Indicators of Compromise per Cyber Threat Intelligence e Incident Response

M. Costa – Sinergy
G. Zanoni – Symantec

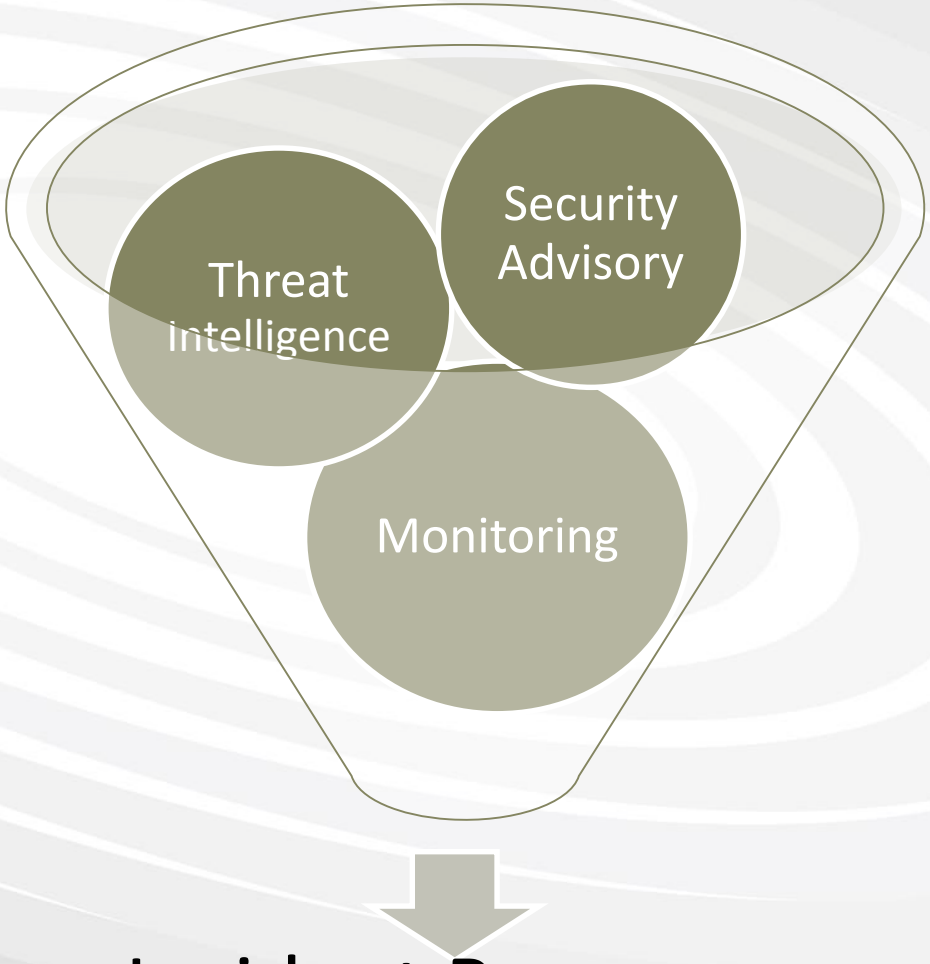
Security Summit Roma 2016

Agenda

- Threat Intelligence (M. Costa)
  - Lo scenario
  - Definizione di Threat Intelligence
  - Indicator of Compromise (IoC)
    - Cosa sono e a cosa servono gli IoC?
    - IoC – Creazione, Raccolta, Condivisione
    - Standard e Tools
- Incident Response (G. Zanoni)
  - La Threat Intelligence nella realtà: SOC, MSSP

Incident Management - Scenario

Gestione degli Incidenti di Sicurezza: elementi principali



Incident Management - Attività

Advisory	• Progettare e implementare
Monitoring	• Controllo on-site
Threat Intelligence	• Analisi
Incident Response	• Gestire l'attacco

Incident Management - Attori

Advisory	• Security Partner	SINERGY
Monitoring	• MSS & Security Partner	Symantec SINERGY
Threat Intelligence	• Managed Security Service Provider	Symantec
Incident Response	• MSS & Security Partner	Symantec SINERGY

“Threat” - Definizioni

- Definizione nello Standard ISO 27000

  “a **potential cause of an unwanted incident**, which may result in harm to system or organization”

- Definizione NIST SP 800-30

  “any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service”

“Threat” - Definizioni

- **CyberThreat** – Department Homeland Security (DHS)

  “is **any identified effort** directed toward access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security, or availability of data, an application, or a federal system, without lawful authority”

… si… ma sappiamo riconoscere IN TEMPO UTILE se la minaccia diventa un VERO attacco ?!?

Esempio di Threat: APT (Advanced Persistent Threat)

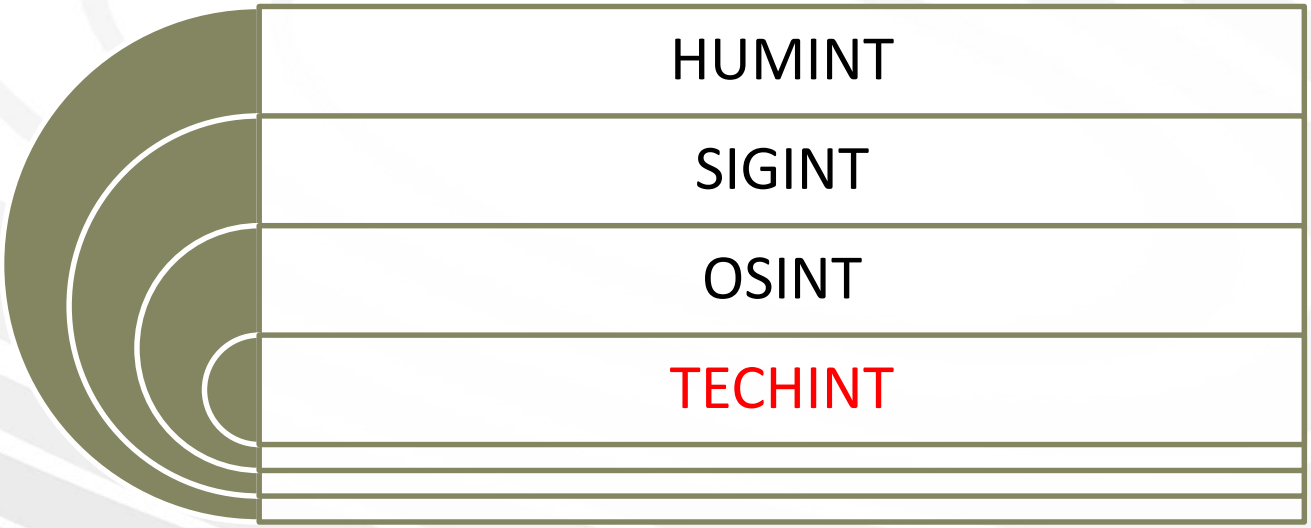
- **APT** non è (solo) malware oppure una singola attività ostile, ma definisce una serie di azioni offensive dalle seguenti caratteristiche:
  - **Target**: mirati su obiettivi specifici, con una strategia d'attacco complessa
  - **Attori**: criminali organizzati, entità governative, spie industriali, mercenari o gruppi con capacità equivalenti
  - **Strumenti**: sistemi di intrusione allo stato dell'arte: Malware avanzato, in combinazione con Social Engineering
  - **Timing**: tempi anche molto lunghi (mesi/anni)

- **Possibili Contromisure?**
  - Tecnologiche, Organizzative e…

Intelligence

Intelligence

Information that provides relevant and sufficient **understanding** for mitigating the impact of a harmful event in the cyber domain*



Techint - digital footprint of technology
OR the forensic trails of an attack

* Bank of England - CBEST

Threat Intelligence

Information about threats and threats actors that provides relevant and sufficient **understanding** for mitigating the impact of a harmful event in the cyber domain*

Per gestire minacce sempre più sofisticate
è possibile adottare una delle metodologie standard dell'attaccante: **la ricognizione preventiva del target!**

* Bank of England - CBEST

Threat Intelligence vs Information Gathering

Sfruttare lo stesso principio: effettuare una **ricognizione**

Cercare **elementi capaci di evidenziare l'attacco / compromissione** "ASAP"

*«**Conosci il nemico come conosci te stesso**. Se farai così, anche in mezzo a cento battaglie non ti troverai mai in pericolo»*
(Sun Tzu – L'Arte della Guerra)

Threat Intelligence

Non è una novità!

Usata da anni con elementi quali ad esempio:

- Database di vulnerabilità, firme antivirus, IP/URL reputation
- Firme di traffico di rete, netflow, ecc.
- Specifici pattern di attacco evidenziati da CERT e/o Security Firms
- Forensics evidence

e infatti...

Threat Intelligence

Esistono “Fornitori di Threat Intelligence”, ma…

Attenzione a cosa si compra... **Non è un prodotto**!

Perchè?

- Le informazioni devono essere contestualizzate
- Se sono solo liste di “raw data”, possono essere poco utili

Threat Intelligence (2.0?)

Esempi di informazioni che dovrebbero essere disponibili:

- Chi mi sta attaccando? Perchè?
- Come mi stanno attaccando?
- Stanno attaccando i miei partner/fornitori/terze parti o i miei competitors?
- Che metodi stanno usando? Quali skill/tools?

Ovvero servono:

- **Tools, Tactics and Procedures (TTP)…**
- …a integrazione delle **evidenze "osservabili"** (file, hash, IP ecc.): **IoC** !!!

