Indicators of Compromise per la Cyber Threat Intelligence e l'Incident Response

R. Leone, Sinergy, r.leone@sinergy.it
G. Zanoni, Symantec, Gabriele_Zanoni@symantec.com

Security Summit Milano 2016

AGENDA

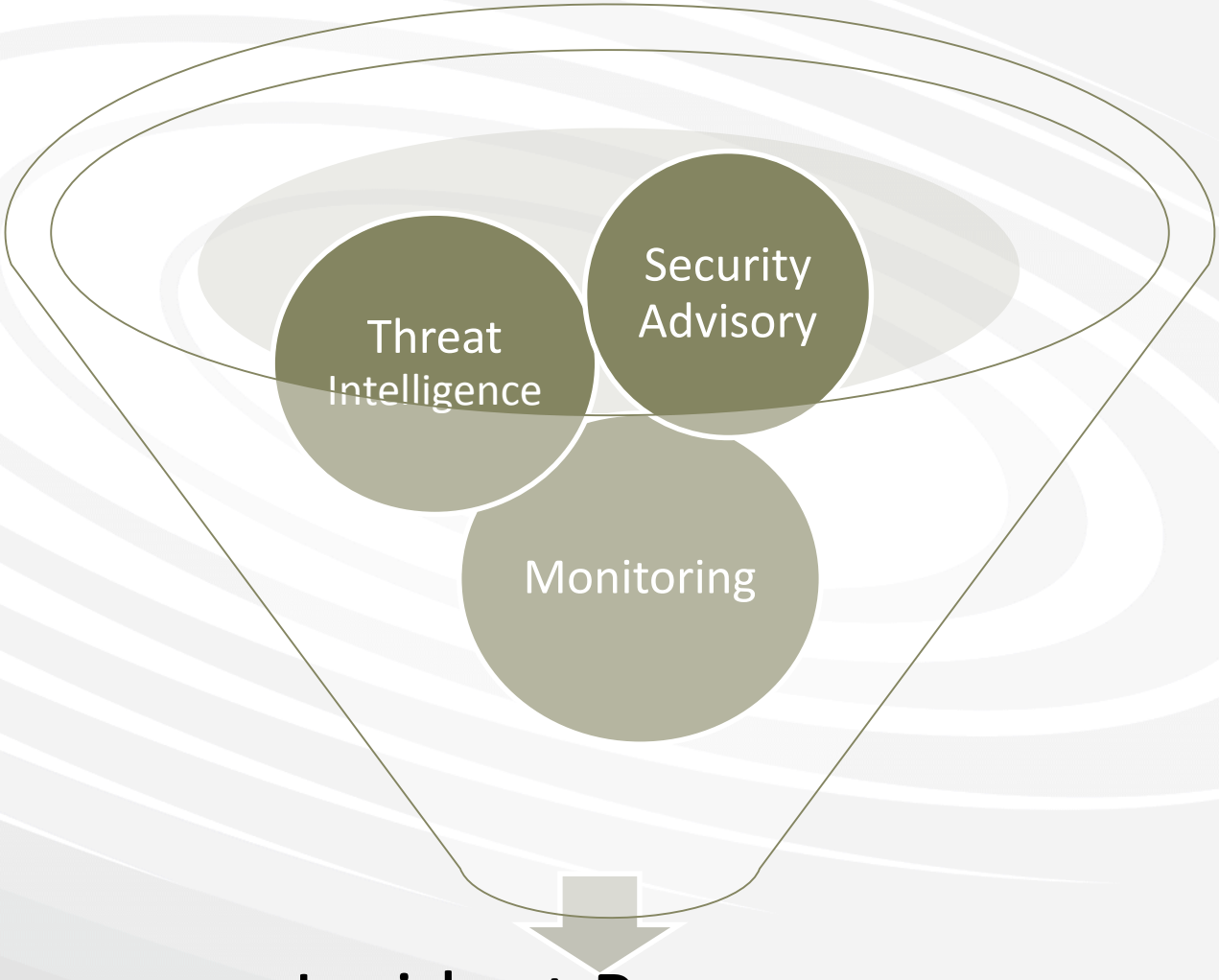
- Lo scenario
- Definizioni di *Threat & Intelligence*
- Indicator of Compromise (IoC)
- Cosa sono e a cosa servono gli IoC?
- IoC – Creazione, Raccolta, Condivisione
- Standard e Tools

- La Threat Intelligence nella realtà: SOC, MSSP

Riferimenti sull'ultima slide

Disclaimer*: molte definizioni sono in inglese*

SCENARIO


Security Advisory
Threat Intelligence
Monitoring
Incident Response

ATTIVITA'

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

ATTORI

Advisory	• Security Partner
Threat Intel	• Managed Security Service Provider
Monitoring	• Managed Security Service Provider
Incident Response	• MSS & Security Partner

"THREAT" - DEFINIZIONI

- DEFINIZIONE NELLO STANDARD ISO
  - a **potential cause of an unwanted incident**, which may result in harm to system or organization [ISO/IEC 27000:2016]

- 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

- **CYBER**THREAT – DHS – Department Homeland Security
  - "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"

- IN PRATICA:
  - " *… si… ma sappiamo riconoscere IN TEMPO UTILE se la minaccia diventa un VERO attacco ?!?*"

Esempio: 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

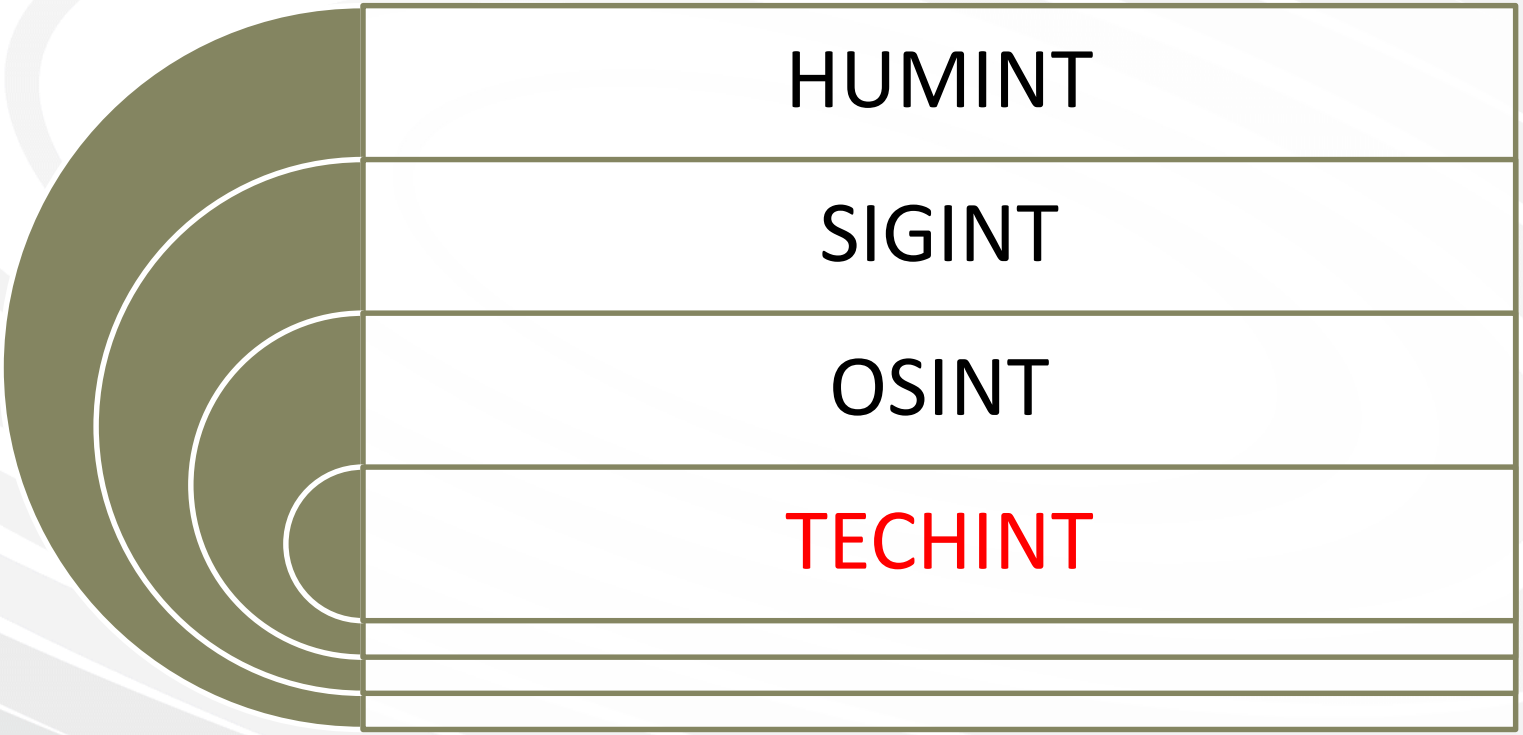
Strumenti: sistemi di intrusione allo stato dell'arte: Malware avanzato, in combinazione con Social Engineering

Timing: tempi anche molto lunghi (mesi/anni)

CONTROMISURE?

