London, 20 March 2019 – FIRST CTI Symposium

Metrics and ATT&CK™

Or how I failed to measure everything.

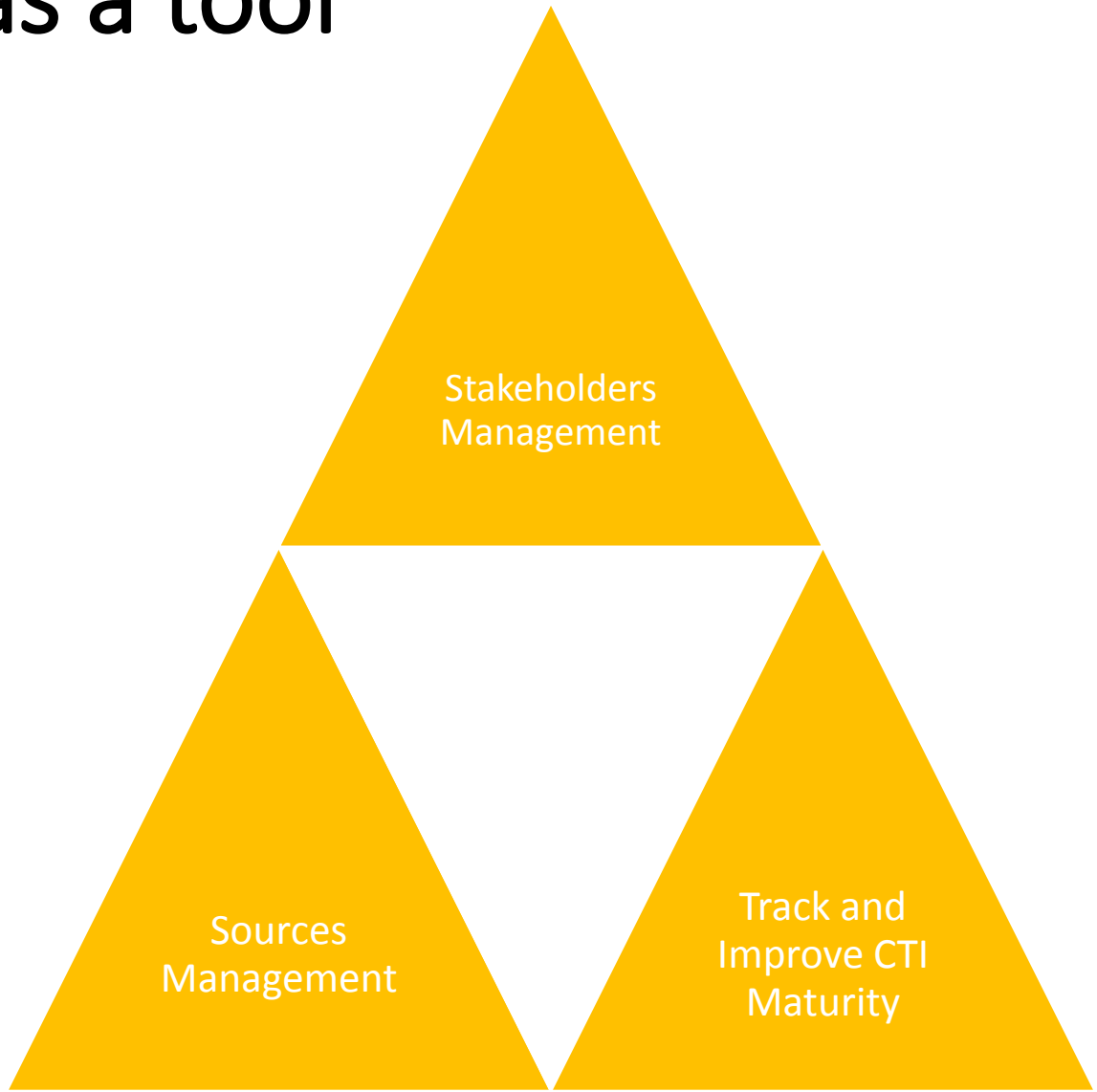
Introduction

Who?

Francesco Bigarella, Intelligence analyst @ ING Bank

1. IoC != intelligence
2. Small overhead for the analyst
3. Better insights
4. One standard framework

ATT&CK™ as a tool



Why ATT&CK™

- Metrics generation
- Standardisation and alignment
- Common language
- Derive new requirements
- Source quality and gaps
- Prioritization and focus

Limitations

- Not always a good fit
- Information loss at requirement mapping
- Limited coverage
- All Techniques are equal

Key to successful integration

- Stakeholder management
- Requirements setting + process
- Understanding your environment and assets
- Valuable intelligence sources
- Mapping to ATT&CK

Easy Right?