Indicator of Compromise

- Gli elementi distintivi che concorrono all'utilizzo della TechInt sono gli IoC

- **Indicator of Compromise**: un artefatto individuato su reti o sistemi elaborativi che indica, con un elevato grado di confidenza, la presenza di un'intrusione informatica*

*RSA Corporation

Indicator of Compromise

Esempi di **IoC**

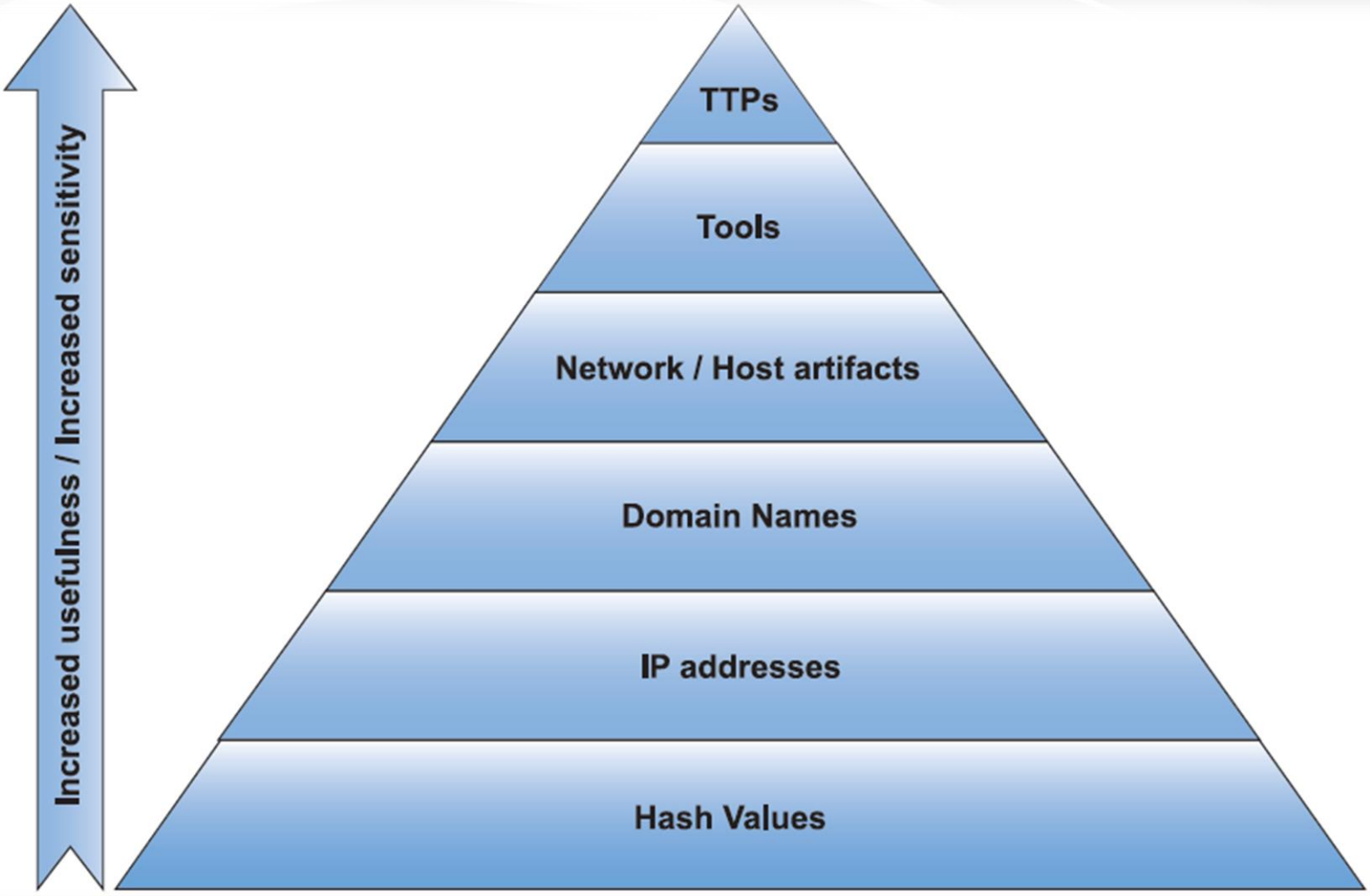
- IP e URL (compromessi o di reputazione scadente)
- Hash (di sample, malware ecc)
- Parti di Windows Registry
- File
- Associazioni porte e applicazioni anomale
- Traffico anomalo (es: DNS malformato)
- …

Indicator of Compromise

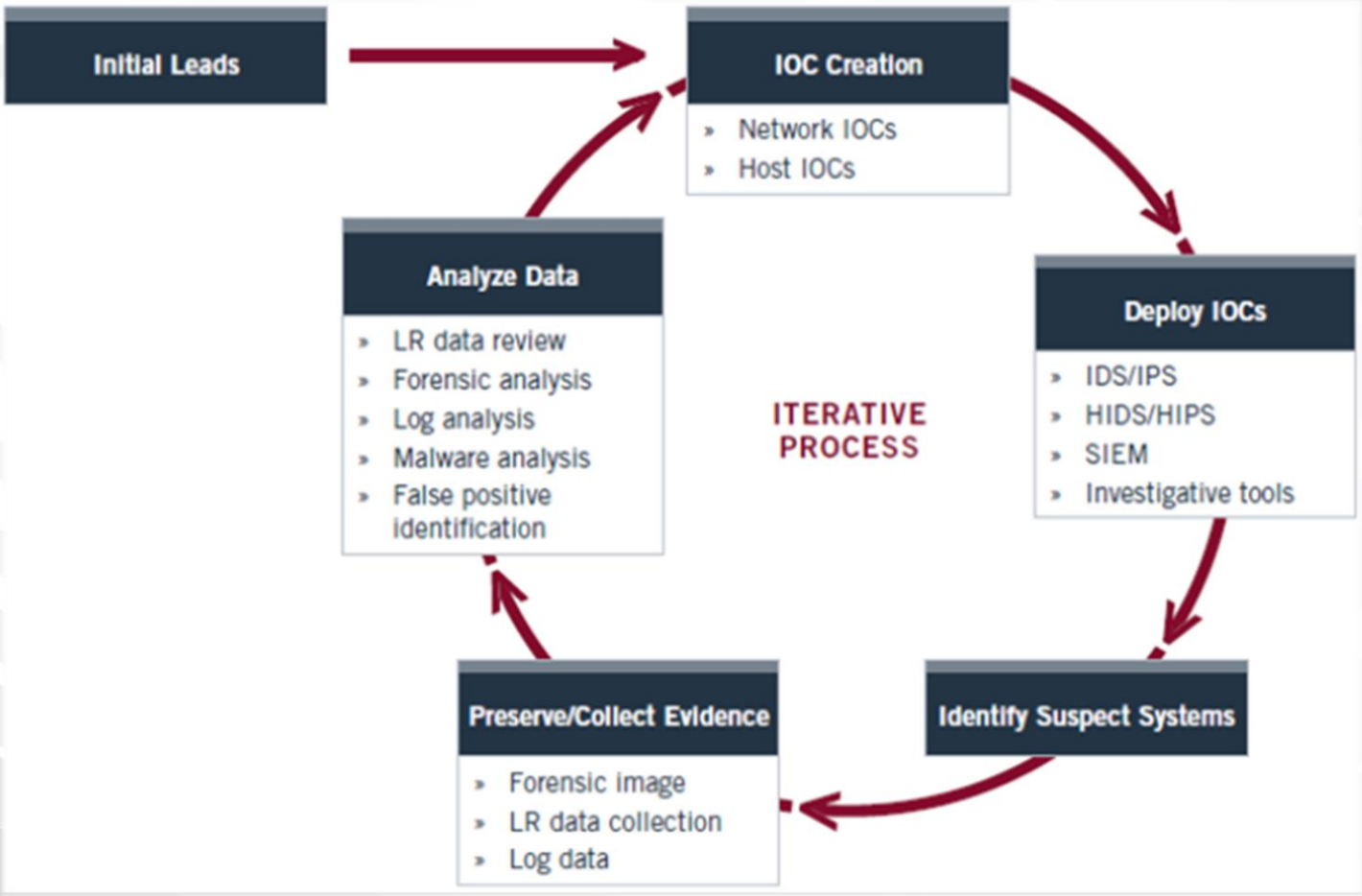
Ma possono essere creati anche IoC “comportamentali”, ovvero anomalie:

- Nel traffico di rete
- Nell‘attività di accesso ai sistemi
- Uso di credenziali privilegiate
- Risposte anomale a interrogazioni HTML (esempio dopo una SQL injection)

Indicator of Compromise



Indicator of Compromise LifeCicle (es. OpenIoC)



E' sempre più importante la CONDIVISIONE delle informazioni !!!

IoC Quality

Creare un IoC è semplice, ma deve essere un elemento **efficace** ed **efficiente** per l'analista:

- Un IoC
  - deve essere **specifico** (indicare una modalità precisa di attacco/compromissione)
  - deve raccogliere abbastanza informazioni da rendere **complesso** per l'attaccante **evadere** l'IoC individuato
  - **facile** da elaborare, modificare e condividere

IoC Management

- **Creare IoC**: Facile
- **Categorizzarli**: Complesso
- **Utilizzarli**: Moderatamente Complesso
- **Condividerli**: Complesso

Servirebbe un Framework per gestire queste informazioni in modo strutturato..!

IoC: Standard(?)