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

THREAT INTELLIGENCE: DEFINIZIONE

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

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*

* Bank of England

THREAT INTELLIGENCE

Per gestire minacce sempre più sofisticate
è possibile adottare una delle metodologie standard dell'attaccante:

- la ricognizione preventiva del target!

THREAT INTELLIGENCE vs. INFORMATION GATHERING

Usare la stesso principio -
una *ricognizione:* cercare elementi capaci di evidenziare l'attacco/compromissione
"asap"

THREAT INTELLIGENCE

Non è una novità: usata da anni con elementi quali:

- ✓ 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**”

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
- ✓ Dovrebbero fornire almeno: il meccanismo di distribuzione, gli attori, le potenziali vittime, il vettore di attacco, TTP ecc.

THREAT INTELLIGENCE (2.0 ?)

- Le informazioni che devono essere rese disponibili: (ad esempio)

  - 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 le TTP :
Tools, Tactics and Procedures
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 la presenza di un'intrusione informatica, con un elevato grado di confidenza *

*RSA Corporation

INDICATOR of COMPROMISE

- **Esempi di IoC**:

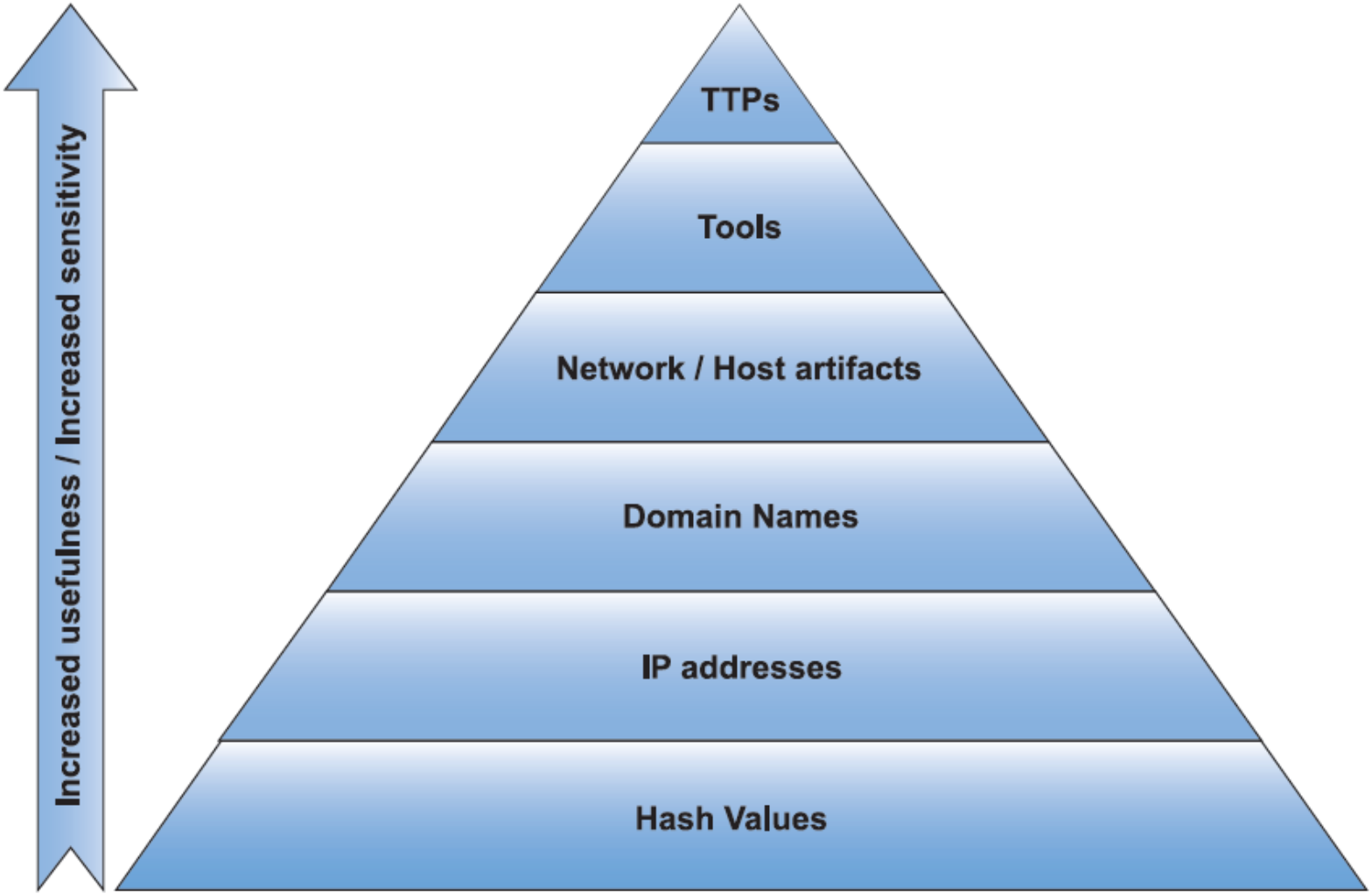
- IP e URL (compromessi o di reputazione scadente)
- Hash (di sample, malware ecc)
- Parti di Windows Registry
- File
- Associazioni porte e applicazioni anomale
- Traffico anomalo (es: DNS malformato)
- .....

INDICATOR of COMPROMISE

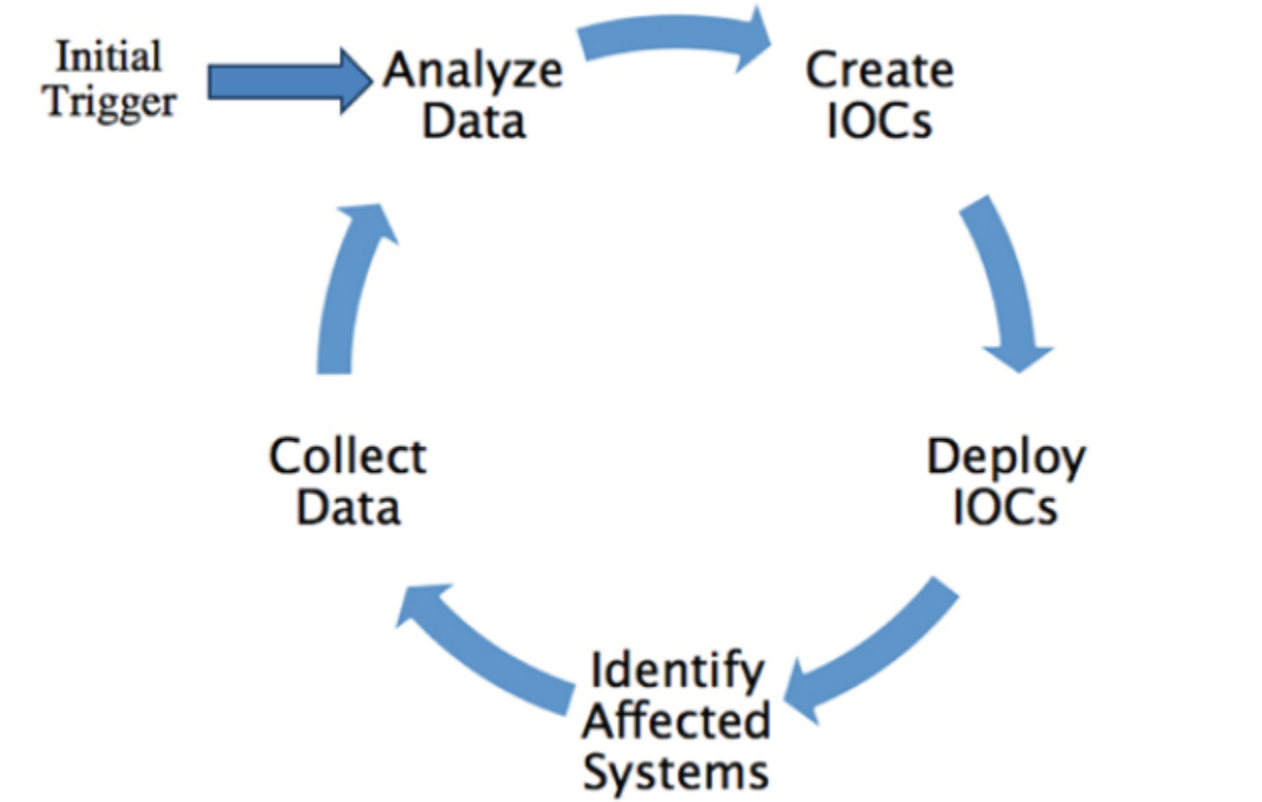
- Ma possono essere creati anche IoC “comportamentali”, ovvero **anomalie**:
  - Nel traffico di rete
  - Nell‘attività di accesso ai sistemi
  - Uso di credenziali privilegiate
  - Risposte anomale a interrogazioni HTML (esempio dopo una SQL injection)

