



FireEye iSIGHT Intelligence

Robert Želazo – Regional Director, Eastern Europe, FireEye

Prague, Sep 14, 2016

Some false things you may have heard around...

- “APT is just Advanced Malware, and you need **Advanced Malware Protection**”
- “Stop trying to **Detect** when you can **Prevent**”
- “Our APT solution offers **Remediation**”

The real problem is the hacker, not the malware

IT'S A "WHO,"
NOT A "WHAT"



THERE'S A HUMAN AT A KEYBOARD

HIGHLY TAILORED AND
CUSTOMIZED ATTACKS

TARGETED SPECIFICALLY AT YOU

THEY ARE
PROFESSIONAL,
ORGANIZED AND
WELL FUNDED



NATION-STATE SPONSORED

ESCALATE SOPHISTICATION OF
TACTICS AS NEEDED

RELENTLESSLY FOCUSED ON
THEIR OBJECTIVE

IF YOU KICK THEM
OUT THEY WILL
RETURN



THEY HAVE SPECIFIC OBJECTIVES

THEIR GOAL IS LONG-TERM
OCCUPATION

PERSISTENCE TOOLS ENSURE
ONGOING ACCESS

What happens after Malware ?



- Expand Access and obtain valid credentials
 - Credentials stolen by keyboard logging
 - Credentials stolen by network sniffing
 - Encrypted Credentials stolen from disk and brute forced
- Strengthen foothold
 - Lateral movement using OS Tools
 - Further internal reconnaissance
 - Non malware based backdoors
 - Multiple backdoor fail-safes



APT29 – ONE OF THE MOST ADVANCED CYBERGROUPS

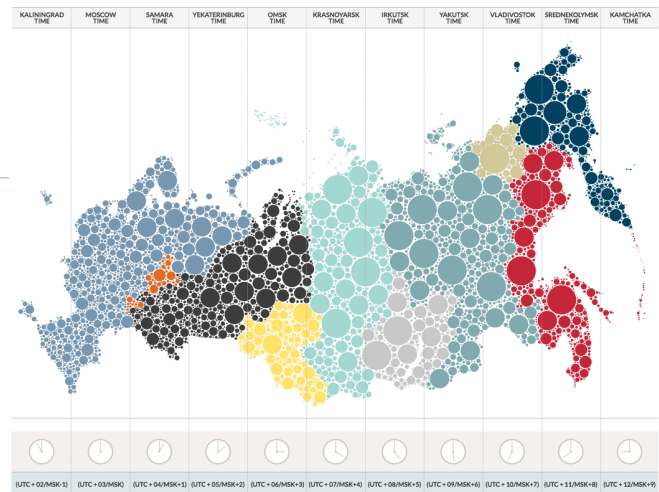


Russian Threat Groups

- FireEye monitors various Russian threat groups – for example:
 - APT28
 - APT29
- The groups frequently design innovative ways to cover their tracks
- APT29 has been particularly active throughout 2015
 - new downloaders, payloads, and targets

APT29: Sponsored by the Russian Gov

- Probable Russian threat actor supporting nation state missions
 - Espionage versus strategic European-related targets
 - interest in Russia-Ukraine issues
 - Work hours align with the UTC +3 time zone (Moscow, St. Petersburg)
 - Operations ceased on Russian holidays
- Disciplined focus on operational security
 - Almost exclusive use of compromised servers, legitimate services, and similar
 - Anti forensics
- Aggressive and advanced skills
 - Targeting both intelligence targets and defenders alike
 - Monitor remediation efforts
 - Rapid tool development cycle to support new deployments



2015 Toolset

Initial Compromise	Maintain Presence
COZYCAR SWIFTKICK / MINIDIONIS	SEADADDY SAYWHAT QUEENPIECE HAMMERTOSS Powershell

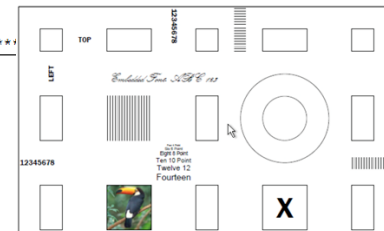
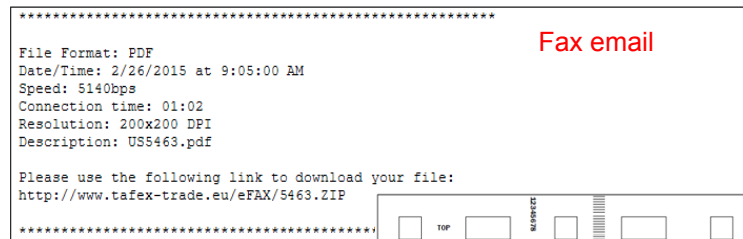
Generic Spearphishing

