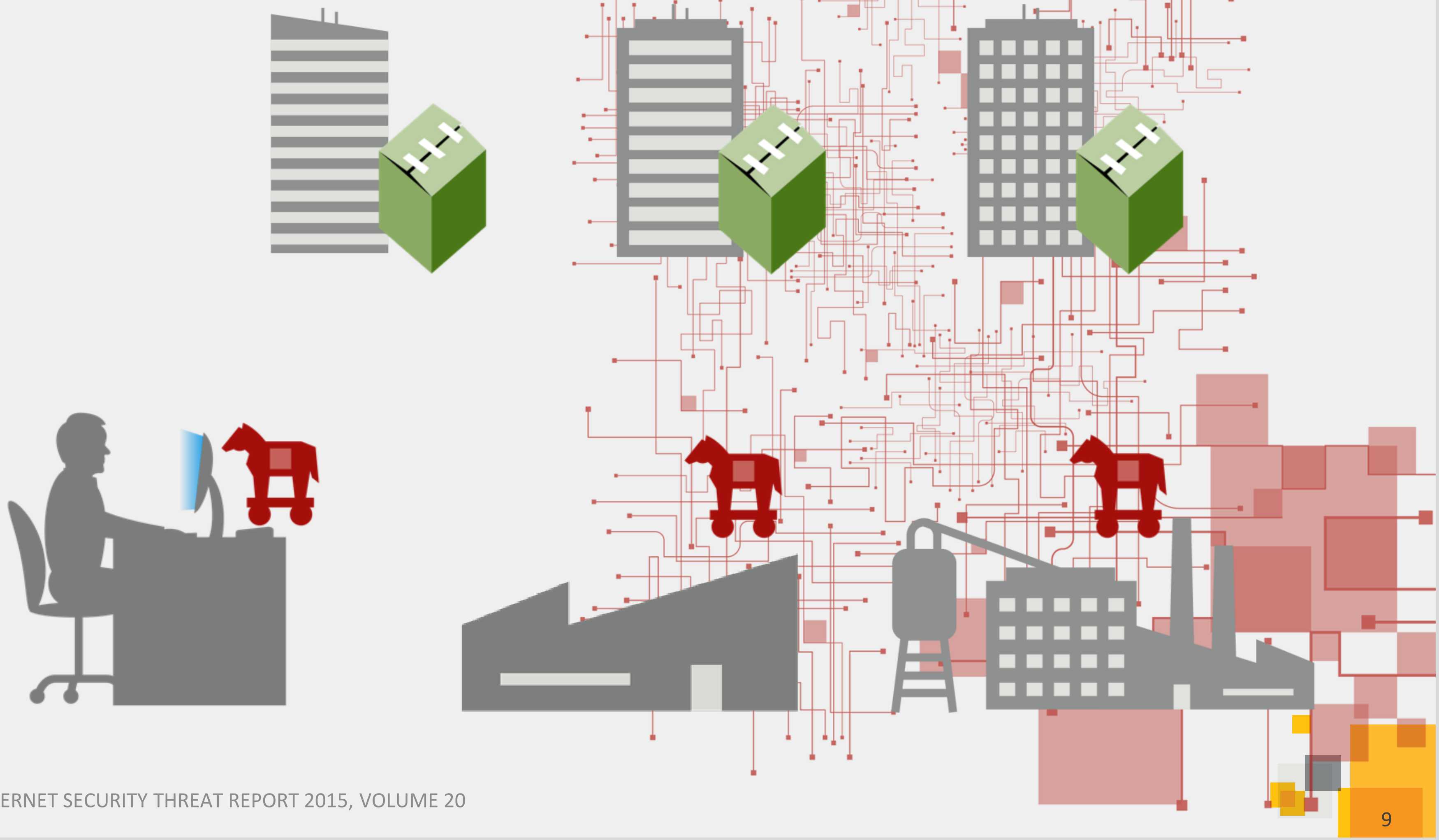
or

Trojan.Karagany

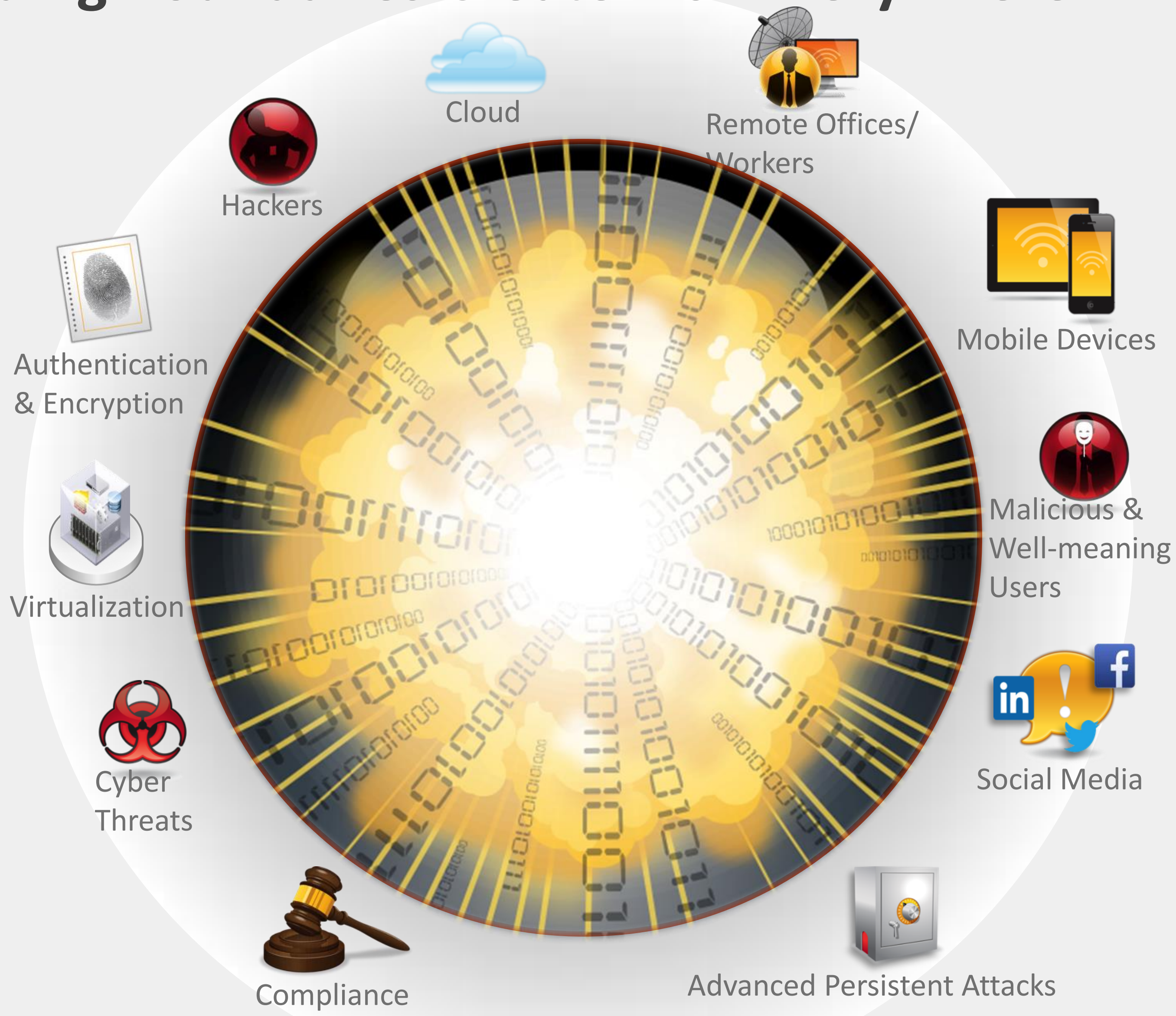
How It Works: Trojanized Update



How It Works: Trojanized Update



Expanding Boundaries Create Risk Everywhere



Cloud

Remote Offices/ Workers

Mobile Devices

Malicious & Well-meaning Users

Social Media

Advanced Persistent Attacks

Compliance

Cyber Threats

Virtualization

Authentication & Encryption

Hackers

Technology Practices - Creating the Path of Unified Security

Helping consumers and businesses transform the way they view security as an enabler for their businesses.

Threat Protection

A holistic view via a 'customer hub' of threat information, which in turn forms part of our Global Intelligence Network (GIN).

- Endpoints: SEP, CSP, Suites, Mobility
- Gateways/Networks: Threat Gateway, Web Gateway etc.