SINERGY

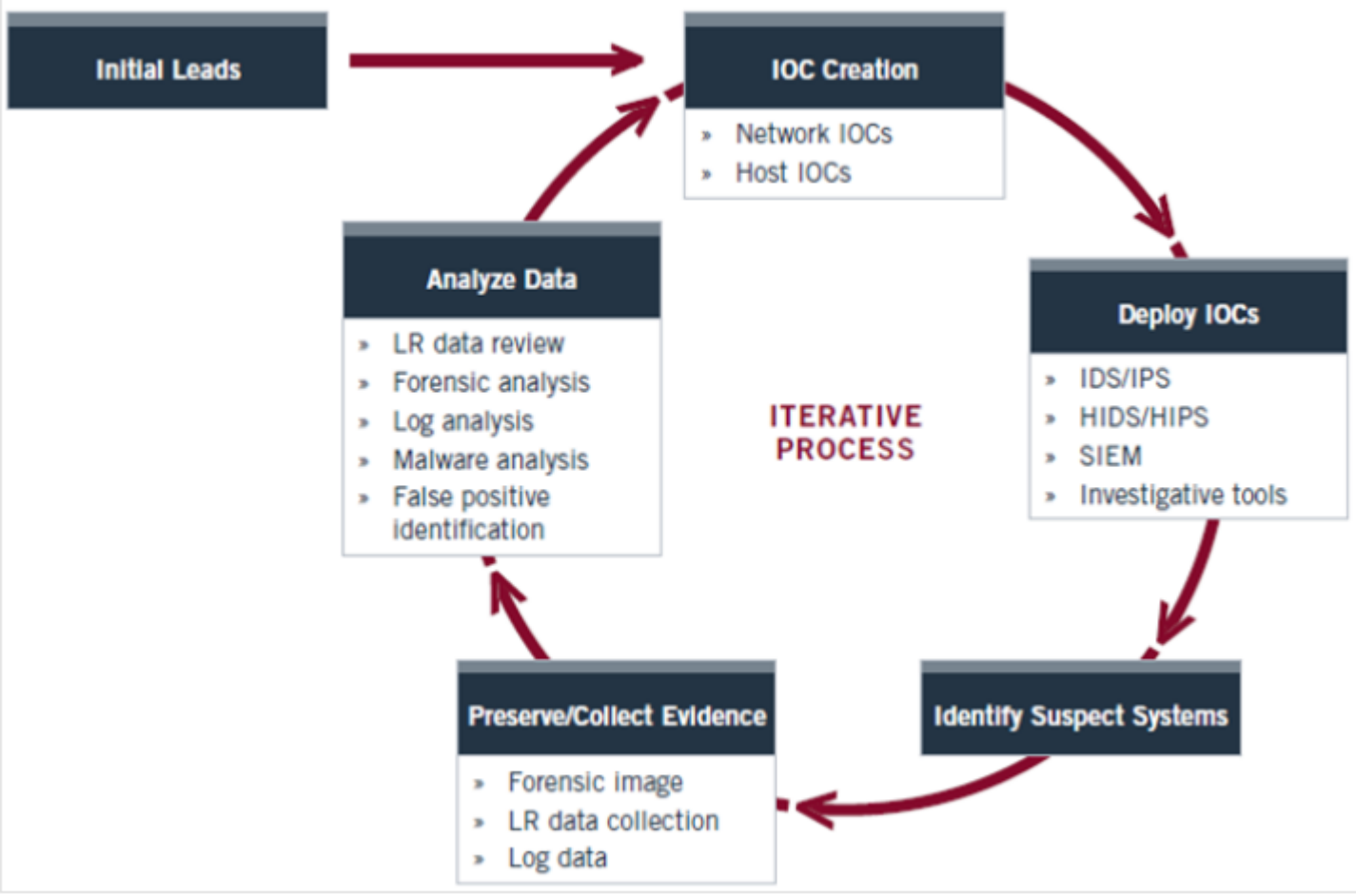
INDICATOR of COMPROMISE



INDICATOR of COMPROMISE LIFECYCLE



OpenIoC LIFECYCLE



Ed è sempre più importante la CONDIVISIONE delle informazioni !!!

IoC QUALITY

- **Creare un IoC è semplice , ma deve essere un elemento EFFICACE ed EFFICENTE per l'analista:**

1. Lo IoC deve essere Specifico (indicare una modalità precisa di attacco/compromissione)

2. Al tempo stesso deve raccogliere abbastanza informazioni da rendere complesso per l'attaccante evadere l'IoC individuato

3. Facile da elaborare e manipolare

IoC MANAGEMENT

- CREARE IoC: Facile
- CATEGORIZZARLI: Complesso
- UTILIZZARLI: Moderatamente Complesso
- CONDIVIDERLI: Complesso

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

IoC MANAGEMENT

- **Standard proposti per IoC**: OpenIoC, STIX, CybOX, RFC ...
- **Distribuzione degli IoC**: protocollo TAXII
- Tool per gestire/distribuire IoC

IoC : Standard?

- *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, MAEC, ...

OpenIoC

OpenIoC è un framework (un XML Schema, estendibile)

•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

Openloc Tool

File Search Tools Help

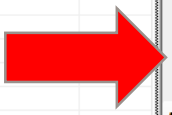
Name	Created	Updated	Source
Trojan.Malwerewolf.B	2014-10-11 23:29:15Z	2014-11-30 04:14:26Z	InterDimS

Name: Trojan.Malwerewolf.B
Author: InterDimSham
GUID: 1ffd7770-1da2-4447-b72a-41c026041a07
Created: 2014-10-11 23:29:15Z
Modified: 2014-11-30 04:14:26Z

Type	Reference
group	Intel.Feed.A
threatgroup	APT-MWW
report	1
category	Backdoor
grade	8

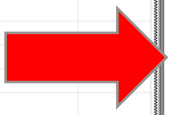
Description:

A report from A Intel Feed described APT group APT-MWW using a trojan backdoor that is being identified as Trojan.Malwerewolf.B.
Since this is an APT actor using custom malwere we have put a risk factor of 8.
The ticket tying all our internal details is in ticket #1.



Add: AND OR Item

- OR
  - File MD5 is d41d8cd98f00b204e9800998ecf8427e
  - File MD5 is d41d8cd98f00b204e9800998ecf8427e
  - Port Remote IP contains 127.0.0.1
  - UrlHistory URL contains remote.localhost:8080/mww/c2?
  - Network DNS contains remote.localhost
  - AND
    - OR
      - File Path contains \AppData\Local\Temp
      - File Path contains \Local Settings\Temp
    - OR
      - File Name is FILE1.exe
      - File Name is FILE2.exe
  - AND
    - Registry Key Path contains Software\Microsoft\Windows\CurrentVersion\Run
    - Registry Value contains FILE1.exe
  - AND
    - Registry Key Path contains Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
    - Registry Value contains FILE2.exe



Comment	
Comment	
Content	
ContentType	string
Content	**FILE2.exe**
Length	9
Context	
Document	RegistryItem
Search	RegistryItem/Value
ContextType	mir
Indicator Item	
ID	36838b1a-5b2a-4e2b-9357-573
Condition	contains

ID
Unique ID of the Indicator Item.

Save

Loaded IOCs: 1

ESEMPIO

Openloc Tool

File Search Tools Help

Name	Created	Updated
Chewbacca Tor Banking Trojan	2014-01-07 22:26:15Z	2014-01-07 22:4
Cryptowall 1.0 and 2.0	2014-12-04 09:31:06Z	2014-12-04 10:5
Flamer,Skywiper	2012-06-04 15:15:17Z	2012-06-04 21:3
Operation Windigo	2014-03-18 20:23:23Z	2014-03-21 15:5
STUXNET VIRUS (METHODOLOGY)	0001-01-01 00:00:00Z	2011-11-04 19:3
Zeus	0001-01-01 00:00:00Z	2011-10-28 19:2

Name: Operation Windigo

Author: David Westcott

GUID: ec3b97c8-5de7-444d-9bd9-8f868ca04748

Created: 2014-03-18 20:23:23Z

Modified: 2014-03-21 15:58:14Z

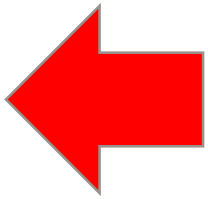
T.. R..