- 2014 – early 2015 Campaign used generic lures / decoys

- “You’ve got a fax”
- “Office Monkeys”

- Lure site very relevant

- Compromised legitimate / prominent sites to deliver “fax”
 - International issues and diplomacy sites
 - European stock exchange
 - US state and local government
 - Prominent US university








- July'2015 campaign showed much more-targeted / topical lures...some generic

APT29's HAMMERTOSS – Advanced persistent threat

- Backdoor detected in early 2015
- Designed to make it difficult for security professionals to detect and characterize the extent of APT29's activity.
- Multiple layers of obfuscation
- Mimicking the behavior of legitimate users:
 - Usage of commonly visited websites: Twitter, GitHub, and cloud storage services

FireEye Threat Intelligence Sources

	Generation Methods	Detects	Context Type
Collected	 <p>Malware Collection → Analysis → Intelligence</p> <p>400,000 unique daily malware samples 10,000 malicious identifiers detected daily</p>	<ul style="list-style-type: none"> • Botnets • Commodity malware • C2 callbacks 	<ul style="list-style-type: none"> • Malware family name • Risk score
Curated	 <p>Team of security experts put intelligence into context</p>  <p>300 Tracked attack groups 40 Industry-specific threat profiles</p>	<ul style="list-style-type: none"> • APT-style attacks • Targeted malware 	<ul style="list-style-type: none"> • Malware family name • Risk score • Attack group name • Attack group dossier
Focused Rule Sets & IOCs	 <p>Advanced Detection Hunt team monitors for current threats and generate rule packs & IOCs to assist with detection</p> 	<ul style="list-style-type: none"> • Vulnerability • Analytics • Authentication, authorization, and accounting • Incident watchlist • Emerging threats 	<ul style="list-style-type: none"> • Malware family name • Risk score • Threat impact level • Insightful threat details

Using Cyber Threat Intelligence to Enhance Security

- What is Intelligence?
- Why is Cyber Threat Intelligence important?
- Leveraging Cyber Threat Intelligence
 - Enhance security technologies
 - Streamline processes
 - Improve security programs
- iSIGHT Offerings
- Case study
- Questions

WHAT IS INTELLIGENCE?

Cyber Threat Intelligence - Definition

- Intelligence is information that has been collected, processed and disseminated with the purpose of:
 - Reducing the degree of uncertainty about an adversary, potential adversary, situation or threat, which may be experienced by decision makers.
 - So they can make **informed**, **reasoned**, and **timely** decisions.