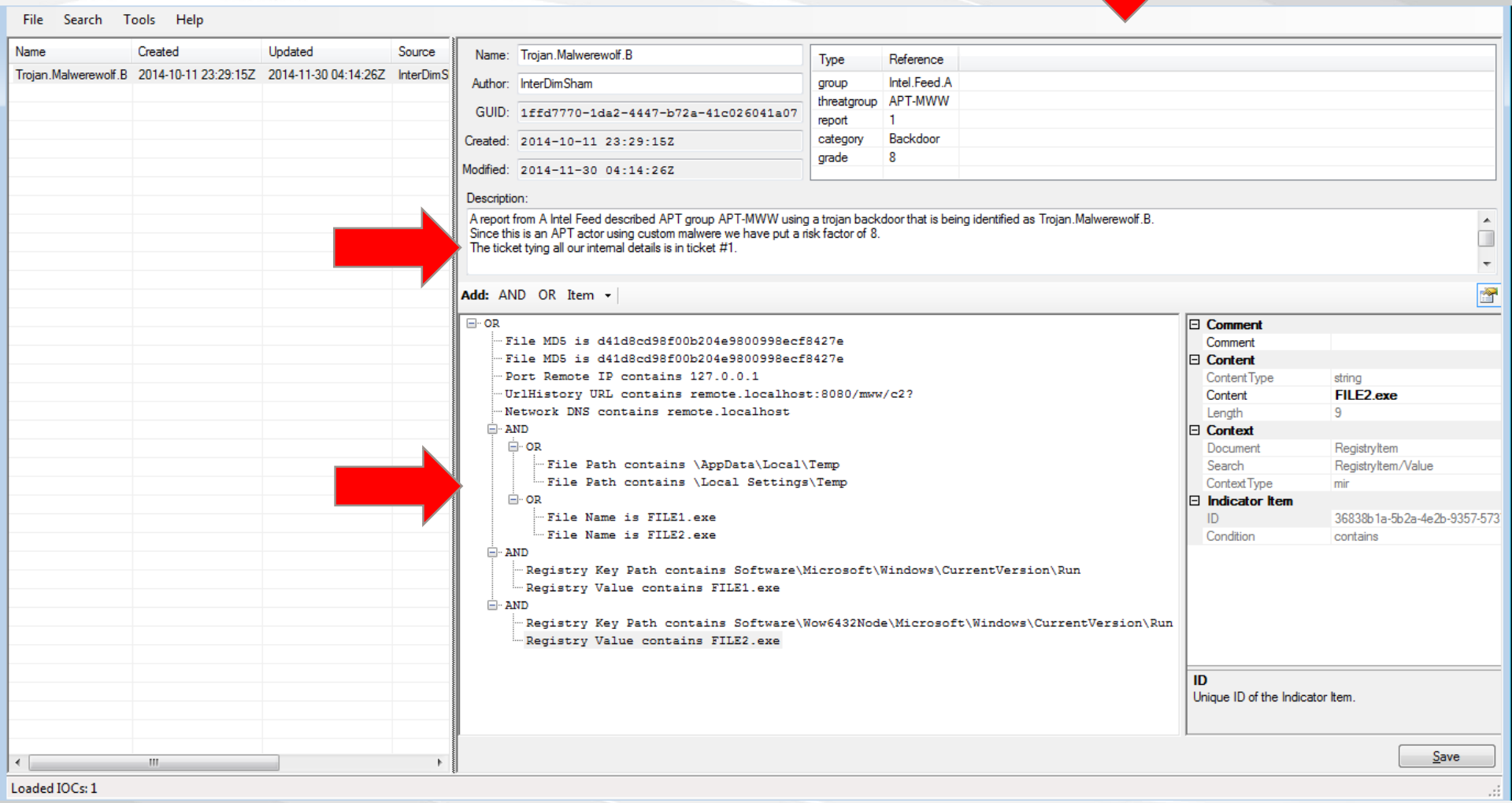
- Mandiant (Private Company) – **OpenIoC**: uno dei primi e più utilizzati
- OASIS – **STIX e TAXII** (precedentemente MITRE.org)
- OASIS – **CyBOX** (precedentemente MITRE.org)
- IETF – **RFC 5070 - IODEF**
- Altre proposte: **YARA**, **MMDEF** (Malware Metadata Exchange Format), **MAEC** (Malware Attribute Enumeration and Characterization), ...

OpenIoC

- **OpenIoC** è un framework (un XML Schema, estendibile) per descrivere le caratteristiche tecniche che identificano un threat, le metodologie di attacco o altre evidenze riconducibili ad attività malevole.
- OpenIoC permette di raggruppare logicamente gli artefatti digitali, che possono quindi essere trasmessi ad altre applicazioni

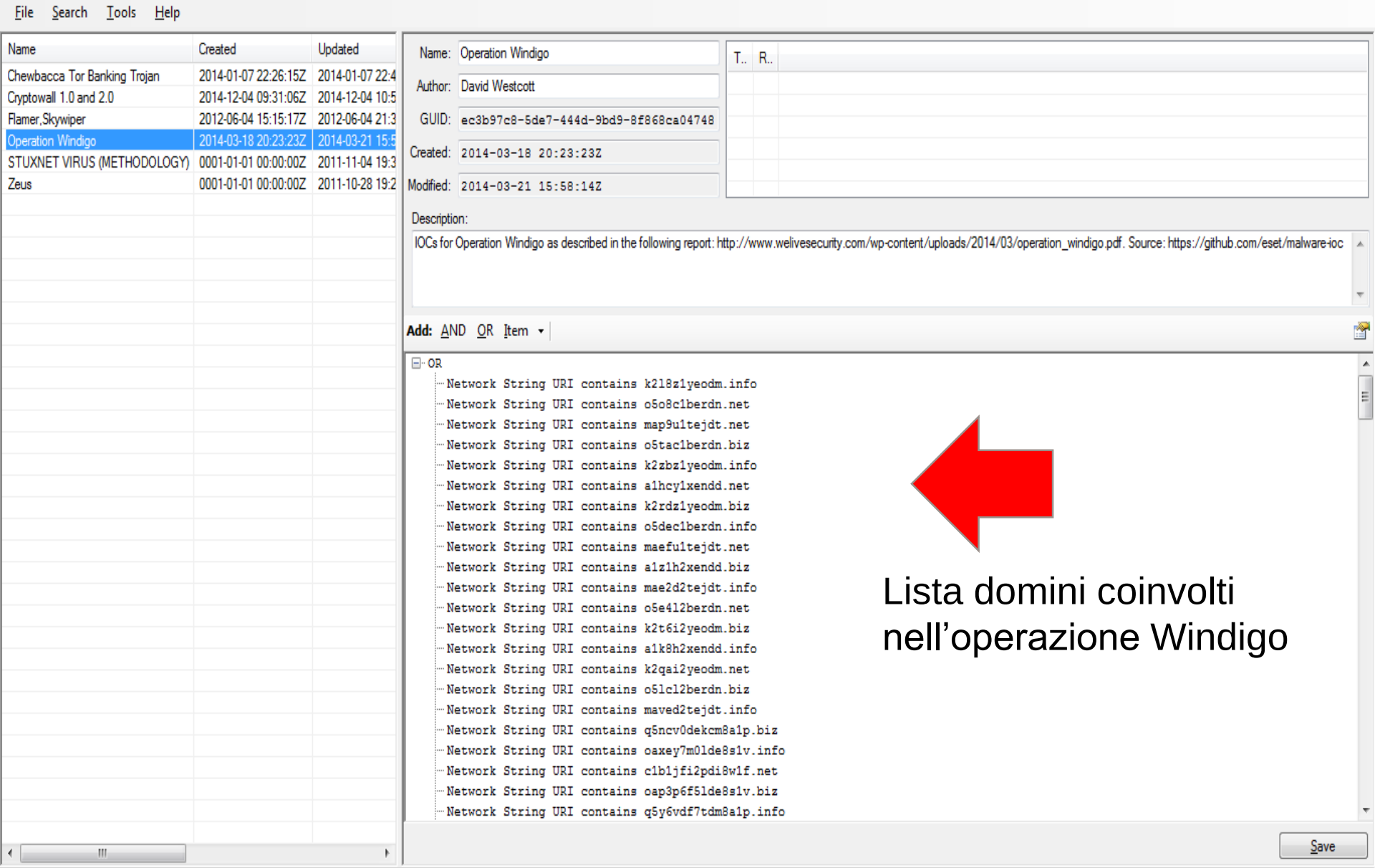
- Gli elementi descrittivi che può gestire sono:
  - **Metadati**
  - **Riferimenti**
  - **Definizioni**

Esempio OpenIoC



APT Trojan.Malwerewolf.B

Esempio OpenIoC



Lista domini coinvolti nell'operazione Windigo

CybOX

Cyber Observable eXpression (CybOX™)

- CybOX è un **linguaggio** (XML Schema) utilizzato per la descrizione di «Observable Objects»
- Gli Observables sono artefatti chiaramente identificabili sui sistemi informativi che possono essere riconducibili ad attività malevola
- Esempi di Observables sono:
  - Indirizzi IP
  - Hash
  - Chiavi di registro
  - URI
  - Sessioni HTTP
  - ecc.