Description:

IOCs for Operation Windigo as described in the following report: http://www.welivesecurity.com/wp-content/uploads/2014/03/operation_windigo.pdf. Source: https://github.com/eset/malware-ioc

Add: AND OR Item

- OR
  - Network String URI contains k2l8z1yeodm.info
  - Network String URI contains o5o8c1berdn.net
  - Network String URI contains map9u1tejdt.net
  - Network String URI contains o5tac1berdn.biz
  - Network String URI contains k2zbz1yeodm.info
  - Network String URI contains a1hcy1xendd.net
  - Network String URI contains k2rdz1yeodm.biz
  - Network String URI contains o5dec1berdn.info
  - Network String URI contains maefu1tejdt.net
  - Network String URI contains a1z1h2xendd.biz
  - Network String URI contains mae2d2tejdt.info
  - Network String URI contains o5e4l2berdn.net
  - Network String URI contains k2t6i2yeodm.biz
  - Network String URI contains a1k8h2xendd.info
  - Network String URI contains k2qai2yeodm.net
  - Network String URI contains o5lcl2berdn.biz
  - Network String URI contains maved2tejdt.info
  - Network String URI contains q5ncv0dekcm8a1p.biz
  - Network String URI contains oaxey7m0lde8s1v.info
  - Network String URI contains c1b1jfi2pdi8w1f.net
  - Network String URI contains oap3p6f5lde8s1v.biz
  - Network String URI contains q5y6vdf7tdm8a1p.info

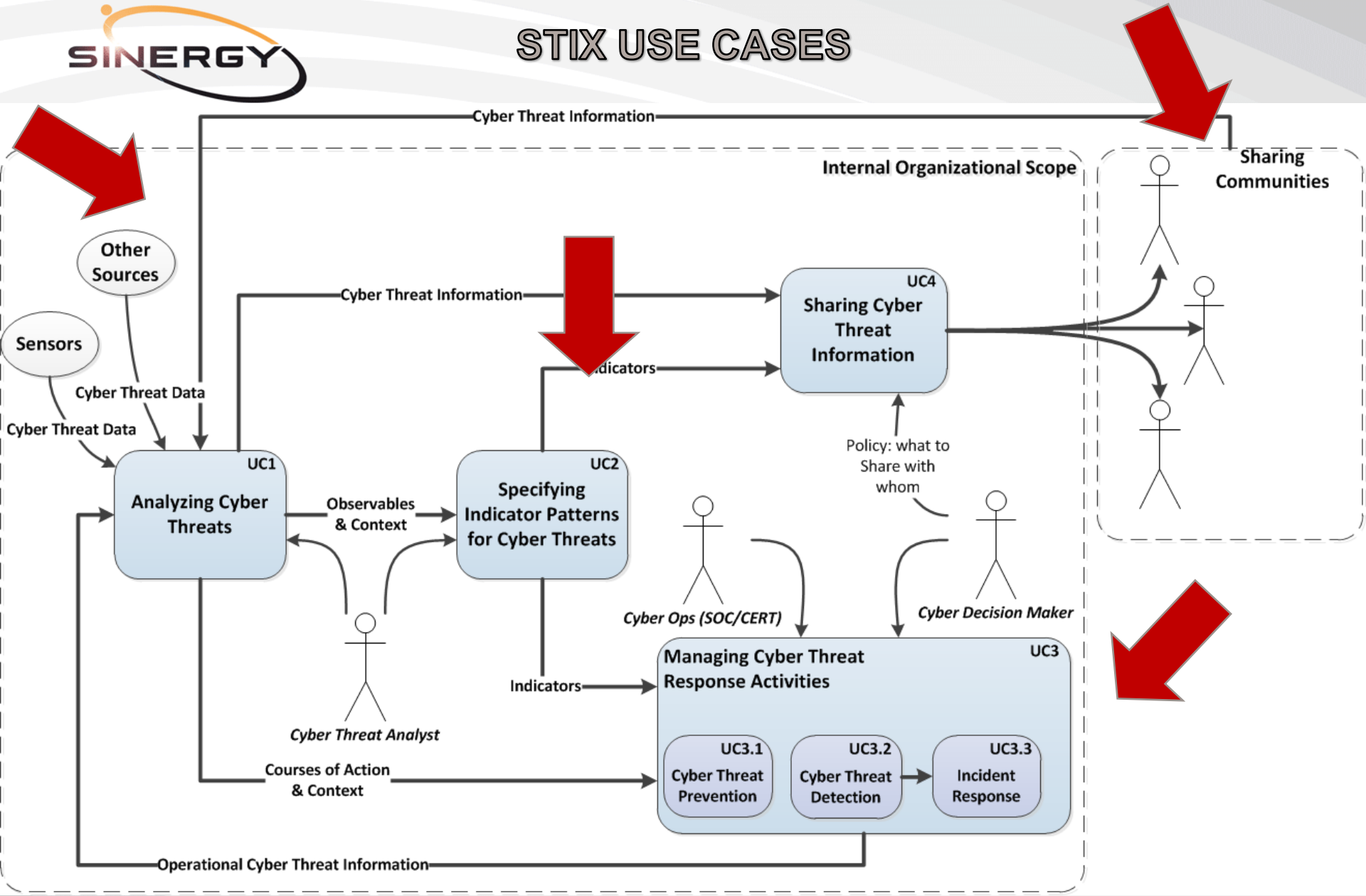


Save

STIX

- Structured Threat Information eXpression (STIX™)
- E’ un linguaggio ed un framework (XML Schema)
- Pensato per gestire le informazioni relative alle CyberThreats per i più comuni c*asi 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 CASES



TAXII

- Trusted Automated eXchange of Indicator Information (TAXII™)

- Originariamente lanciato da Homeland Security, con le seguenti specifiche:

  - 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

  - Informali:
    - https://www.iocbucket.com/
    - …

  - Formali:
    - OTX – Open Threat Exchange (OSSIM)
    - 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