- Mail Systems: Groupware, Mail/ Messaging Protection

+

Information Protection

A complete cloud security suite that provides protection for customer and enterprise information travelling in and out of an organization

- Identity: SAM, VIP, MPKI
- Data protection: DLP, Key mgmt. and encryption
- Risk analytics: IRIS

+

Cyber Security

Services to facilitate & adopt our technologies

- Assessments: Consulting
- Monitoring: MSS
- Incident Response: MATI (Managed Advanced Threat Intelligence)
- Deepsight: Intelligence Datafeeds

Global Intelligent Network | UNIQUE VISIBILITY

175M
endpoints

57M attack sensors in
157 countries

182M web attacks
blocked last year

3.7T
rows of telemetry

100 Billion
more/month

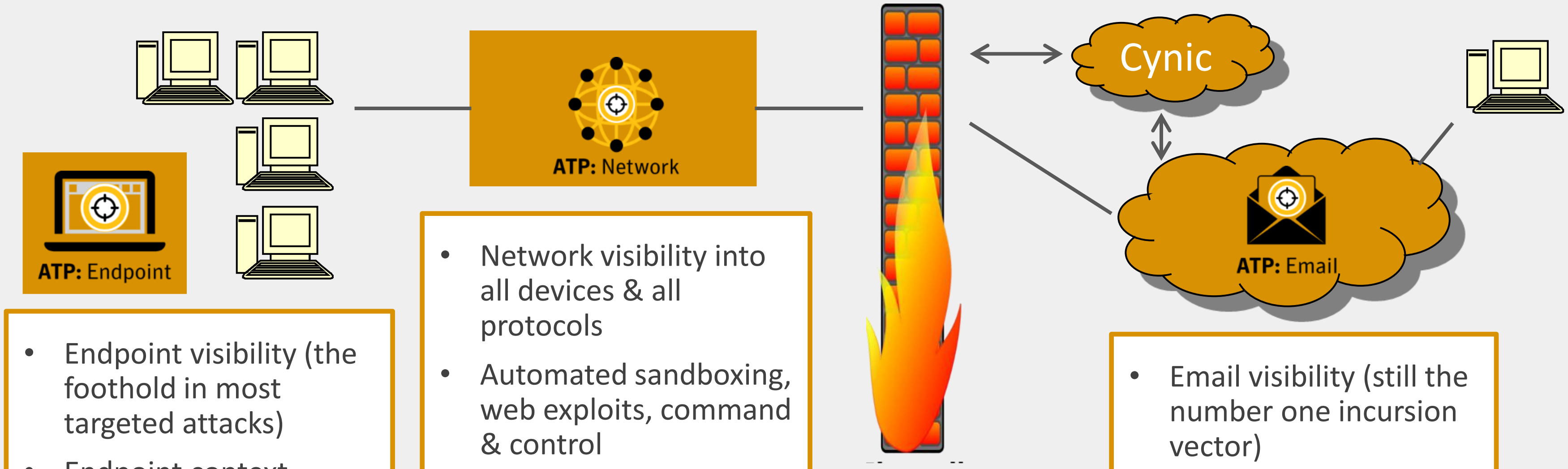
30% of world's enterprise
email traffic scanned/day