Cyber Threat Intelligence - Definition

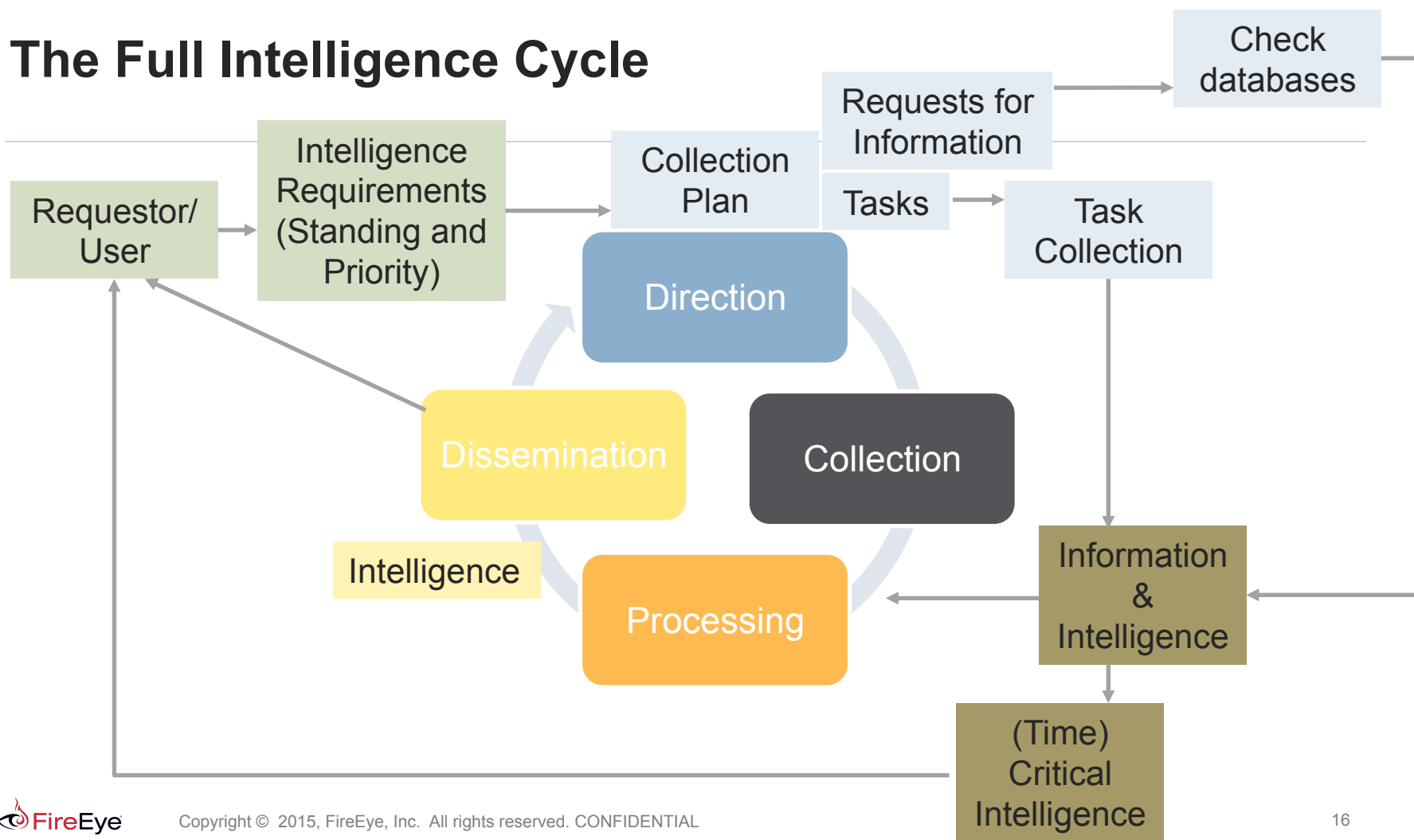
Not to be confused with:

“Information is **unprocessed data of every description** that may be used in the production of intelligence. It is normally collected by **individual** sensors, systems or capabilities.”