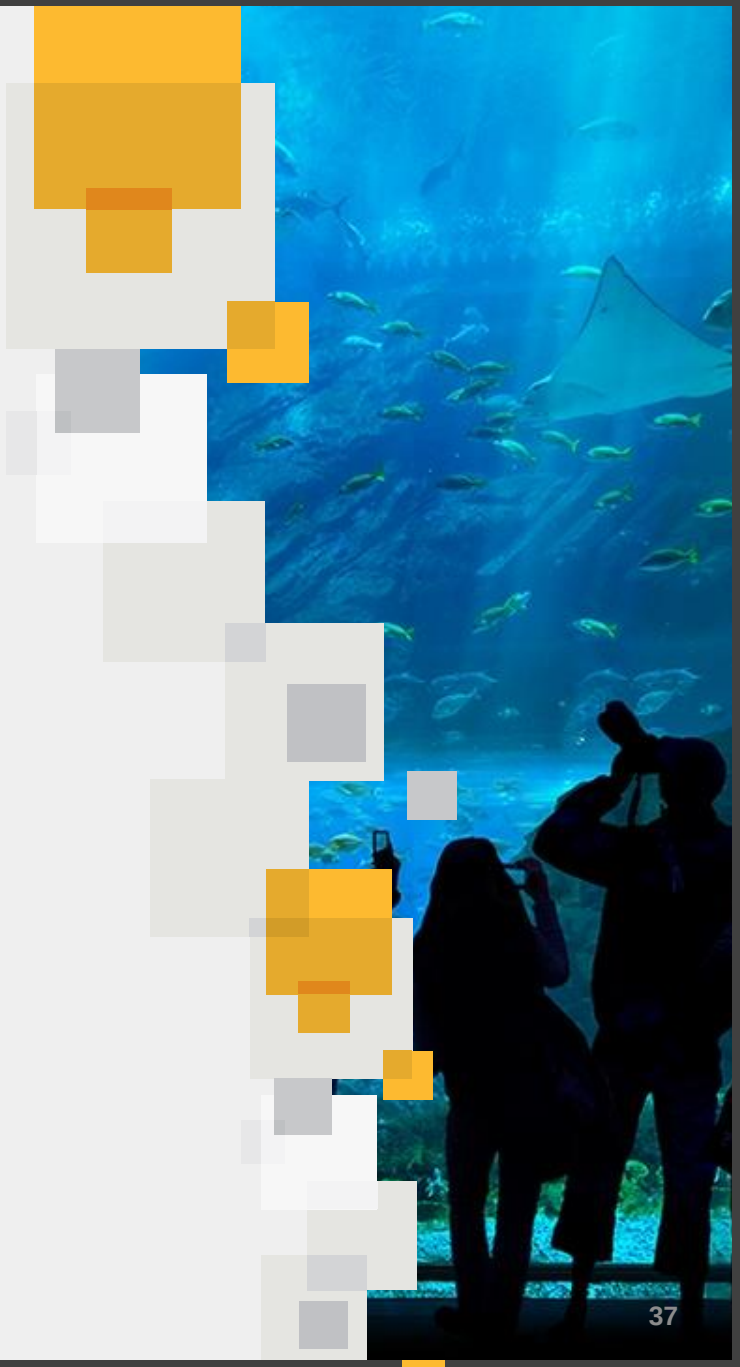
Gabriele Zanoni

EMEA Incident Response Investigator
Symantec Cyber Security Services

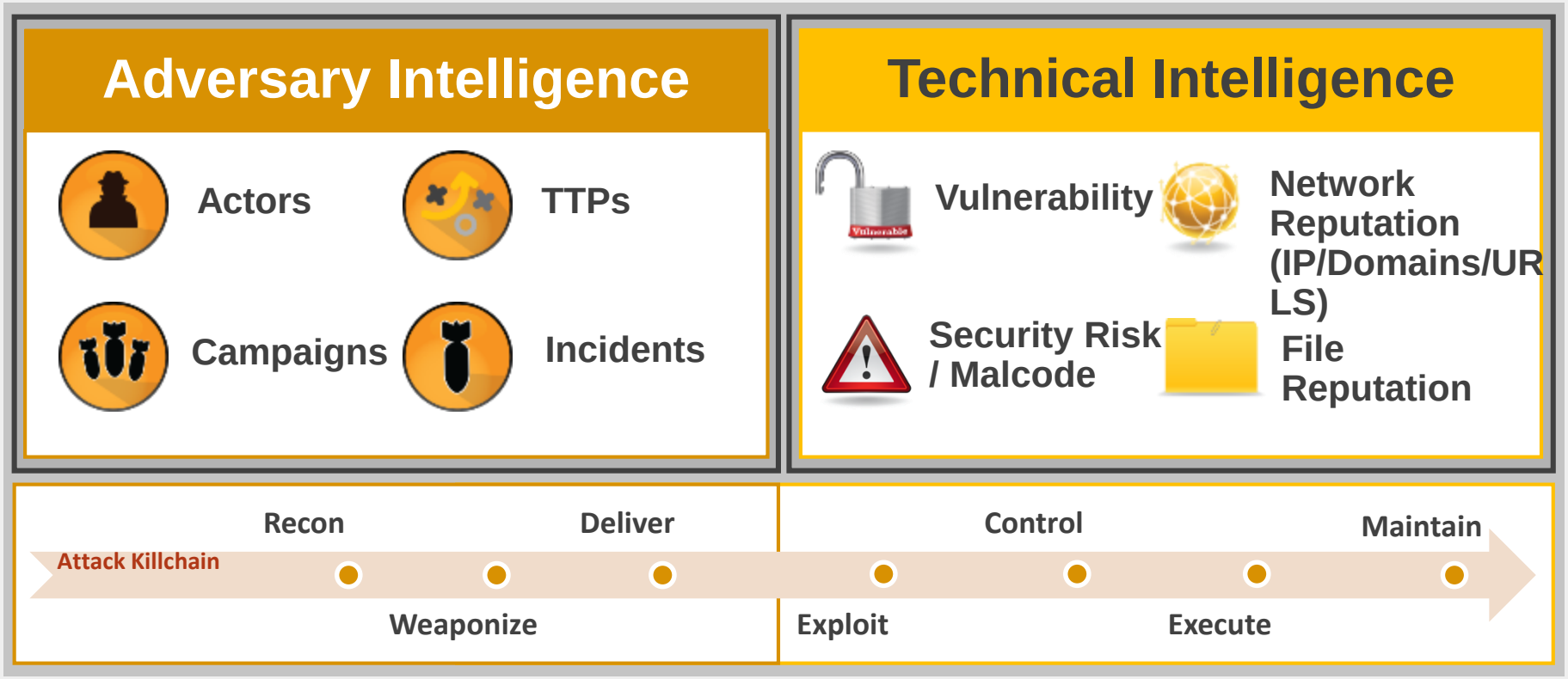
Index

1	Technical and Adversary Intelligence
2	IoC usage in a MSS provider
3	IoC and Incident Response

Technical and Adversary Intelligence

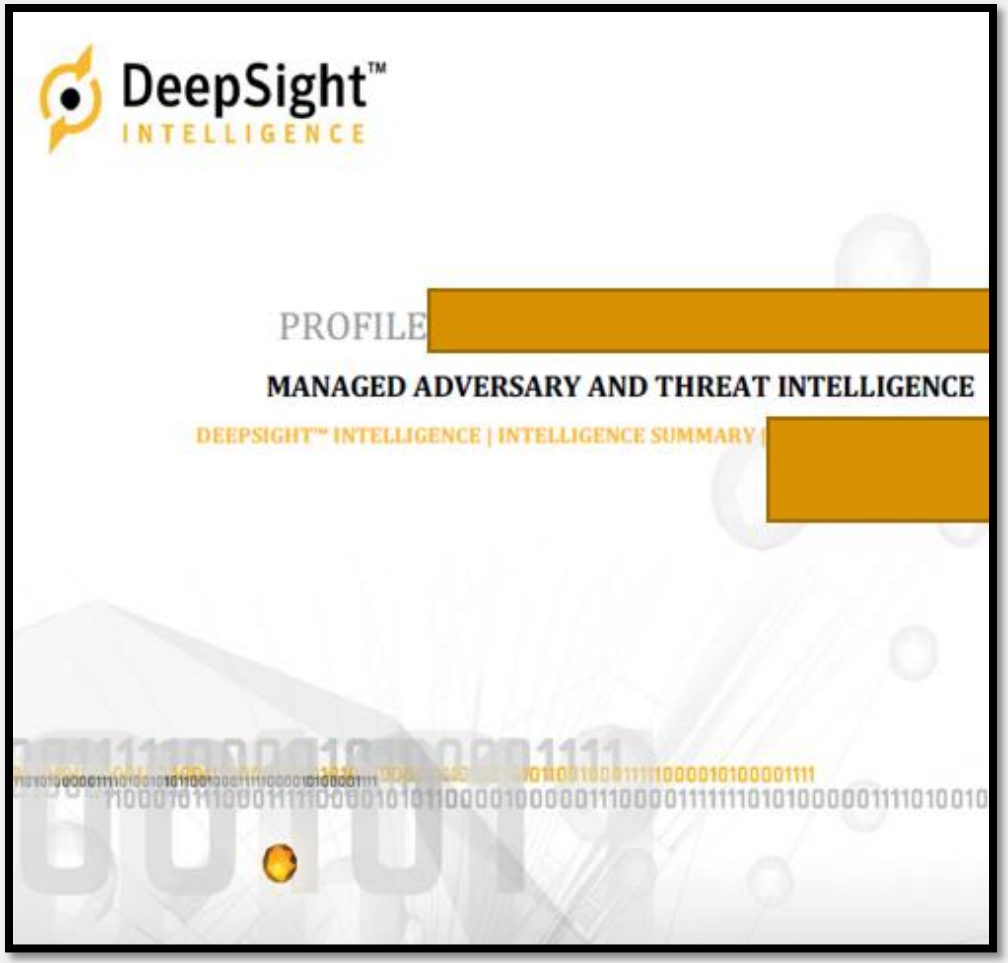


Intelligence Has to Evolve



Outside your perimeter *Inside your perimeter*