1.8 Billion
web requests

9
threat response centers

500+
rapid security response team

Core Protection by 3 Control Points



- Endpoint visibility (the foothold in most targeted attacks)
- Endpoint context, suspicious events, & remediation
- Requires SEP – no new agent – and deployed as a virtual appliance

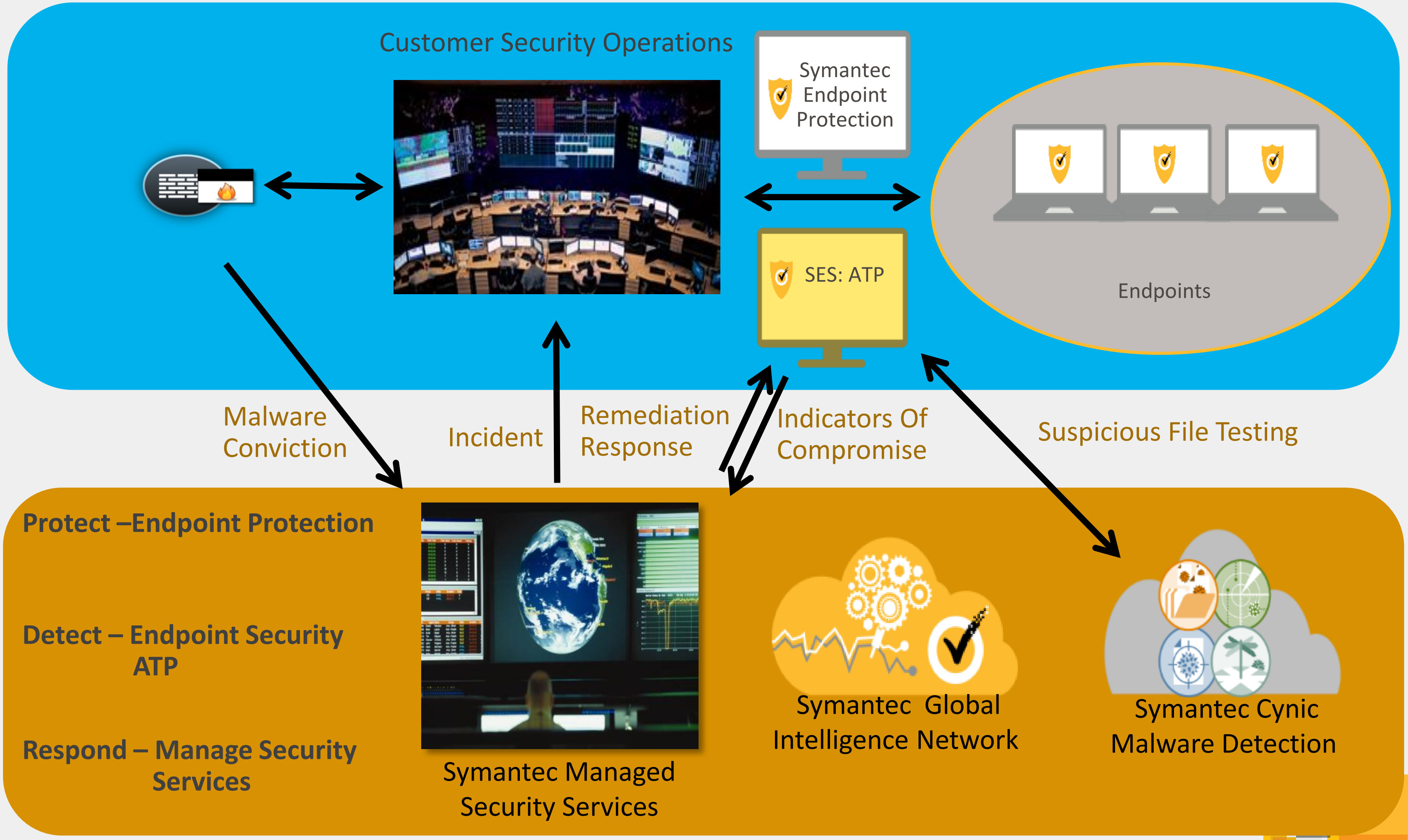
- Network visibility into all devices & all protocols
- Automated sandboxing, web exploits, command & control
- Deployed off a TAP or inline as virtual or physical appliance

- Email visibility (still the number one incursion vector)
- Email trends, targeted attack identification, sandboxing
- Cloud-based easy add on to Email Security.cloud

How can Customer Achieve These Outcomes?

- Improved Security Posture ✓
  - Integrated – Combine Latest Malware Detection with Endpoint IoC & Response
  - Defence In Depth – Endpoint Detection is the Last chance to identify Malware
  - Containment – Stop the spread, Prevent more breaches
  - Faster Response – Reduce the Impact & Severity of a breach
- Reduced Operational Overhead ✓
  - Single Agent – Reduced Management Costs
  - Automation – Event Monitoring, Breach Identification & Remediation
  - Containment – Stop the spread, reduce the remediation effort
  - Automated Recovery – Less work to recover, and back to work sooner
- Reduced Computational Overhead ✓
  - Faster, Lighter & Smarter Endpoint Protection
  - Extend SoE refresh/Upgrade cycles

What does this look like?