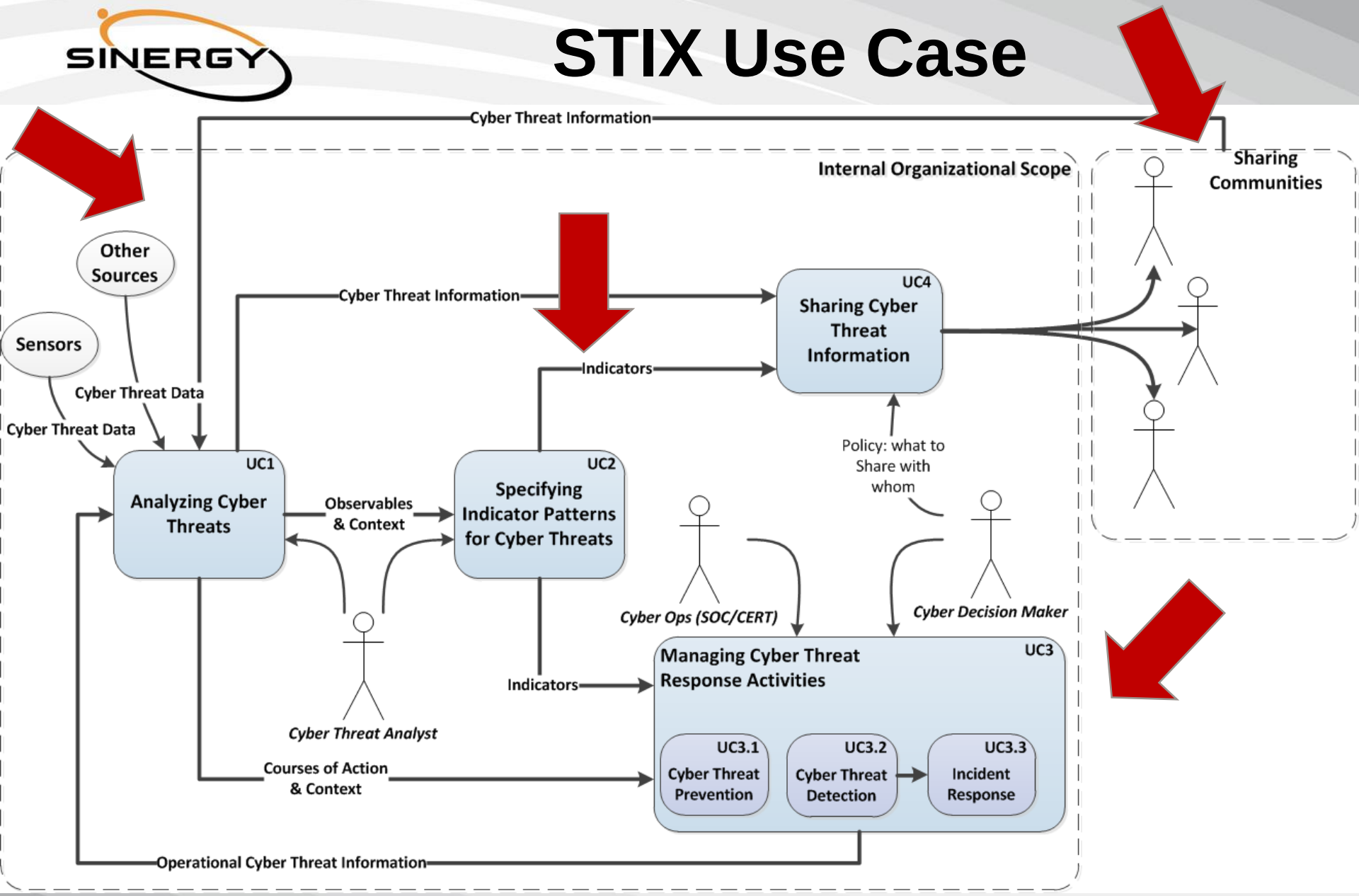
STIX

Structured Threat Information eXpression (STIX™)

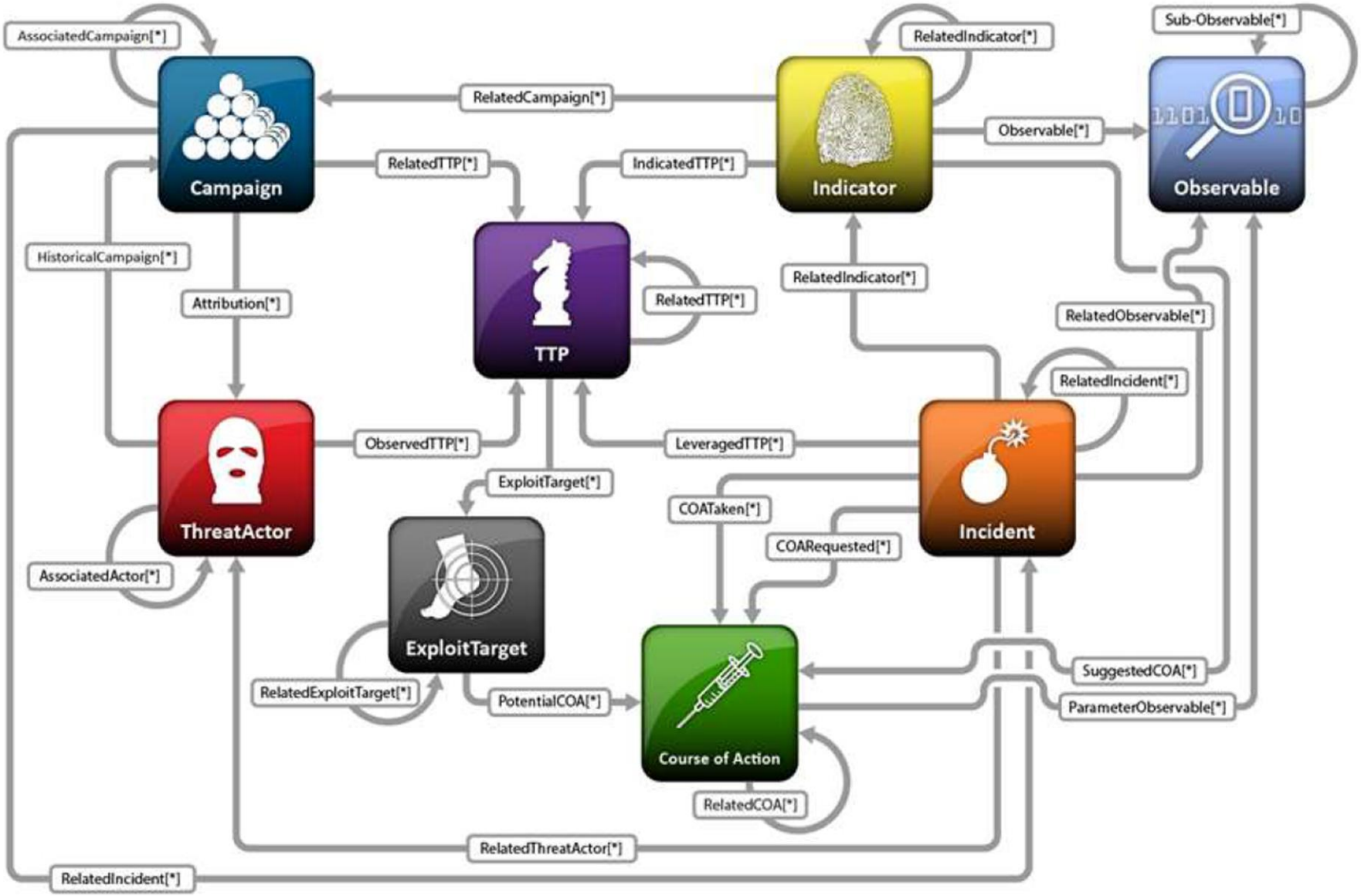
- E’ un **linguaggio** standardizzato (XML Schema) per la descrizione delle informazioni relative ai CyberThreats.
- Pensato per gestire le informazioni relative ai CyberThreats per i più comuni casi d’uso:
  - Creazione di IoC
  - Arricchimento di informazioni di contesto
  - Distribuzione degli IoC

- È molto più completo di OpenIoC, può gestire anche indicatori quali *C&C activity, data exfiltration activity, compromised login credentials* …

STIX Use Case



STIX Architecture



TAXII

Trusted Automated eXchange of Indicator Information (TAXII™)

- E' un **insieme di specifiche** (XML Schema) che definisce le modalità di scambio e condivisione di informazioni relative a CyberThreats
- Originariamente introdotto da Homeland Security al fine di:
  - Consentire uno **scambio rapido e sicuro delle informazioni** sulle minacce
  - Supportare un ampio raggio di **casi d'usi e practice relative alla condivisione di cyber info**
  - Supportare l'uso di **meccanismi esistenti**
  - Perseguire l'adozione del protocollo come **standard internazionale**

Tools

- OpenIoC
  - IoC Editor/IoC Finder, OpenIoC-to-STIX
- CyBOX
  - python-cybox, 19 cybiet
- YARA
  - Yara, jsunpack
- SNORT
- STIX
  - Microsoft Interflow, CRITs, MANTIS, python-stix46
- OpenSource
  - http://bluecloudws.github.io/ioceditor/
  - https://github.com/yahoo/PyIoCe

IoC Sharing – Le Community

- IOC Bucket (https://www.iocbucket.com)
- OTX – Open Threat Exchange (https://otx.alienvault.com)
- Information Sharing and Analysis Center (ISAC)
  - FS-ISAC – Servizi Finanziari
  - R-CISC – Retail
  - IT-ISAC – Info technology
  - E-ISAC – Electricity
- …

Riassumendo

- Raccogliere IoC (sia internamente che su Internet)
- Aggiungere le informazioni di contesto (se assenti)
- Sfruttare queste informazioni! (e condividerle …)