The Intelligence Cycle – Simple Version



The Full Intelligence Cycle



FireEye iSIGHT

200+ intelligence Professionals, 29 Languages, 18 Countries

Global Insights

Global Reach

✓ ADVERSARY FOCUSED

✓ GLOBAL COLLECTION

✓ CONTEXTUAL

✓ MULTIPLE DELIVERABLES

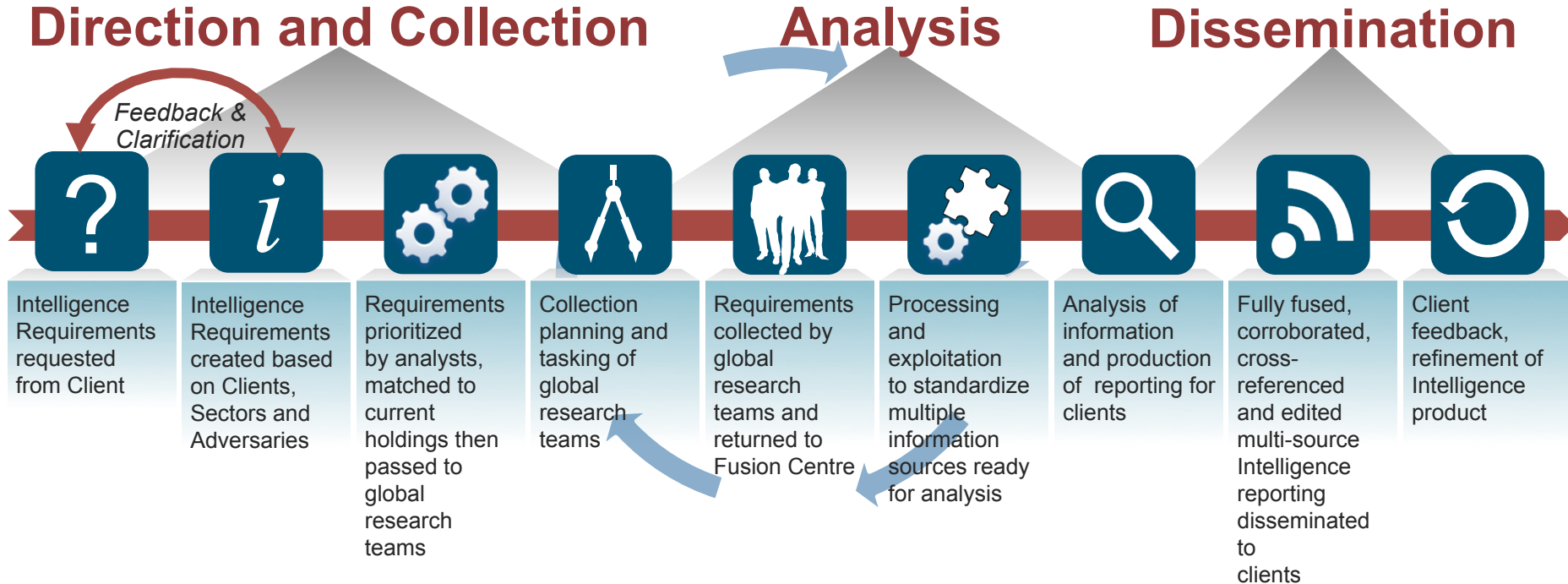
✓ PARTNERSHIP

✓ ACTIONABLE



Cyber Threat Intelligence Production

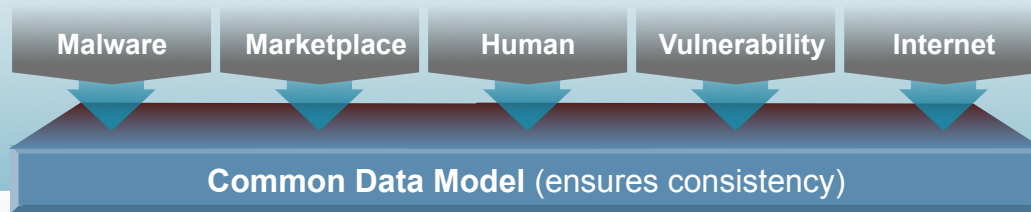
Formal Process Yields Rich, Contextual Threat Intelligence



Cyber Threat Intelligence Process

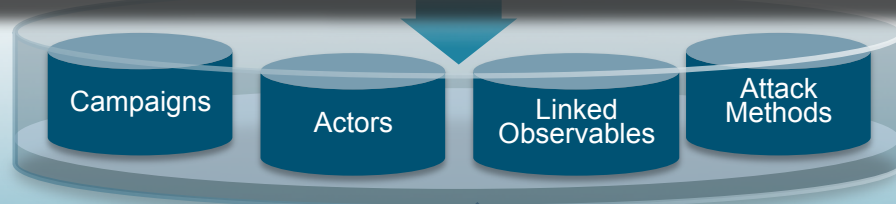
Collection - Global Intelligence Gathering

Collection systems and research team create raw observables...



utilized to create tagged, categorized "wires" or research elements...

Processing and Analysis

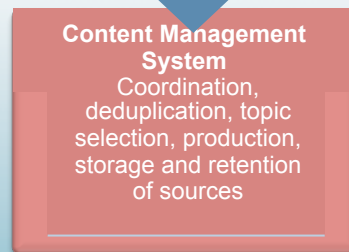


which flow to analytical tools to enrich, prioritize, rate and synthesize our knowledge into...

Dissemination

Deliverable Formats

- ✓ HTML or plain-text via email
- ✓ Portal access with advanced search capability
- ✓ XML delivery
- ✓ Indicator CSVs linked to intelligence context
- ✓ API access
- ✓ Partner Integrations



finished intelligence which is produced and delivered in many formats to the customer.



WHY IS CYBER THREAT INTELLIGENCE IMPORTANT?