Customer Security Operations

Symantec Endpoint Protection

SES: ATP

Endpoints

Malware Conviction

Incident

Remediation Response

Indicators Of Compromise

Suspicious File Testing

Protect –Endpoint Protection

Detect – Endpoint Security ATP

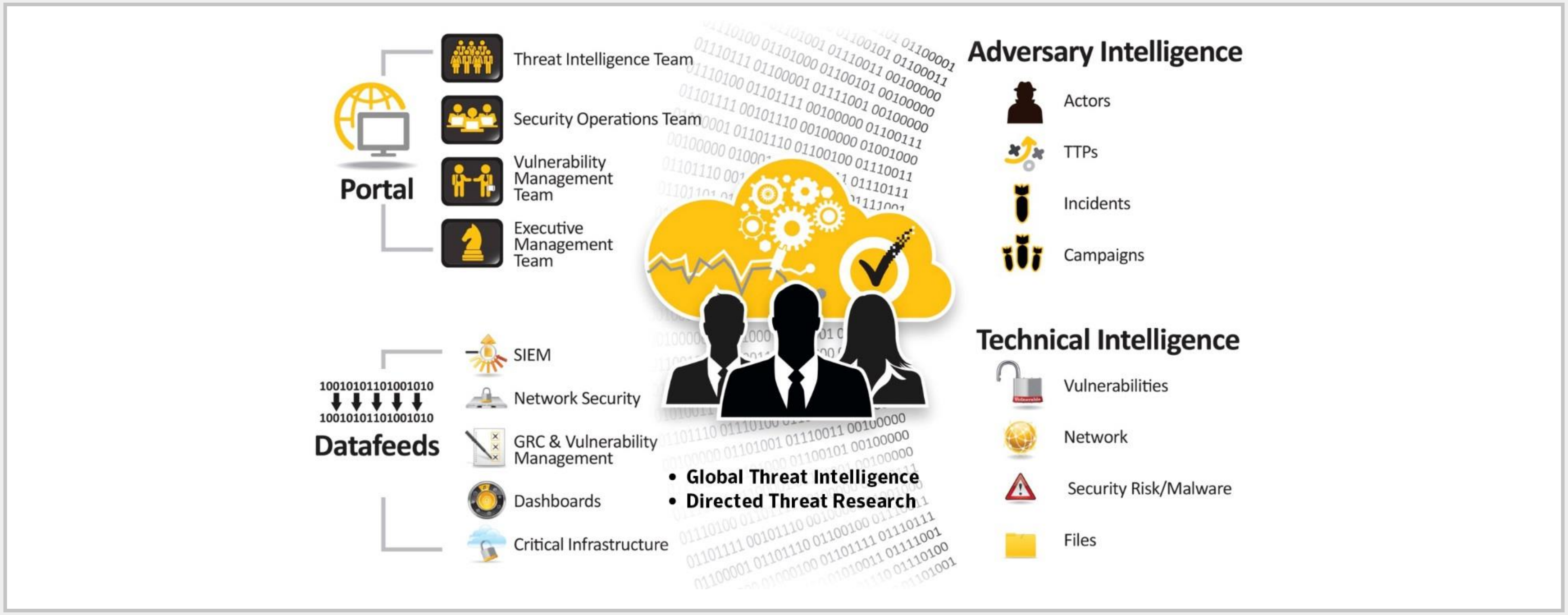
Respond – Manage Security Services

Symantec Managed Security Services

Symantec Global Intelligence Network

Symantec Cynic Malware Detection

DEEPSIGHT INTELLIGENCE



DEEPSIGHT INTELLIGENCE USE CASES

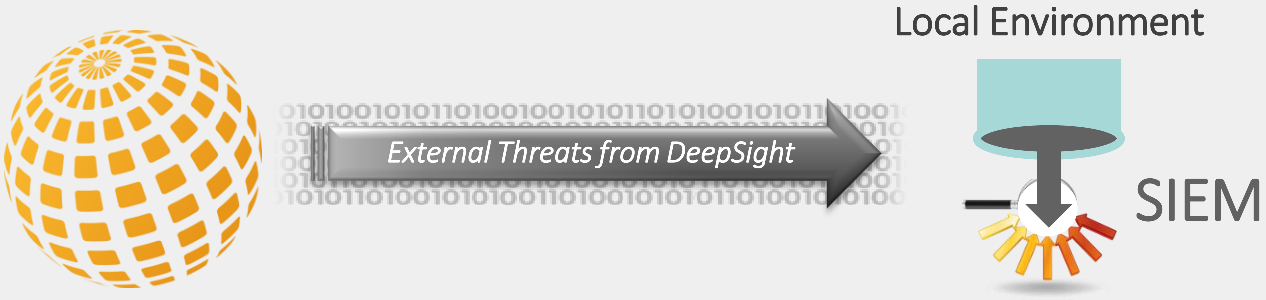
Apply the Global Threat Landscape to Your Environment

Technical

- Attack Quarantine System
- Malware Protection
- Gateways
- Phishing Detections
- Global Sensor Network
- 3rd Party Affiliates

Adversary

- Online Operations
- Social Media Monitoring
- Open Sourcing
- Mining
- Liaisons
- Sharing Forums



1 EXTERNAL THREATS

DeepSight Datafeeds provide external threat data, not known to the security infrastructure, to SOC's/SIEM's for detection & prevention.

2 REPUTATION DATAFEEDS

DeepSight Reputation Datafeeds provide an up-to-date list of "Command and Control" servers of botnets known to DeepSight. Allowing for the detection and the prevention of exfiltration of sensitive data.

3 CONTROL POINTS

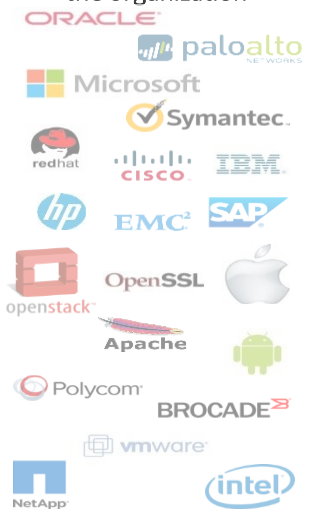
SIEM is used to detect Network control points such as Firewalls and Gateways and used to prevent exfiltration using the DeepSight data.