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

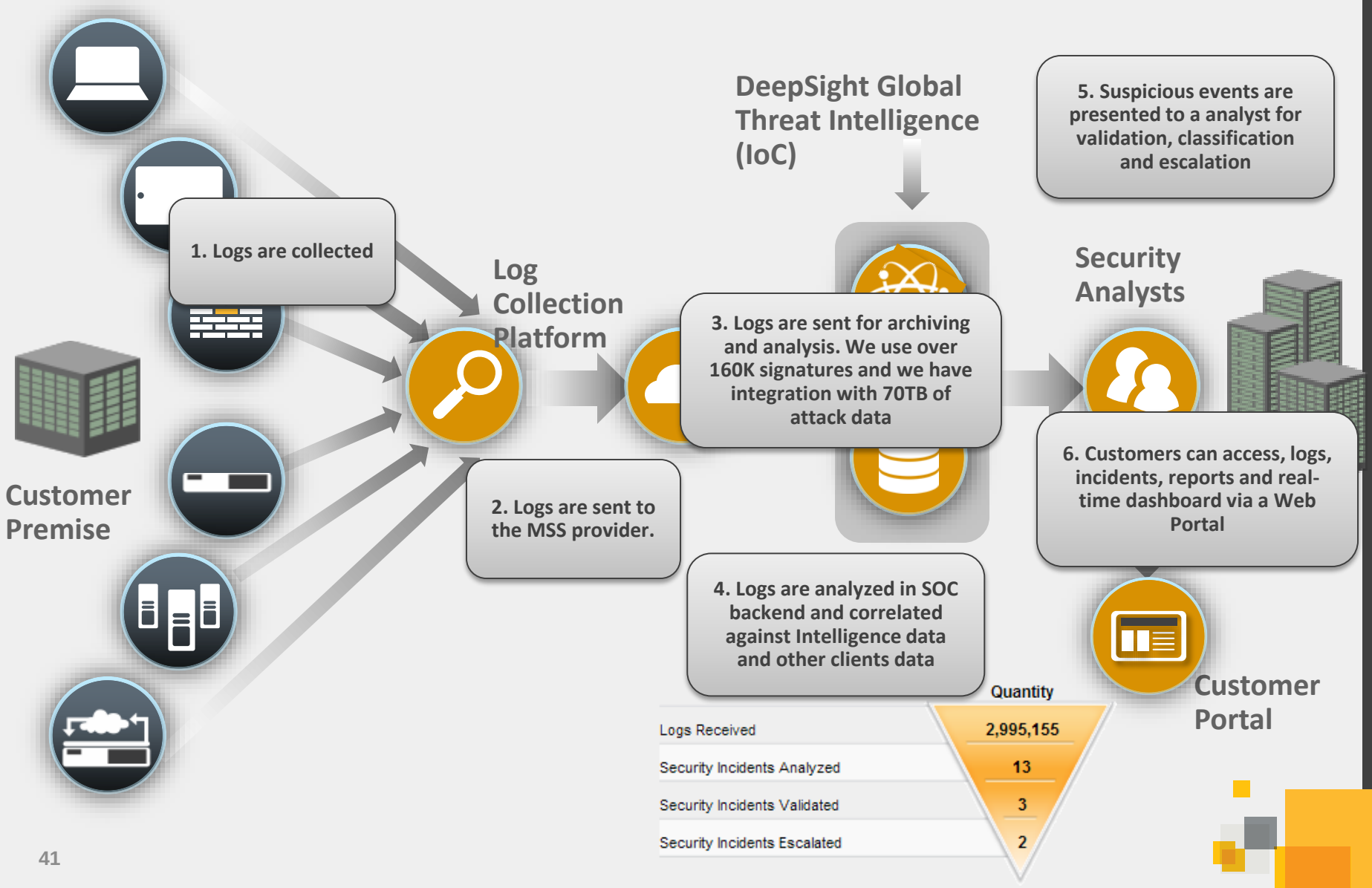


Examples of information provided:

- 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..

IoC usage in a MSS provider

IoC usage inside a Managed Security Service provider

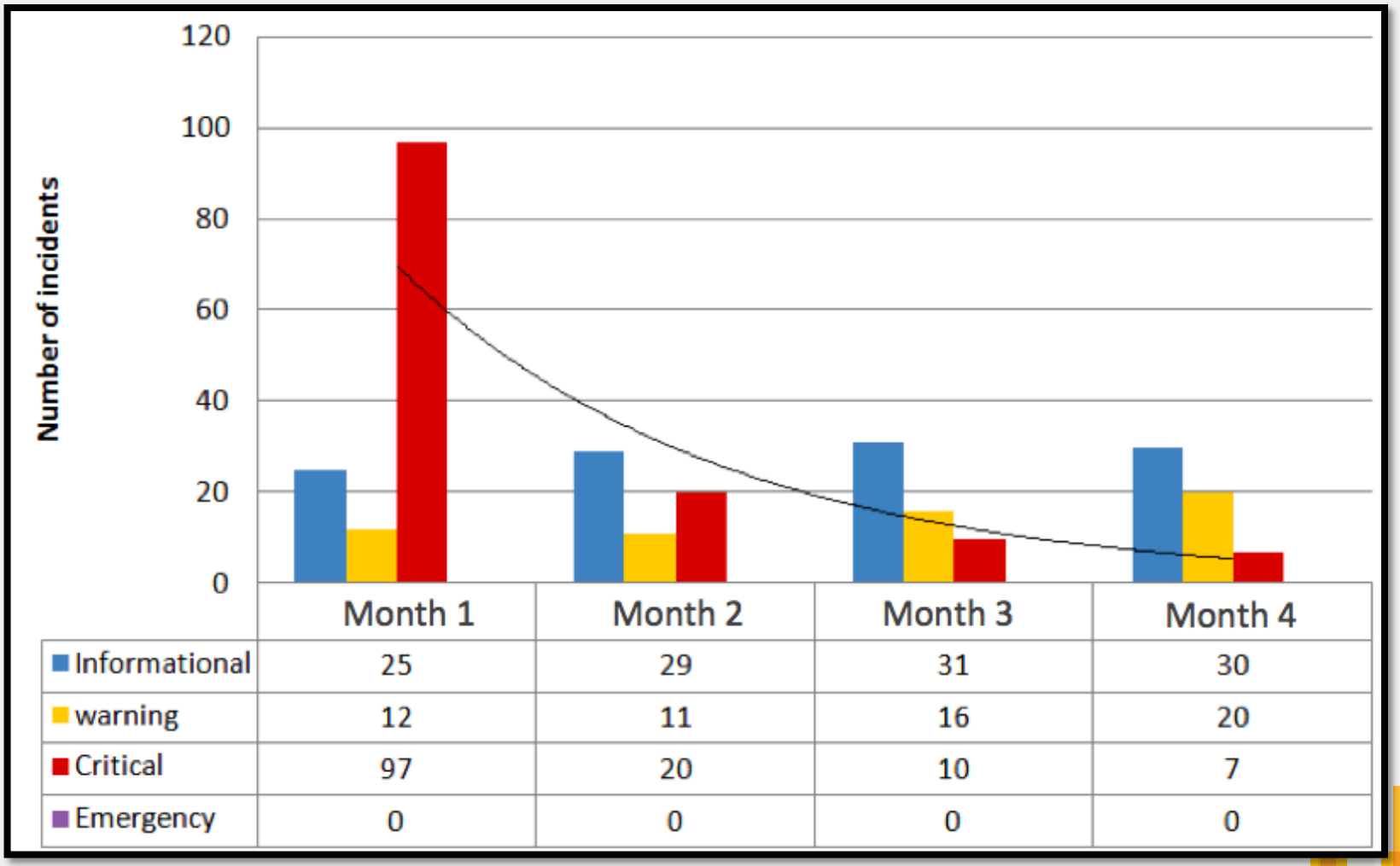


Correlation activities inside MSS

- 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.