Incident Response Team/MSS

IoC usage in MSS and IR

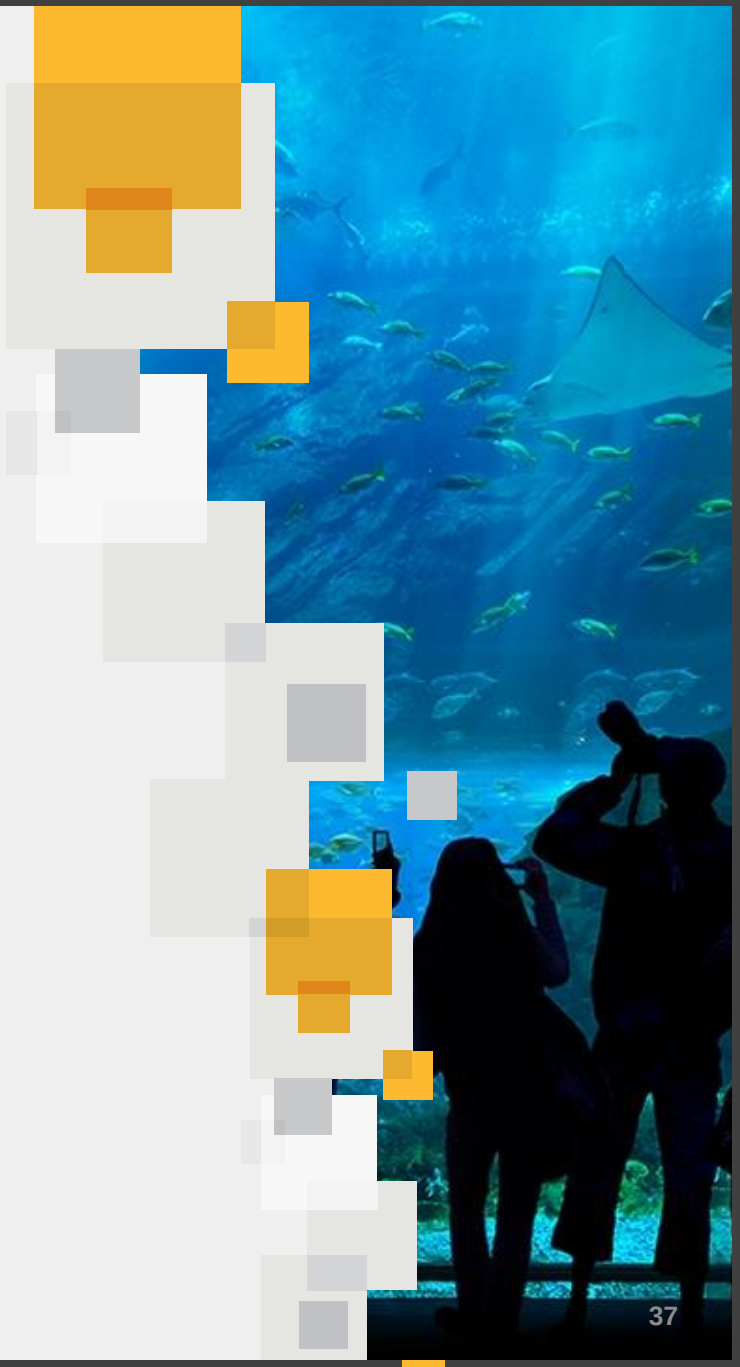
Gabriele Zanoni

EMEA Incident Response Investigator
Symantec Cyber Security Services

Index

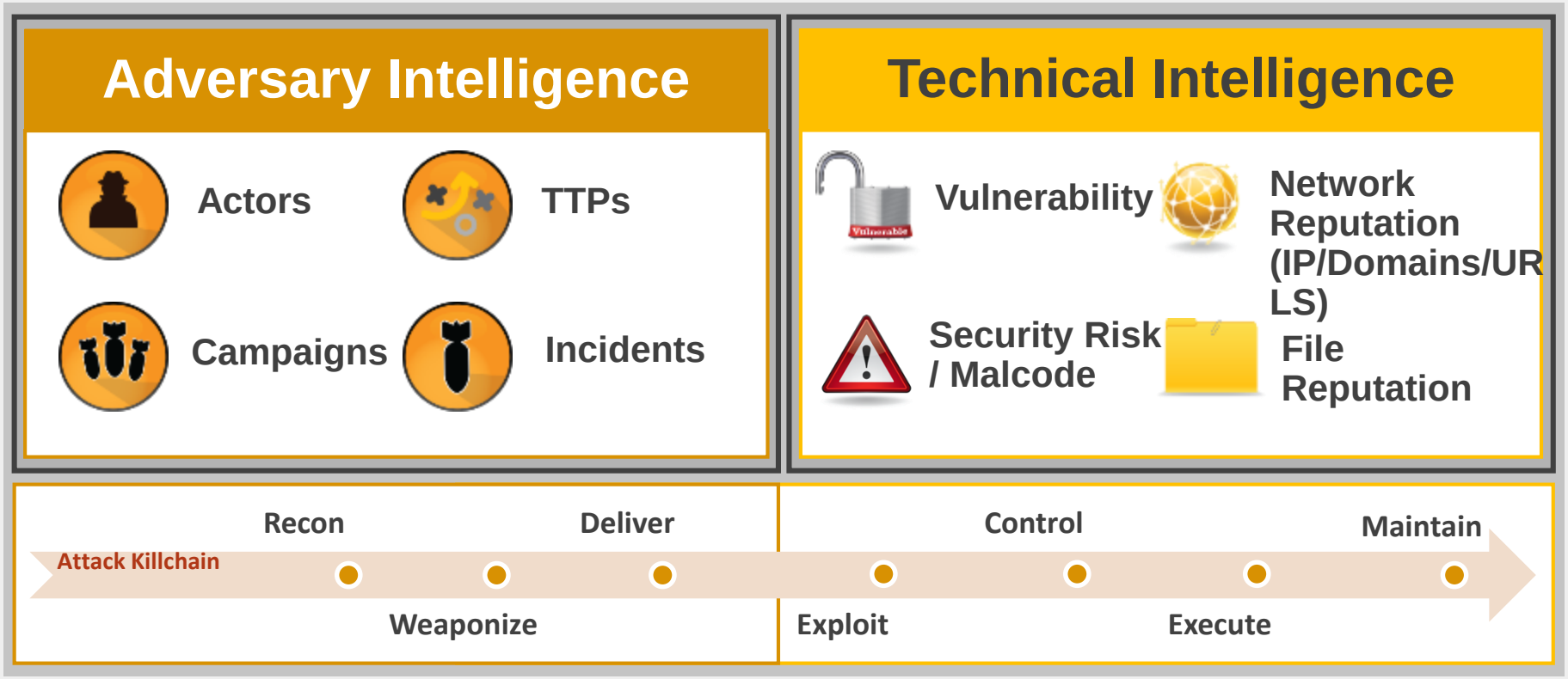
Copyright © 2016 Symantec Corporation

Technical and Adversary Intelligence



Copyright © 2016 Symantec Corporation

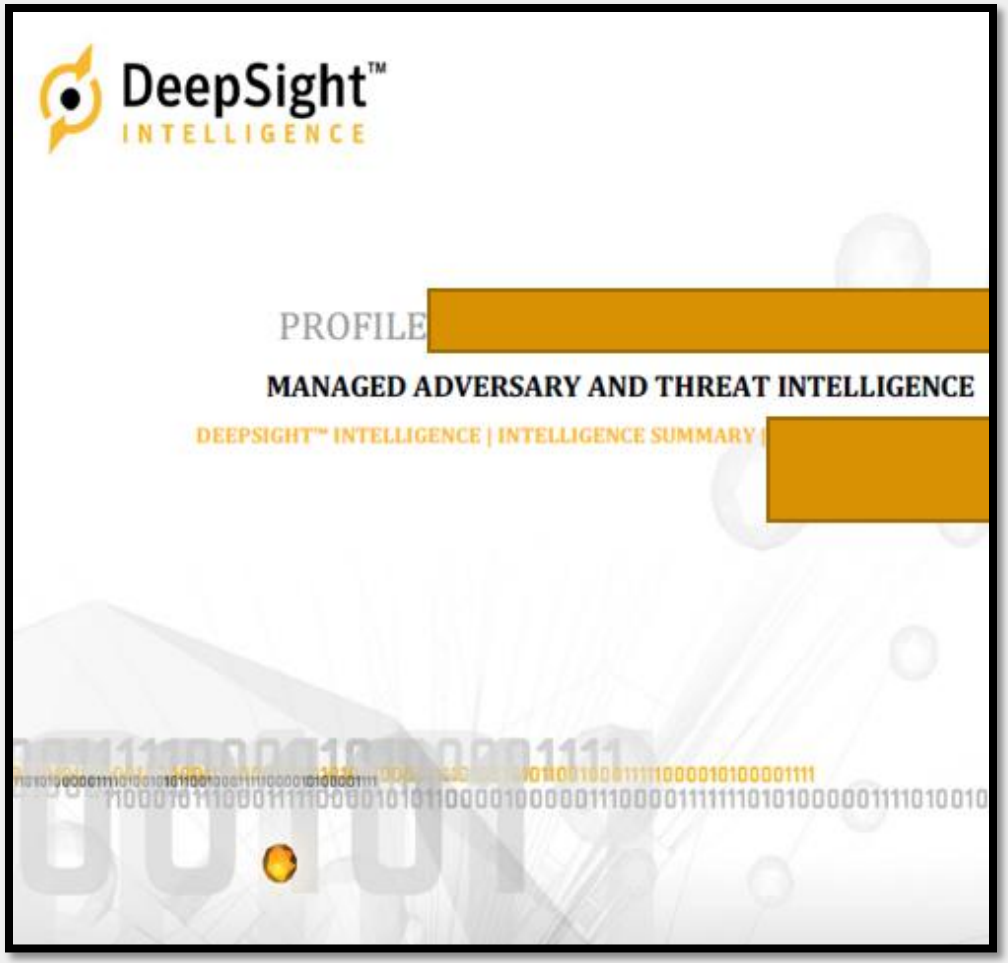
Intelligence Has to Evolve



Outside your perimeter *Inside your perimeter*

Copyright © 2016 Symantec Corporation

Example of a Symantec MATI report (Managed Adversary Threat Intelligence)



Examples of information provided:

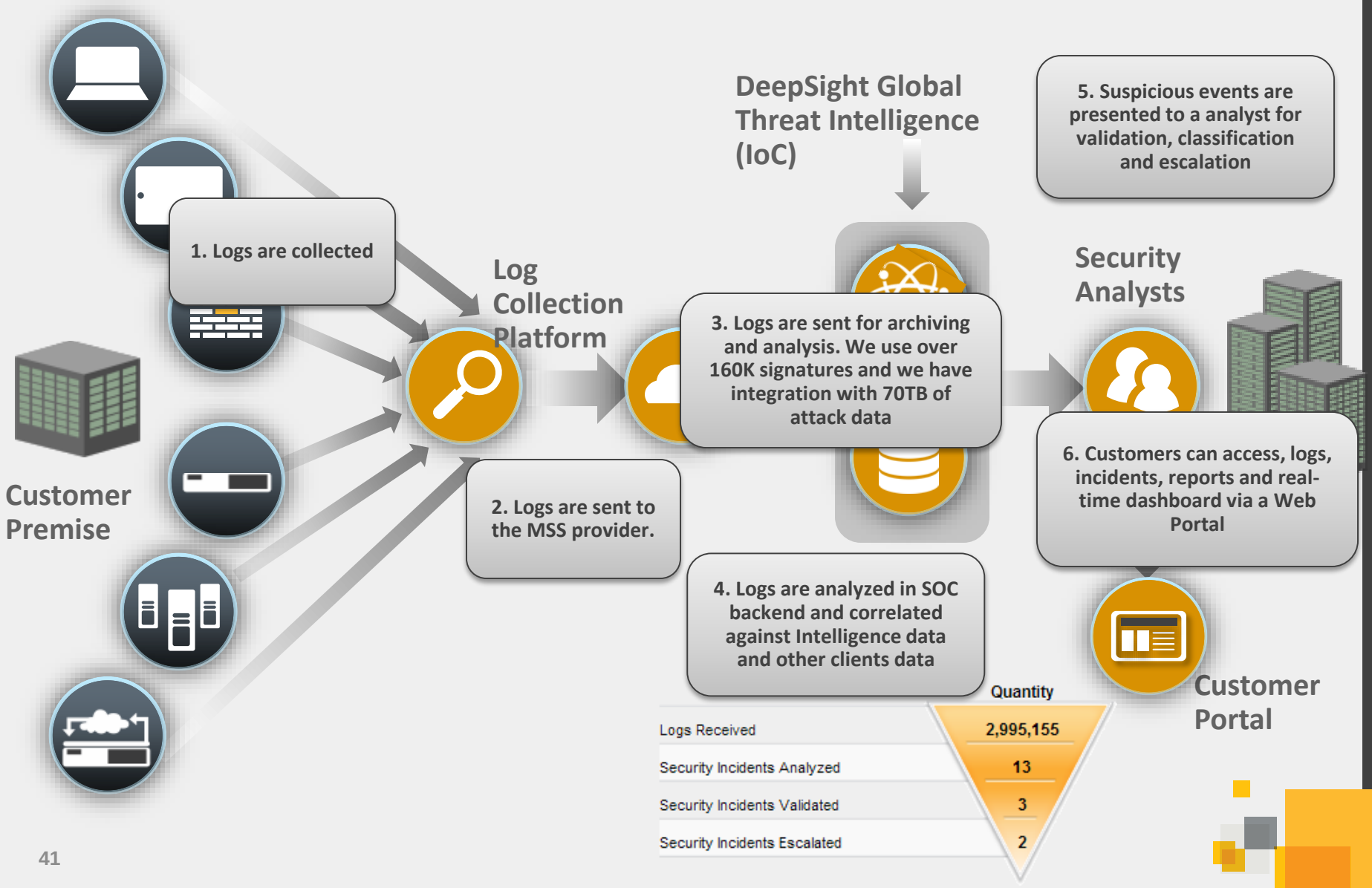
- Adversary Profile
- Campaigns
- Timeline of the attacks
- Attackers' accounts on Socials
- Tactics/Techniques/Procedures
- Indicators of Compromise
- Metadata (Source Region / Target Region / Threat Domain)
- Etc..

Copyright © 2016 Symantec Corporation

IoC usage in a MSS provider

Copyright © 2016 Symantec Corporation

IoC usage inside a Managed Security Service provider



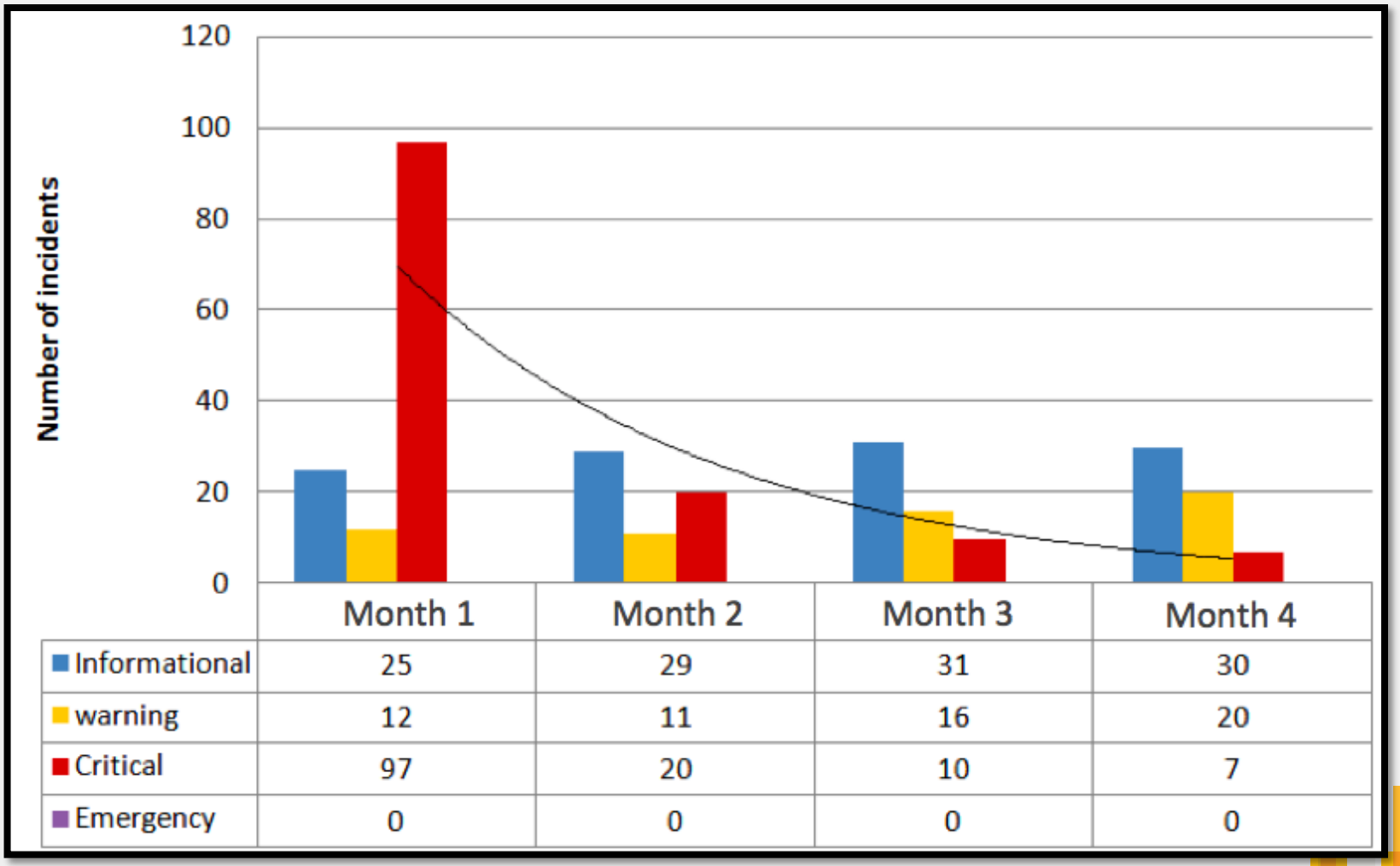
Correlation activities inside MSS

- Examples of IoC based correlations:
  - Network Device (e.g. firewall, router, proxy etc..) correlation: discover network flows going to IP addresses marked as Attack / Bot / CnC / Fraud / Malware / Phishing / Spam.
  - Managed Adversary Threat Intelligence (MATI) correlation: discover if a specific hacking group is targeting an organization.
  - Other data correlation: check of attacking patterns in our Global Intelligence Network
- Examples of correlations with other detection engines:
  - Domain Generation Algorithm (DGA)
  - OSINT from Internet leaked data
  - Smoke detector: use of big data and machine learning techniques to identify "low-and-slow" threats.

Copyright © 2016 Symantec Corporation

This example clearly demonstrates how MSS has improved a customer's security protection and reduced their risk profile in a very quick time frame.