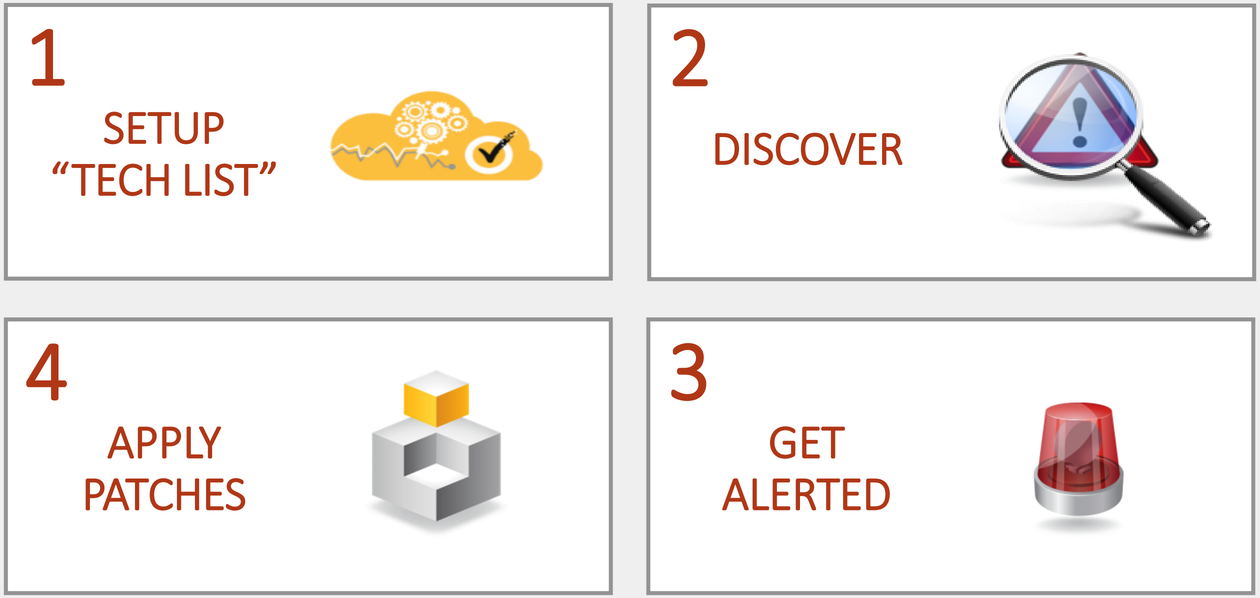
DEEPSIGHT INTELLIGENCE USE CASES

Vulnerability Alerts

Use DeepSight Vulnerability alerts and datafeeds to help identify and prioritize vulnerabilities based on technologies relevant to you.

Enterprise IT Products in the organization





1 SETUP "TECH LIST"

2 DISCOVER

3 GET ALERTED

4 APPLY PATCHES

DEEPSIGHT INTELLIGENCE USE CASES

Incident Response Research

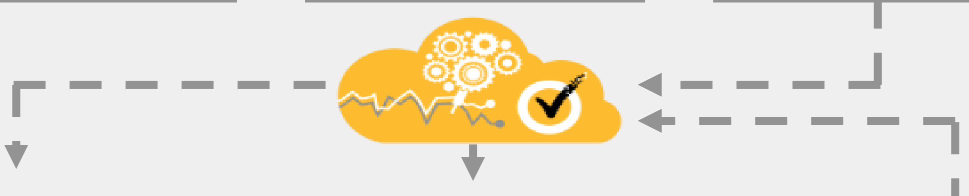
ANALYZE INFECTED SYSTEM

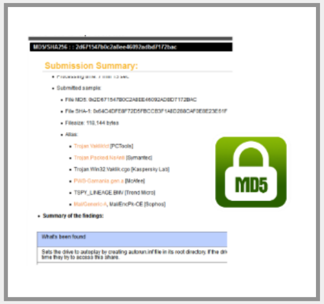
Security Analyst receives an infected system alert for analysis. Artifacts to be further analyzed include: a suspicious attachment and URL's embedded in the email received on the system.

1 SECURITY RISK LOOKUP

2 URL LOOKUP

3 INFORMED DECISION



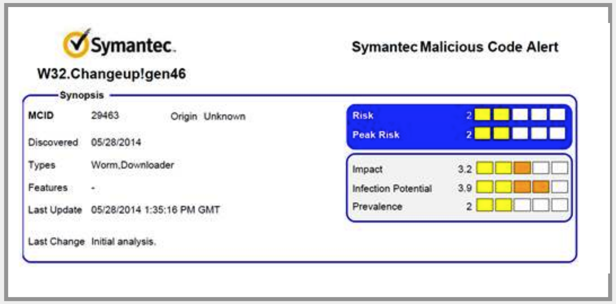


MD5/SHA256 : : 2d671547b0c2a8ee46092adbd7172bac

Submission Summary:

- Processing time: 1 min 13 sec.
- Submitted sample:
  - File MD5: 0x2D671547B0C2A8EE46092ADBD7172BAC
  - File SHA-1: 0x64C4DFE8F72D5FBCCB3F1A8D288C4F0E8E23E61F
  - Filesize: 110,144 bytes
  - Alias:
    - Trojan.Vaklik!ct [PCTools]
    - Trojan.Packed.NsAnti [Symantec]
    - Trojan.Win32.Vaklik.cgo [Kaspersky Lab]
    - PWS-Gamania.gen.a [McAfee]
    - TSPY_LINEAGE.BMV [Trend Micro]
    - Mal/Generic-A, Mal/EncPk-CE [Sophos]
- Summary of the findings:

What's been found
Sets the drive to autoplay by creating autorun.inf file in its root directory. If the dri time they try to access this share.