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

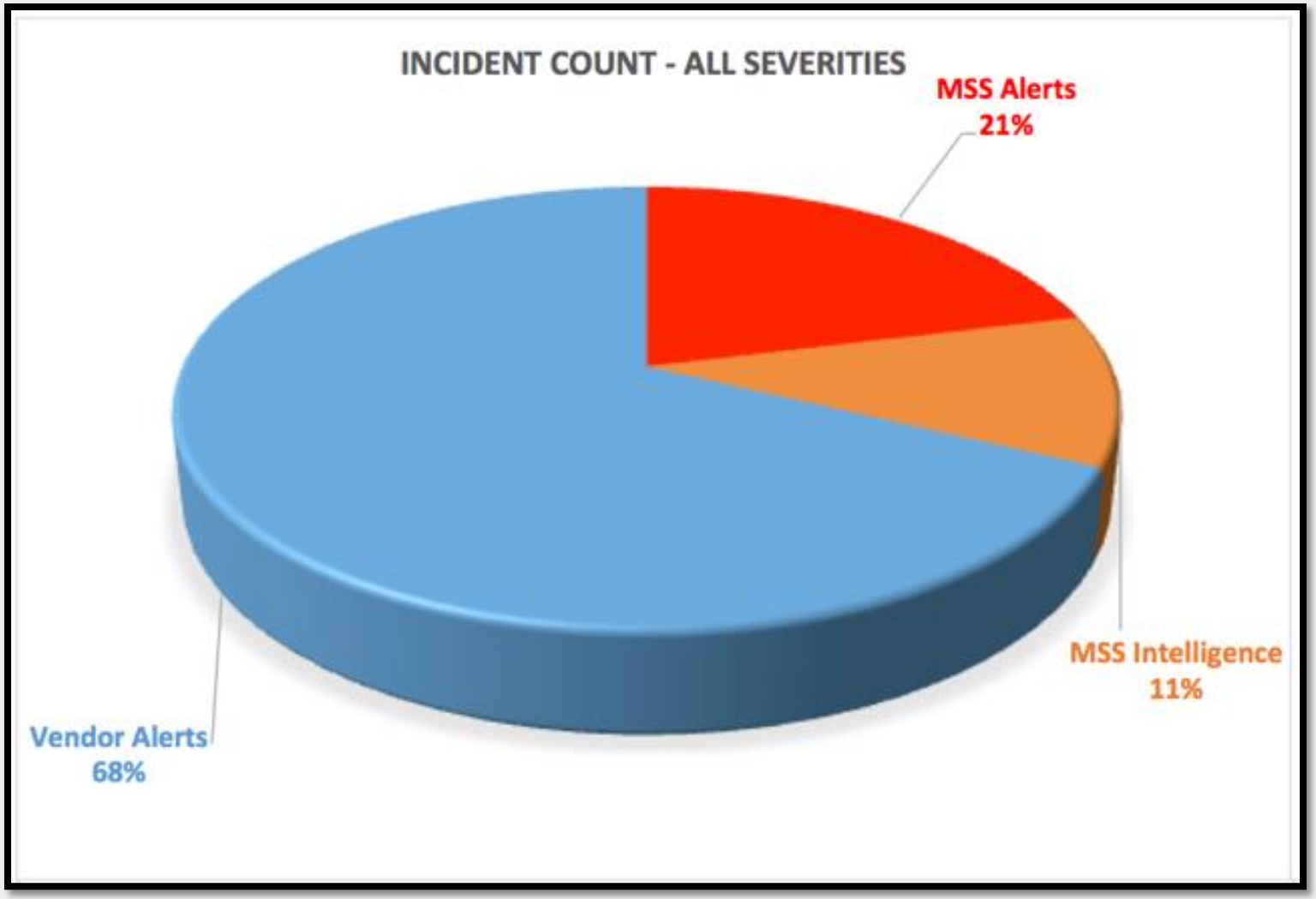
Security Incidents per Month



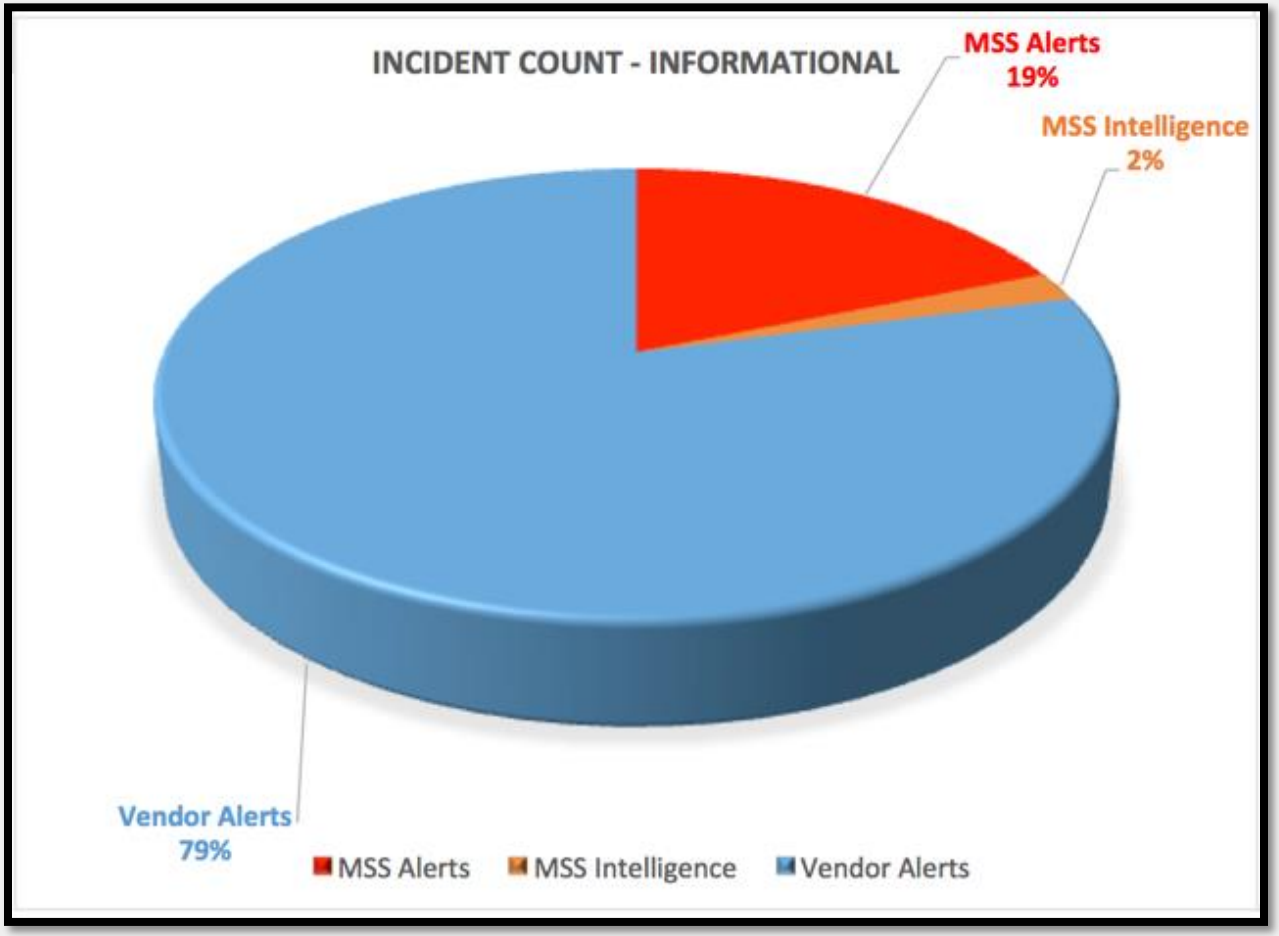
	Month 1	Month 2	Month 3	Month 4
Informational	25	29	31	30
warning	12	11	16	20
Critical	97	20	10	7
Emergency	0	0	0	0

43

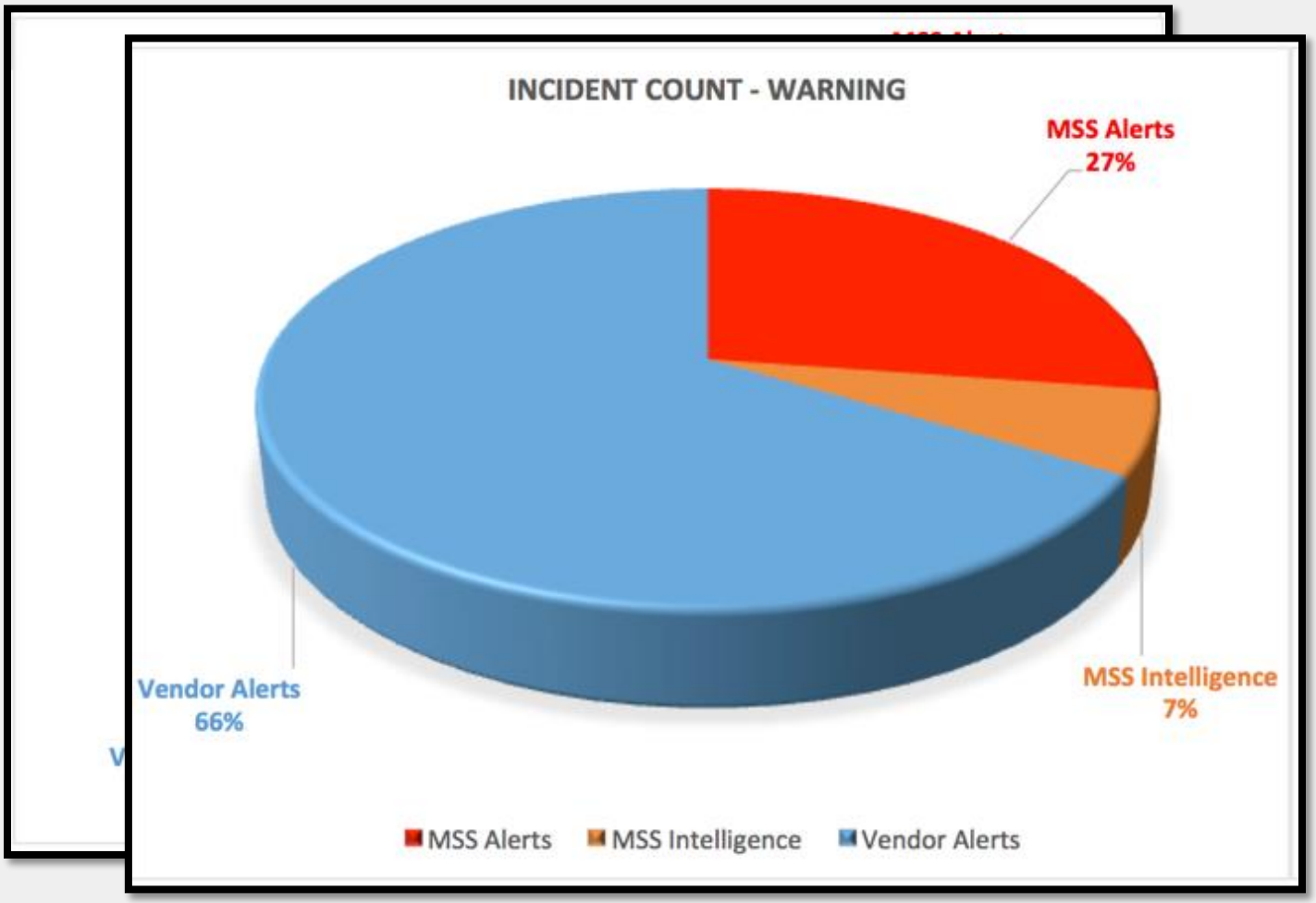
During Feb. 2016 MSS detected ~30K Incidents just for EMEA customers