Cyber Threat Joins the Risk List



How Can Cyber Threat Intelligence Help?

1. Be Proactive
2. Shrink the Problem
3. Improve Prioritization
4. Enhance Executive Communications
5. Connect Security With Business

FORRESTER®

Actionable Intelligence is:

- Accurate
- Aligned with your intelligence requirements
- Integrated
- Predictive
- Relevant
- Tailored
- Timely

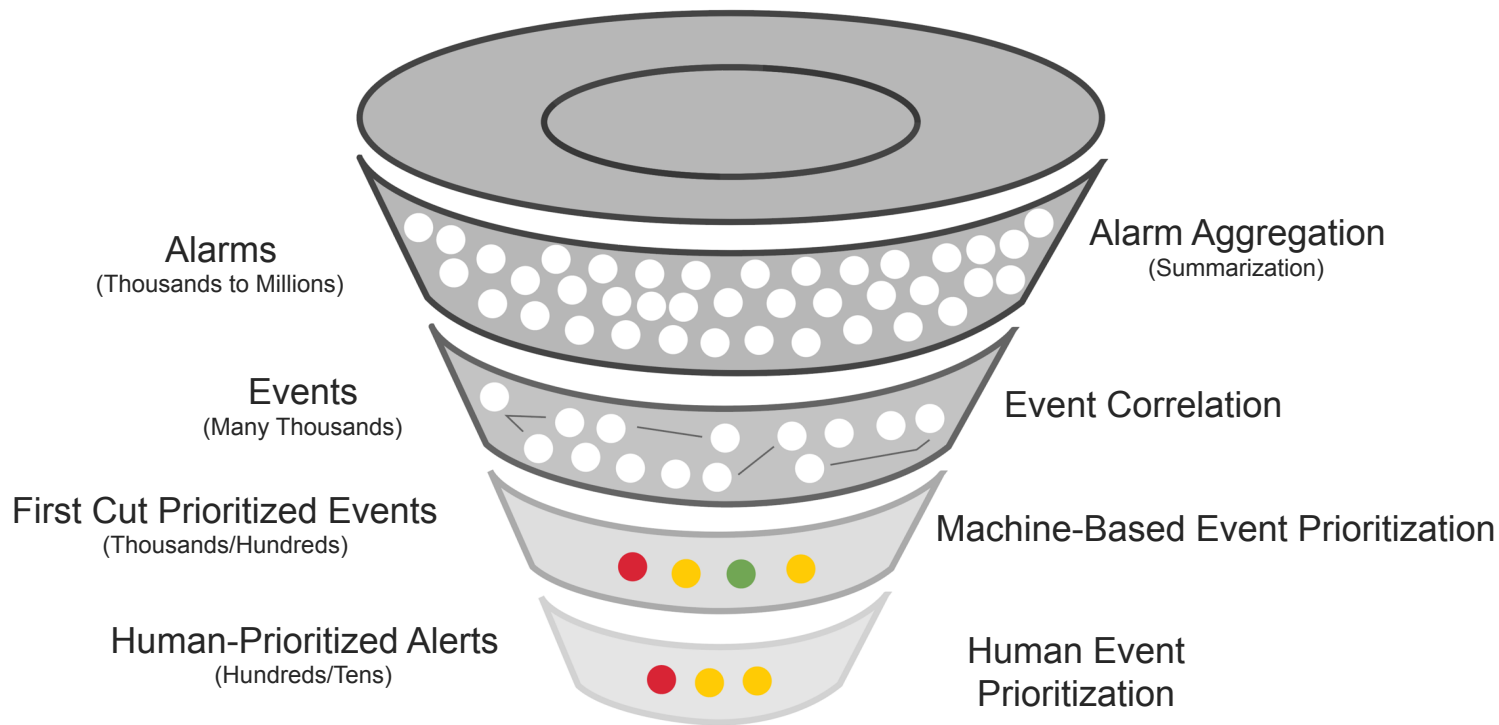
Rick Holland

Blog: Actionable Intelligence, Meet Terry Tate, Office
Linebacker

Published: 11 February 2014

LEVERAGING CYBER THREAT INTELLIGENCE

Leveraging CTI to “Shrink the Problem”