Symantec.

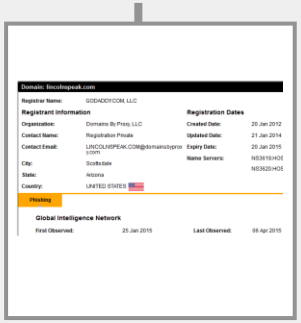
Symantec Malicious Code Alert

W32.Changeup!gen46

Synopsis

MCID	29463	Origin	Unknown
Discovered	05/28/2014		
Types	Worm,Downloader		
Features	-		
Last Update	05/28/2014 1:35:16 PM GMT		
Last Change	Initial analysis.		

Risk	2
Peak Risk	2
Impact	3.2
Infection Potential	3.9
Prevalence	2



Domain: lincolnspeak.com

Registrar Name: GODADDY.COM, LLC

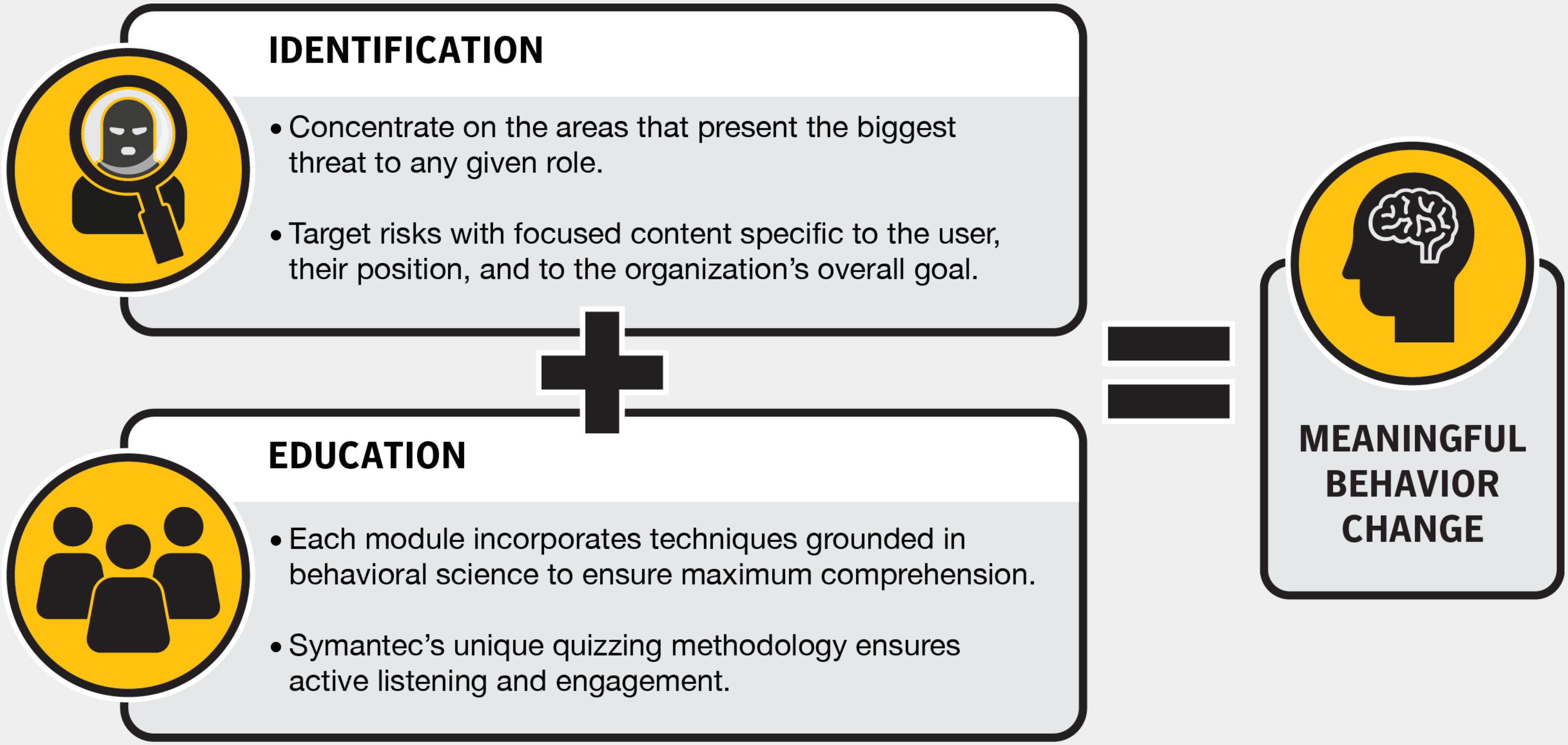
Registrant Information		Registration Dates	
Organization:	Domains By Proxy, LLC	Created Date:	20 Jan 2012
Contact Name:	Registration Private	Updated Date:	21 Jan 2014
Contact Email:	LINCOLNSPEAK.COM@domainsbyproxy.com	Expiry Date:	20 Jan 2015
City:	Scottsdale	Name Servers:	NS3619.HOS NS3620.HOS
State:	Arizona		
Country:	UNITED STATES		

Phishing

Global Intelligence Network

First Observed:	25 Jan 2015	Last Observed:	08 Apr 2015

Security is Everyone's Responsibility



IDENTIFICATION

- Concentrate on the areas that present the biggest threat to any given role.
- Target risks with focused content specific to the user, their position, and to the organization's overall goal.

EDUCATION

- Each module incorporates techniques grounded in behavioral science to ensure maximum comprehension.
- Symantec's unique quizzing methodology ensures active listening and engagement.