Drill down

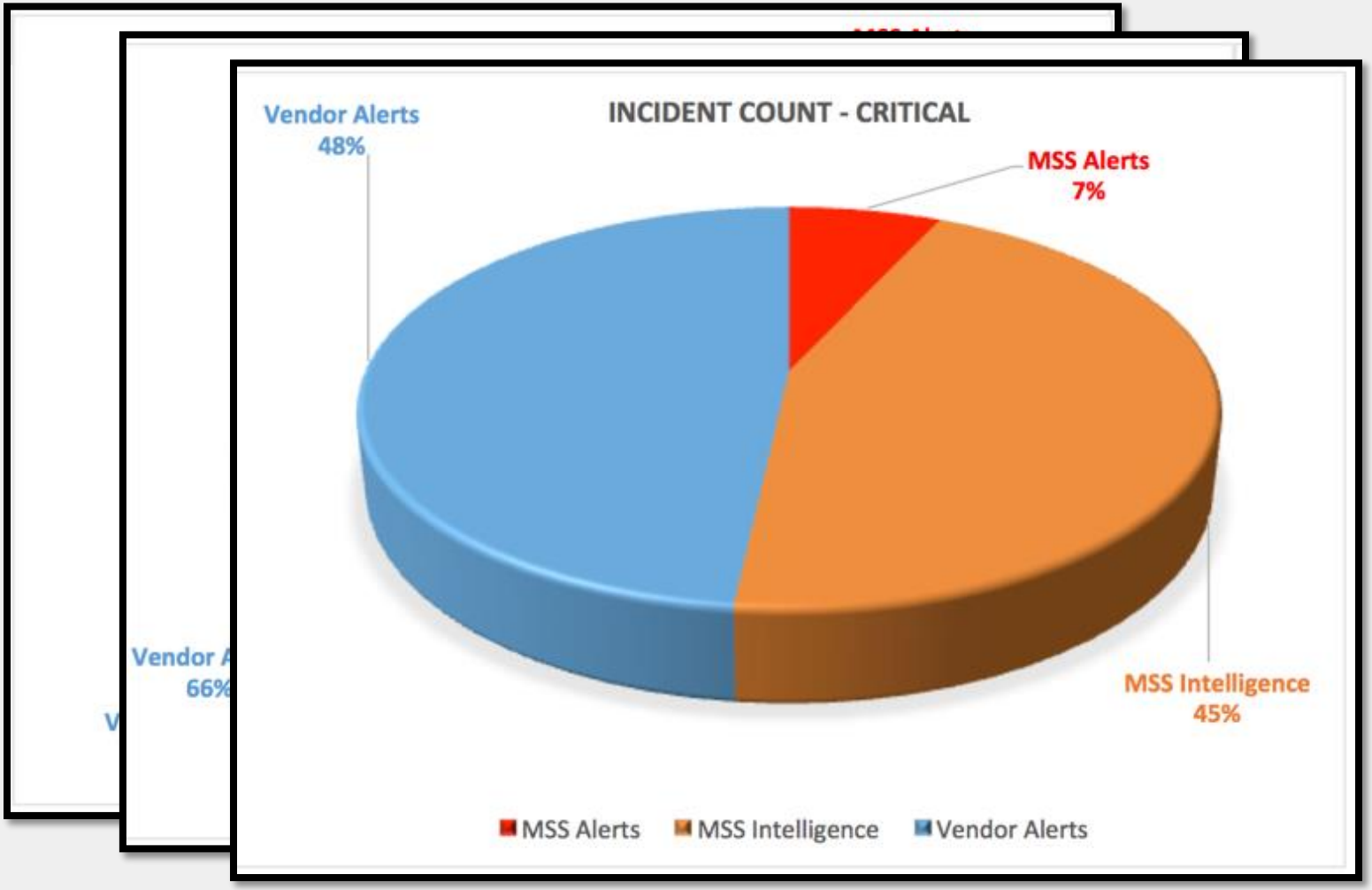


Drill down

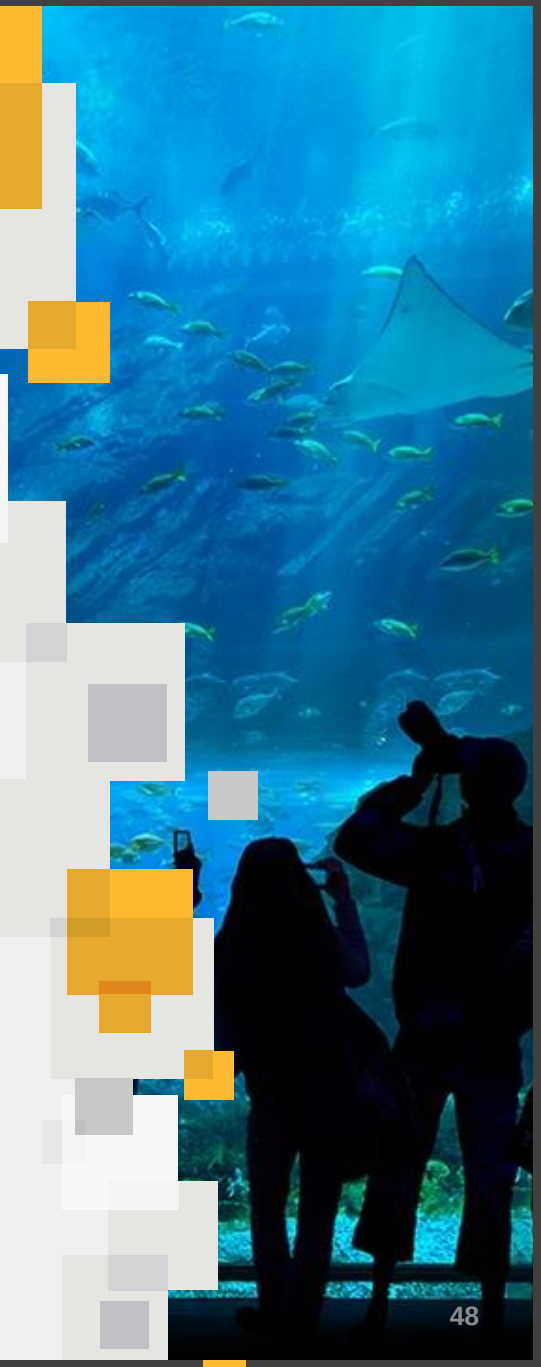


Drill down

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



IoC and Incident Response



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..).

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.

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

Thank you!

Gabriele_Zanoni@symantec.com

EMEA Incident Response Investigator
Symantec Cyber Security Services

Indicators of Compromise per la Cyber Threat Intelligence e l'Incident Response

Roberto Leone, Senior Advisor Sinergy,
r.leone@sinergy.it
www.sinergy.it