Impact of **Context Rich** Cyber Threat Intelligence

Benefit to Multiple Intelligence Consumers

Strategic

CISO
&
Executive

Threat
Intelligence
Team

Operational

Security
Operations Center
(SOC)

Incident
Response
Team

Tactical

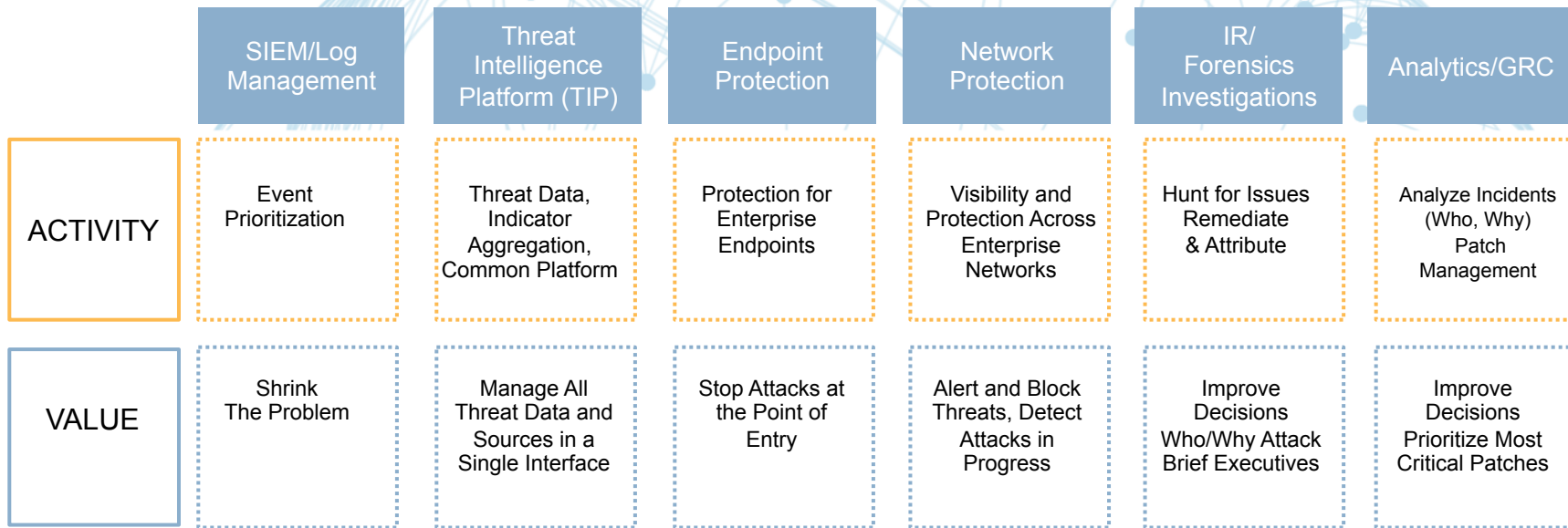
Network
Operations

Systems/Endpoint
Operations

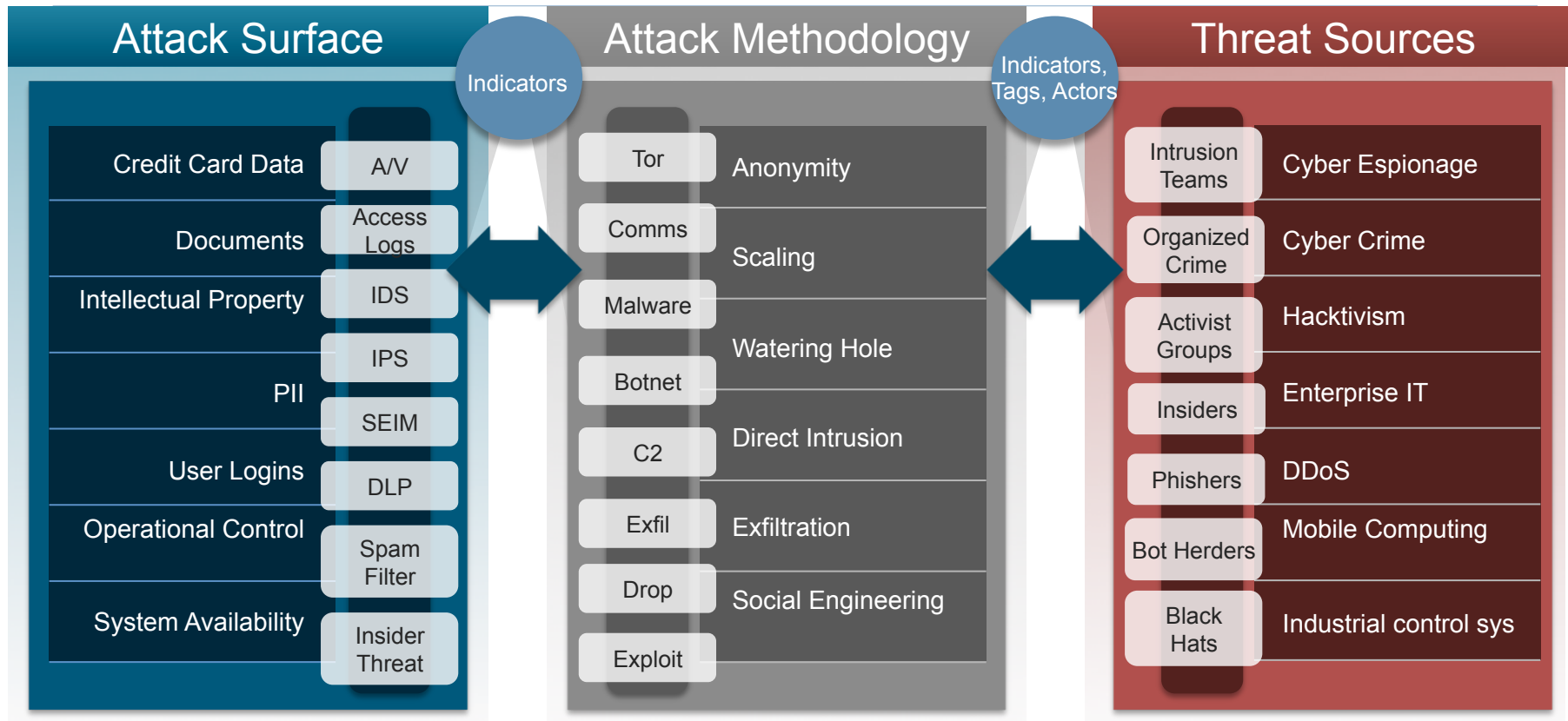
Actionable Threat Intelligence

ACROSS THE INFRASTRUCTURE

ThreatScape® API



Intelligence-Led Security – From the Outside In



Cyber Threat Intelligence

Indicators/IOCs

Malicious Files
(hashes/signatures)

Bad Domain

Bad IP Address

Phishing Lures

Registry Settings

Context

Actors

Attribution

Targets

Campaigns

TTPs, Methods/Playbooks

Motivation/Intent

Cyber Crime
(Money)

Espionage
(Information)

Hacktivism
(Influence)

Destruction
(Kinetic Impact)

Relevant to the Organisation

Report to the CEO, version 1

Last month we:

- Reviewed 1,452,134 log entries
- Detected 423,132 viruses
- Blocked 2,028,43 connections
- Closed 3,095 incident tickets

Report to the CEO, version 2

Last month we detected and blocked two cybercrime attacks linked to a criminal organization in Eastern Europe that has been targeting POS systems at mid-sized retailers. Our actions:

- Prevented the theft of 10 million customer credit card numbers
- Avoided \$78 million in lost revenue and the costs that would have been incurred for notifying customers of the data breach, cleaning up infected systems, and paying regulatory fines and legal fees.

Information v Cyber Threat Intelligence

Aims of Cyber Threat Intelligence

- Enable proactive, risk-based resource allocation
- Shrink the problem
- Improve prioritization
- Enhance executive communications
- Connect security with business



CASE STUDIES

Cyber Threat Intelligence in Action

- Sample Sandworm open source reports 13 – 16 October 2014.