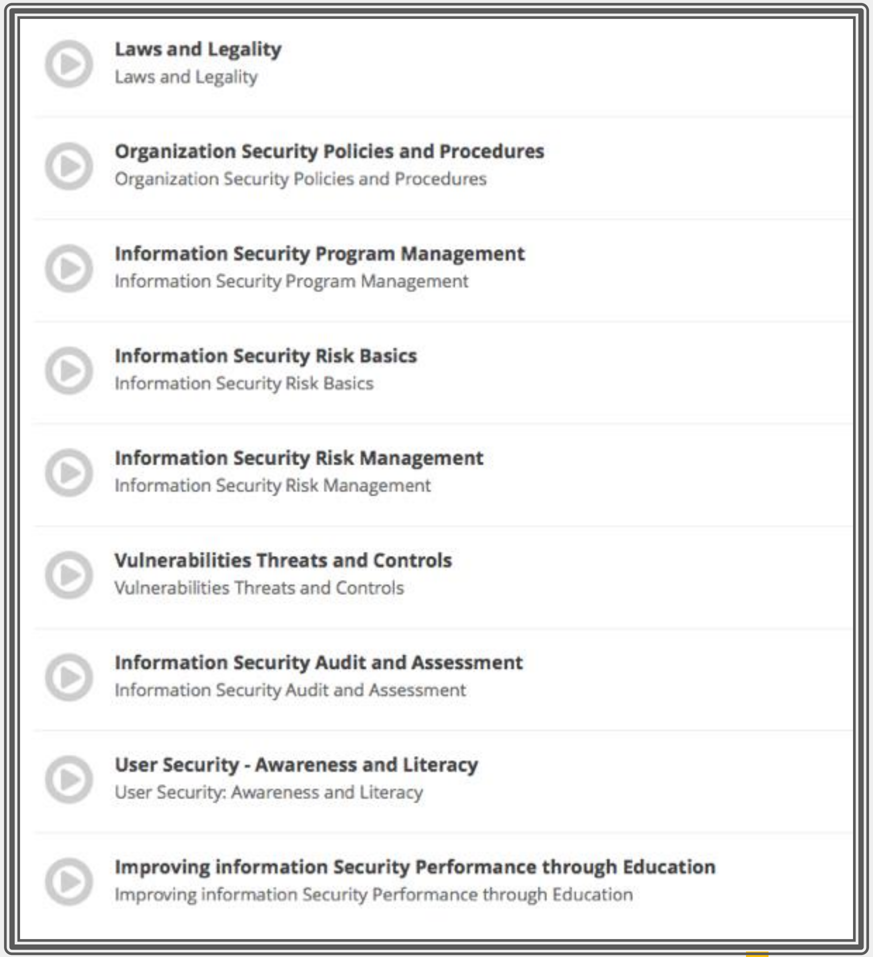
MEANINGFUL BEHAVIOR CHANGE

Security Awareness Service

- Role-based training approach
- Meet compliance mandates
- Regular content refresh
- Unique quizzing methodology

C-Level Executive Training Track

- Focused & specific
- Pair with general awareness modules
- Complete training program for each role



Laws and Legality
Laws and Legality

Organization Security Policies and Procedures
Organization Security Policies and Procedures

Information Security Program Management
Information Security Program Management

Information Security Risk Basics
Information Security Risk Basics

Information Security Risk Management
Information Security Risk Management

Vulnerabilities Threats and Controls
Vulnerabilities Threats and Controls

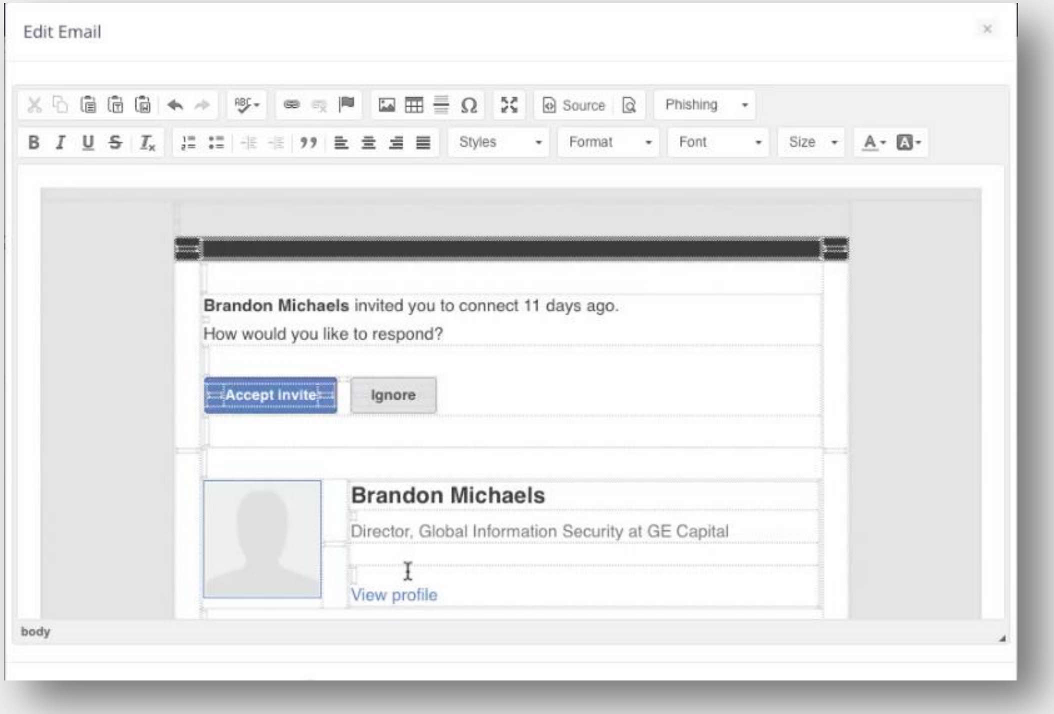
Information Security Audit and Assessment
Information Security Audit and Assessment

User Security - Awareness and Literacy
User Security: Awareness and Literacy

Improving information Security Performance through Education
Improving information Security Performance through Education

Phishing Readiness prepares your teams to think in a defensive manner

- Dedicated, private instances for each organization
- Send unlimited assessments
- Multiple assessment types
- Detailed reporting features
- Integrated user training



Brandon Michaels invited you to connect 11 days ago.
How would you like to respond?