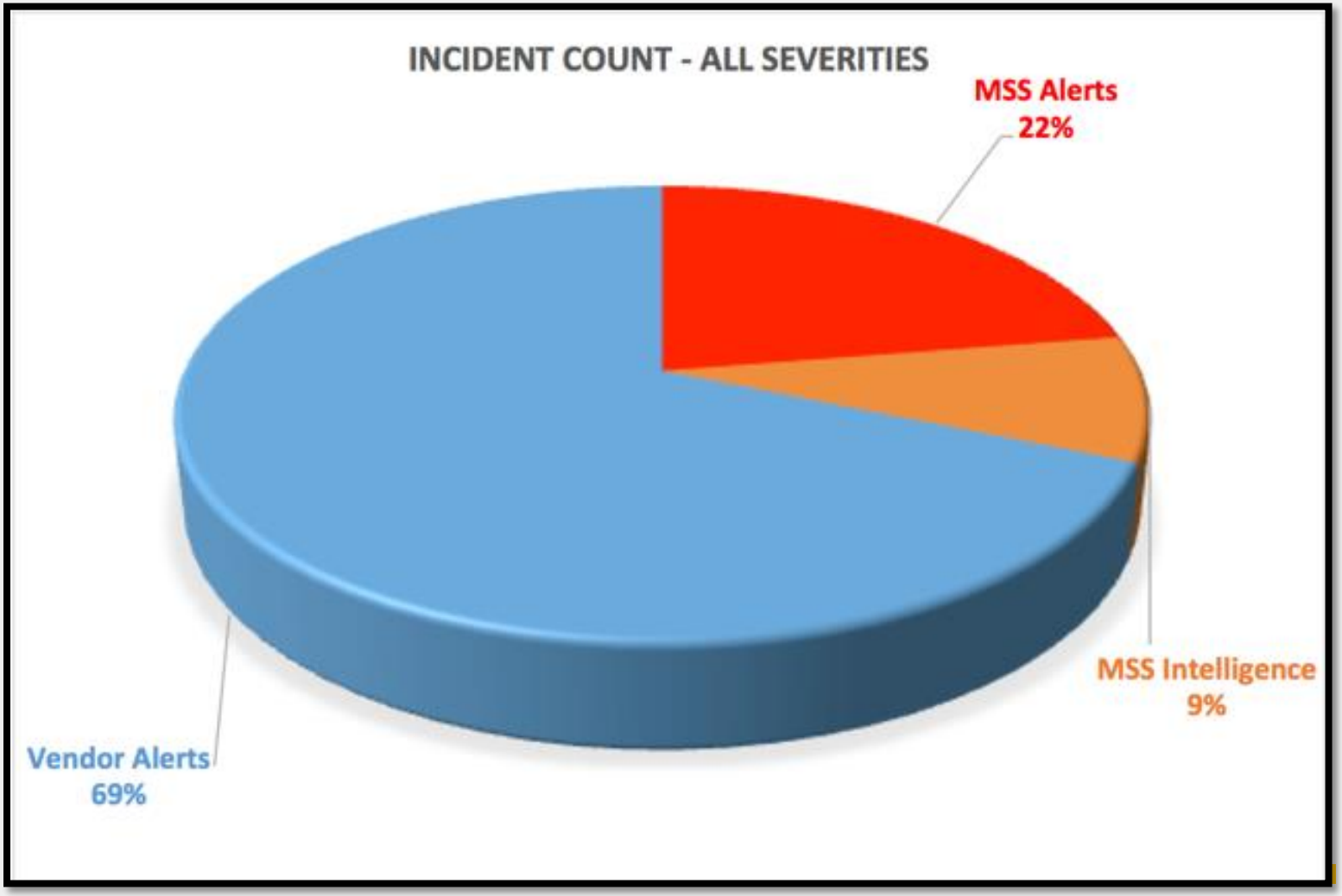
Security Incidents per Month



	Month 1	Month 2	Month 3	Month 4
Informational	25	29	31	30
warning	12	11	16	20
Critical	97	20	10	7
Emergency	0	0	0	0