TrendLabs
SECURITY INTELLIGENCE BLOG
Threat News and Information Direct from the Experts

Bad Sites Botnets CTO Insights Exploits Internet of Things Mac Malware Mobile Social

blog.trendmicro.com Sites > TrendLabs Security Intelligence Blog > Exploits > An Analysis of Windows Zero-day Vulnerability 'CVE-2014-4114' aka "Sandworm"

An Analysis of Windows Zero-day Vulnerability 'CVE-2014-4114' aka "Sandworm"

SensorsTechForum.com
"How to", Technology and PC Security Forum

HOW TO: RANSOMWARE ROOTKIT PC SECURITY TECHNICAL

The Sandworm Malware - How Dangerous Is It?
SensorsTechForum.com > PC security > The Sandworm Malware – How Dangerous Is It?

nakedsecurity
Award-winning computer security news from **SOPHOS**

android vulnerability data loss privacy more...

Symantec Official Blog

Sandworm Windows zero-day vulnerability being actively exploited in targeted attacks

Critical new Windows zero-day has reportedly been used in a limited number of targeted cyberespionage attacks to deliver a back door on to the victim's computer.

By: **Symantec Security Response** **SYMANTEC EMPLOYEE**

Created 14 Oct 2014

rm" malware - what you need to know

Cyber Threat Intelligence in Action

2009 • • • 2013 2014



Cyber Threat Intelligence in Action

- And it continues...

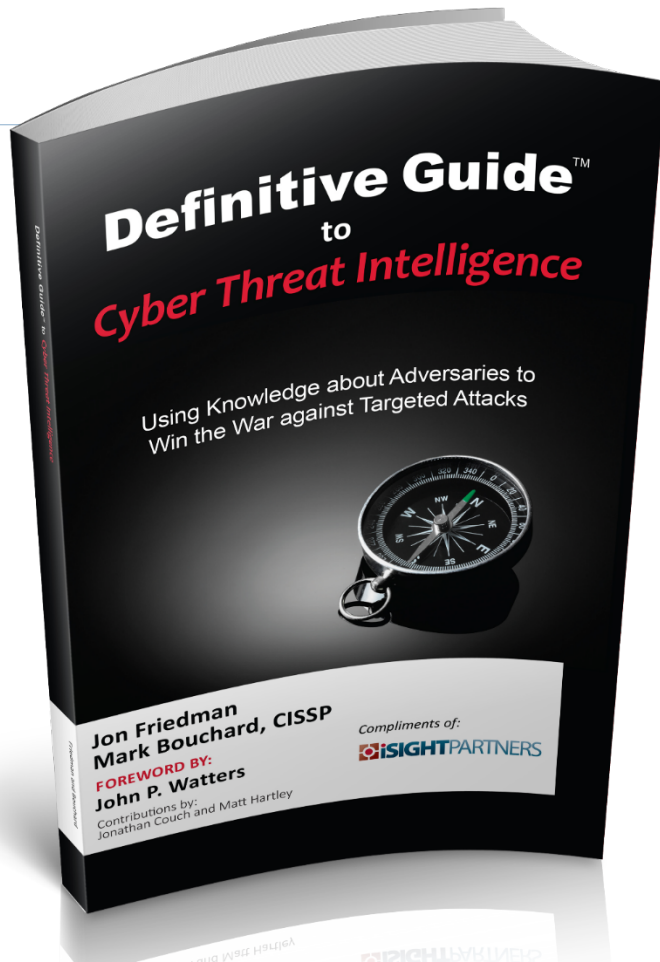
- 18 Nov 15, Sandworm Team tied to broader operation targeting ICS Networks using BlackEnergy
- 25 Nov 15, US academic research and development community targeted with repurposed Sandworm Team exploit
- 30 Mar 15, Changes to BlackEnergy demonstrate EU focus
- 12 Jun 15, BlackEnergy 3 malware used by Sandworm Team is capable of leveraging RPC over SMB¹ for both local and remote connections.
- 30 Dec 15, Cyber Espionage activity in Ukraine resembles sandworm team and nation-wide power outages in Ukraine caused by cyber attacks.
- 24 Jan 16, Spear phishing targeting Ukrainian energy sector distributed GCat Malware; May indicate sandworm team operators are shifting tools
- 29 Feb 16 and 17 Apr 16, Sandworm Team campaign leveraged searchable sensitive documents to target Ukrainian media, Boryspil Airport prior to destructive attacks

¹Remote File Protocol (SMB) over Message Block



Questions

iSIGHT Partners
The Cyber Threat Intelligence Experts



Please take a copy

Available to download at: [http://
info.isightpartners.com/definitive-guide](http://info.isightpartners.com/definitive-guide)