Brandon Michaels
Director, Global Information Security at GE Capital

Benchmark and Improve Your Employees

Training

- Security Awareness Service

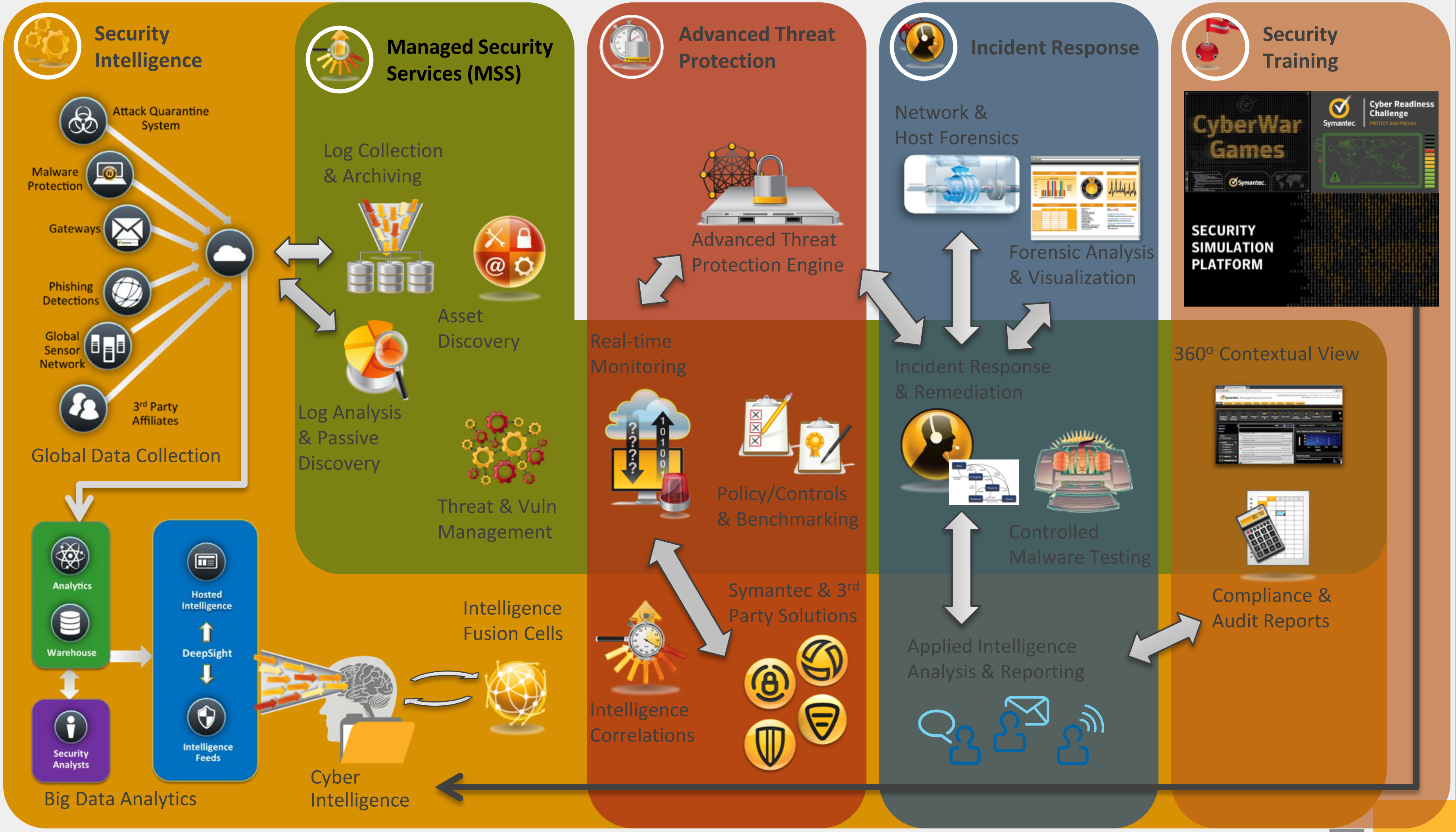
Simulation

- Phishing Readiness

Performance Evaluation

- Security Awareness Service allows you to be sure that each employee assigned to it has viewed and understands the messaging provided
- Phishing Readiness gives you real, behavioral metrics to see how users would respond when presented with a phishing attack.

Cyber Security Integration Strategy



Security Intelligence

Attack Quarantine System

Malware Protection

Gateways

Phishing Detections

Global Sensor Network

3rd Party Affiliates

Global Data Collection

Analytics

Warehouse

Security Analysts

Hosted Intelligence

DeepSight

Intelligence Feeds

Big Data Analytics

Cyber Intelligence

Intelligence Fusion Cells

Managed Security Services (MSS)

Log Collection & Archiving

Asset Discovery

Log Analysis & Passive Discovery

Threat & Vuln Management

Advanced Threat Protection

Advanced Threat Protection Engine

Real-time Monitoring

Policy/Controls & Benchmarking

Symantec & 3rd Party Solutions

Intelligence Correlations

Incident Response

Network & Host Forensics

Forensic Analysis & Visualization

Incident Response & Remediation

Controlled Malware Testing

Applied Intelligence Analysis & Reporting

Security Training

CyberWar Games

Symantec.

Cyber Readiness Challenge

PROTECT AND PREVAIL

SECURITY SIMULATION PLATFORM

360° Contextual View

Compliance & Audit Reports

Q&A