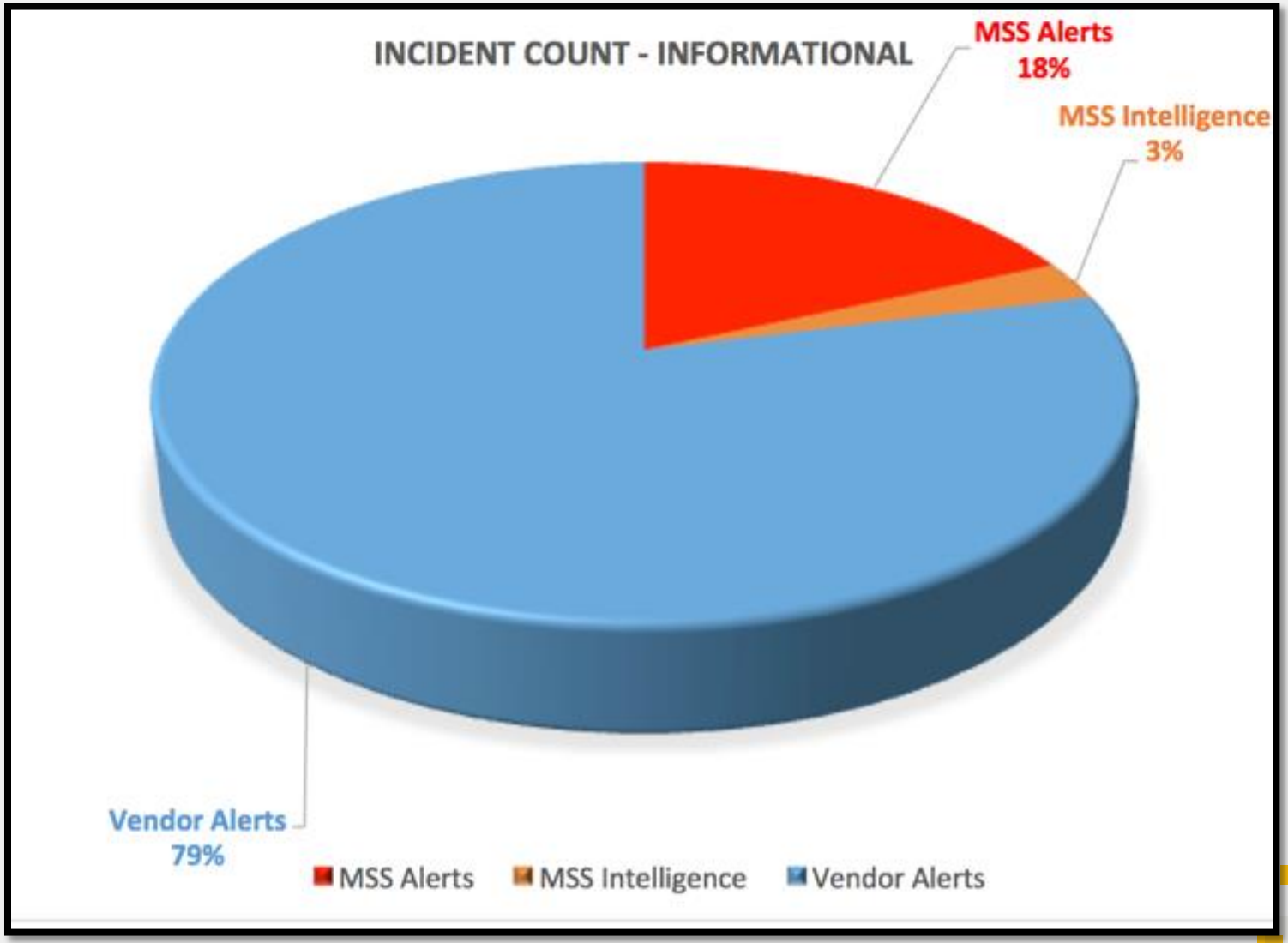
43

During April. 2016 MSS detected ~29K Incidents just for EMEA customers



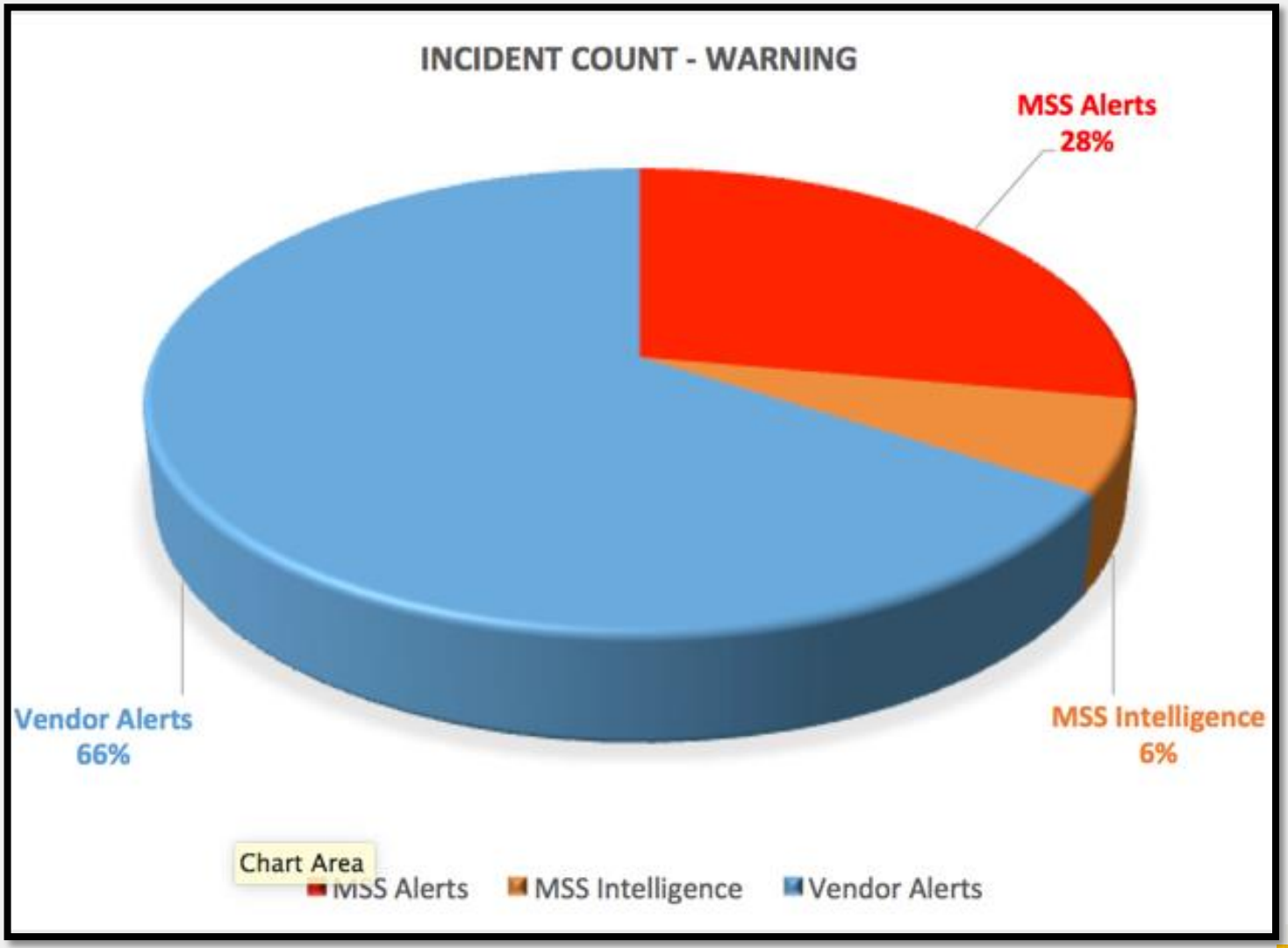
Copyright © 2016 Symantec Corporation

Drill down



Copyright © 2016 Symantec Corporation

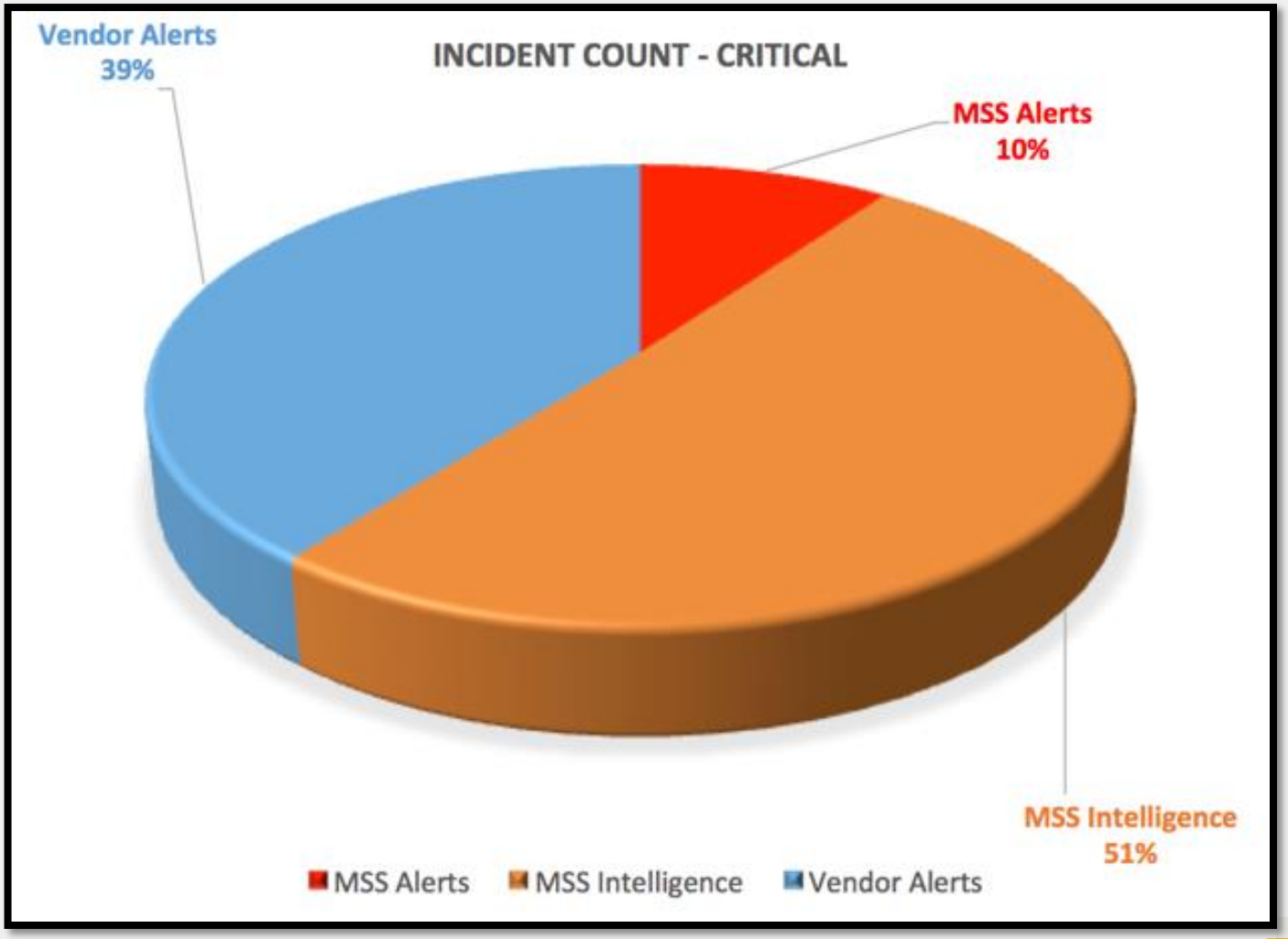
Drill down



Copyright © 2016 Symantec Corporation

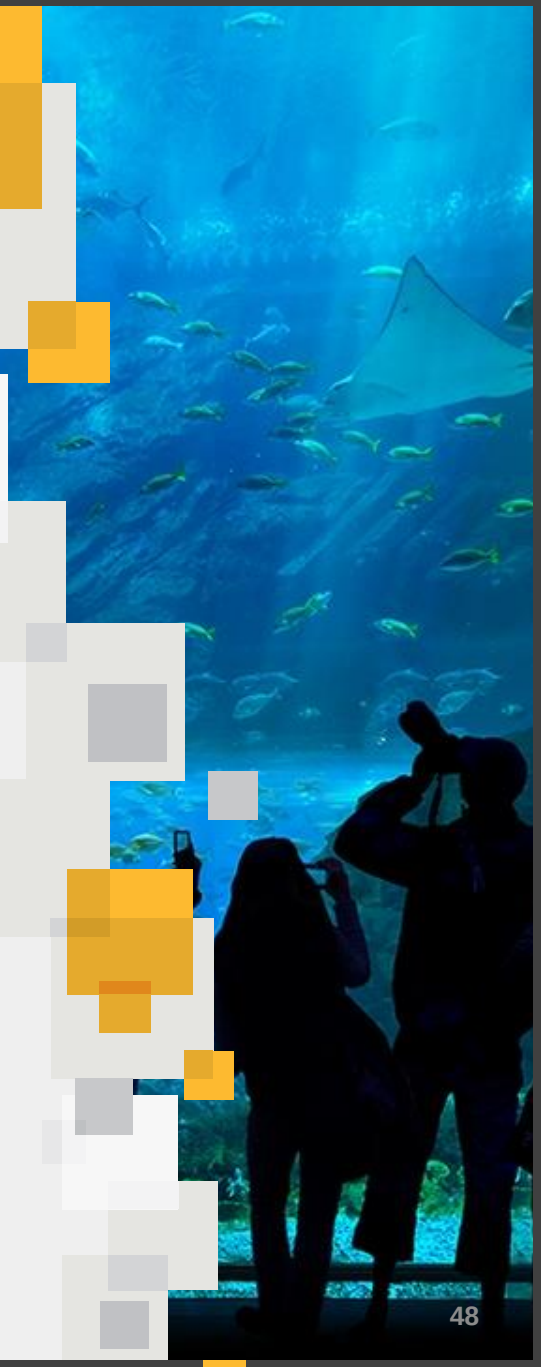
Drill down

If you do not have a reliable and accurate source of intelligence you are blind on 40%-50% of critical incidents!



Copyright © 2016 Symantec Corporation

IoC and Incident Response



Copyright © 2016 Symantec Corporation

IoC usage in Incident Response activities

- Examples:
  - **APT Hunting**: detect if networks/servers have been already compromised, such detection is done using IoC and EDR tools. We enrich the indicators with extra intelligence that is designed to find not just definitive bad, but also artefact of bad (key reg, file path, other files dropped etc..).
  - **Malicious flow detection**: the correlation is performed using a reputational feeds with malicious IP addresses/Domains/URLs.
  - **Identify attackers during an incident**: the TTP could be used to identify if an attack is part of a specific attacking campaigns and reveal the attacker's group.
  - **Preparation:** check of the relevant TTP in order to prepare tailored defending capabilities (e.g. tabletop exercises etc..).

Copyright © 2016 Symantec Corporation

A story from the trench

- Customer called the IR Team sharing details of an incident.
- After the triage call, the IR Team did a deep investigation into intelligence to check other attacks on the same customer's vertical.
- We checked potential Adversary Profiles and we found evidences of the same kind of attack into MATI reports.
- IR Team deployed at customer’s premise was fulfilled with all relevant IoC and has timely detected a known pattern of attack related to a specific attackers’ group.
- Thanks to MATI info, the IR Team was also able to found new malicious binaries and related IoC.
- New signatures have been created and shared with MSS.
- New rules have been ran across all MSS customers.

Copyright © 2016 Symantec Corporation

Cyber Security Services

Intelligent | Vigilant | Responsive | Ready

Track Key Trends and Events and Analyze for Actionable Intelligence	Cyber Intelligent	DeepSight Intelligence and Managed Adversary Intelligence
Protect Against Targeted Attacks, Advanced Threats and Campaigns	Cyber Vigilant	Managed Security Services
Respond Quickly and Effectively to Credible Security Threats & Incidents	Cyber Responsive	Emergency Response and Retainer Services
Strengthen Cyber Readiness to Prevent Today's Advanced Attacks	Cyber Ready	Cyber Security Exercise and Security Simulation

Copyright © 2015 Symantec Corporation

Thank you!

Gabriele_Zanoni@symantec.com

EMEA Incident Response Investigator
Symantec Cyber Security Services

Copyright © 2016 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

Copyright © 2016 Symantec Corporation