Identify the Stakeholders

CISO

Bank being compromised

What she said

Get a foothold within the bank perimeter

What she meant

Initial access

Mapped to ATT&CK

T1193 -> T1

Incident Responder

T1 – T7 – T3

SOC Analyst

T1 – T3 – T9

Spearphishing Attachment

METRIC

T1	T3	T2	T6	T7	T9	= Technique as req.
3	2	1	1	1	1	= Requirements priority

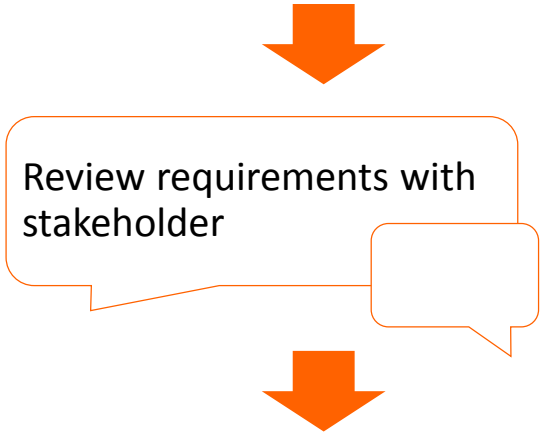
Requirements mapping

I'm interested in ways to compromise payment systems

Daruk,
Payments team

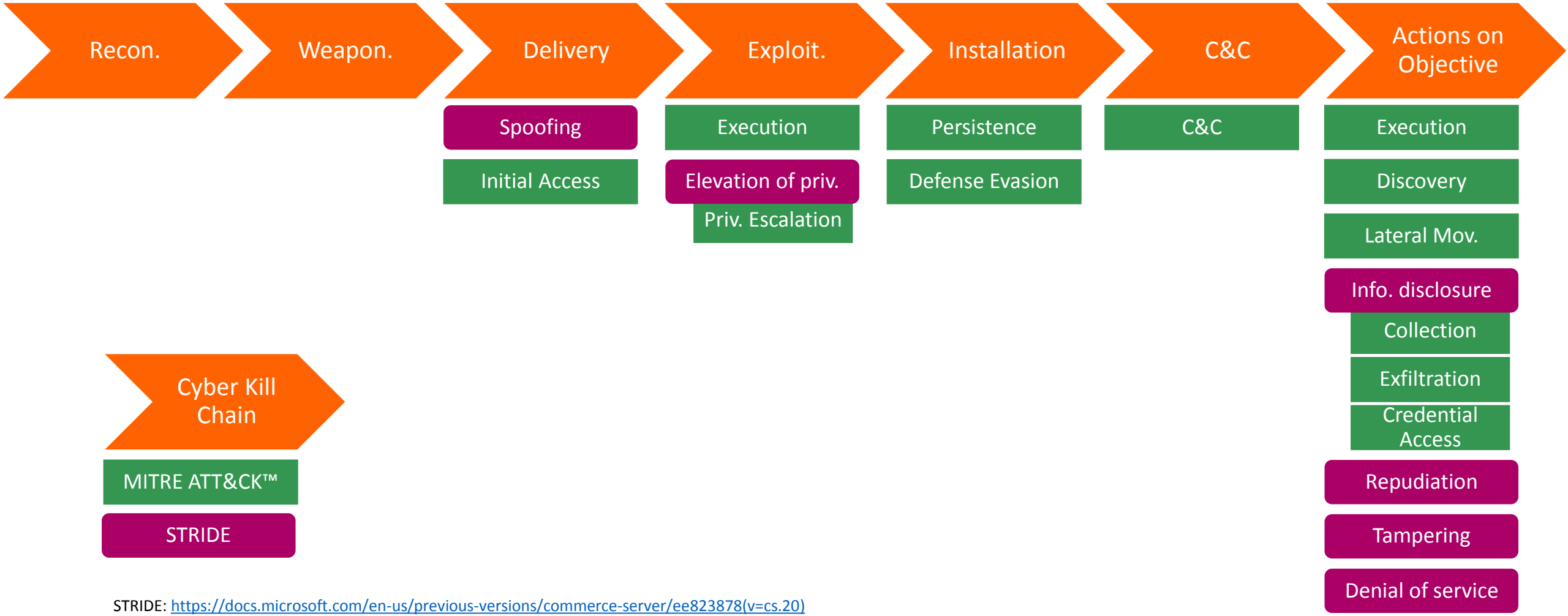
Initial Access (TA0001)
-

+ "payments"



Priv. Escalation (TA0004)	Credential Access (TA0006)	Collection (TA0009)
Valid Accounts (T1078)	Bash History (T1072)	Input Capture (T1056)

Mapping to the other frameworks



STRIDE: https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)
Cyber Kill Chain: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

ATT&CK™ Fraud extension

Initiation	Target Compromise	Perform Fraud	Obtain Fraudulent Assets	Assets Transfer	Monetization
Phishing	Malware	Insider Trading	Compromised payment cards	SWIFT transaction	ATM jackpotting
Spear Phishing	Account-Checking Services	Business Email Compromise	Compromised account credentials	Fund Transfer	Money Mules
Vishing	ATM Black Box Attack	Scam	Compromised Personally Identifiable Information (PII)	Cryptocurrency exchange	Fund Transfer
Social Media Scams		CxO Fraud	Compromised Intellectual Property (IP)		Prepaid Cards
Smishing					Resell Stolen Data
ATM Skimming					ATM Explosive Attack
ATM Shimming					
POS Skimming					

Extending ATT&CK™

- Only when malicious
- Pragmatic approach
- Get the experts

First attempt at https://github.com/burritoblue/attck4fraud

Requirements mapping with ATT&CK™

ATT&CK techniques are limited

SOLUTION	Get creative. Combine. Extend
LONG-TERM SOLUTION	Document and engage MITRE/community

The Threat Actors

Actor Alpha

T2 – T4 – T10 – T12

Actor Beta

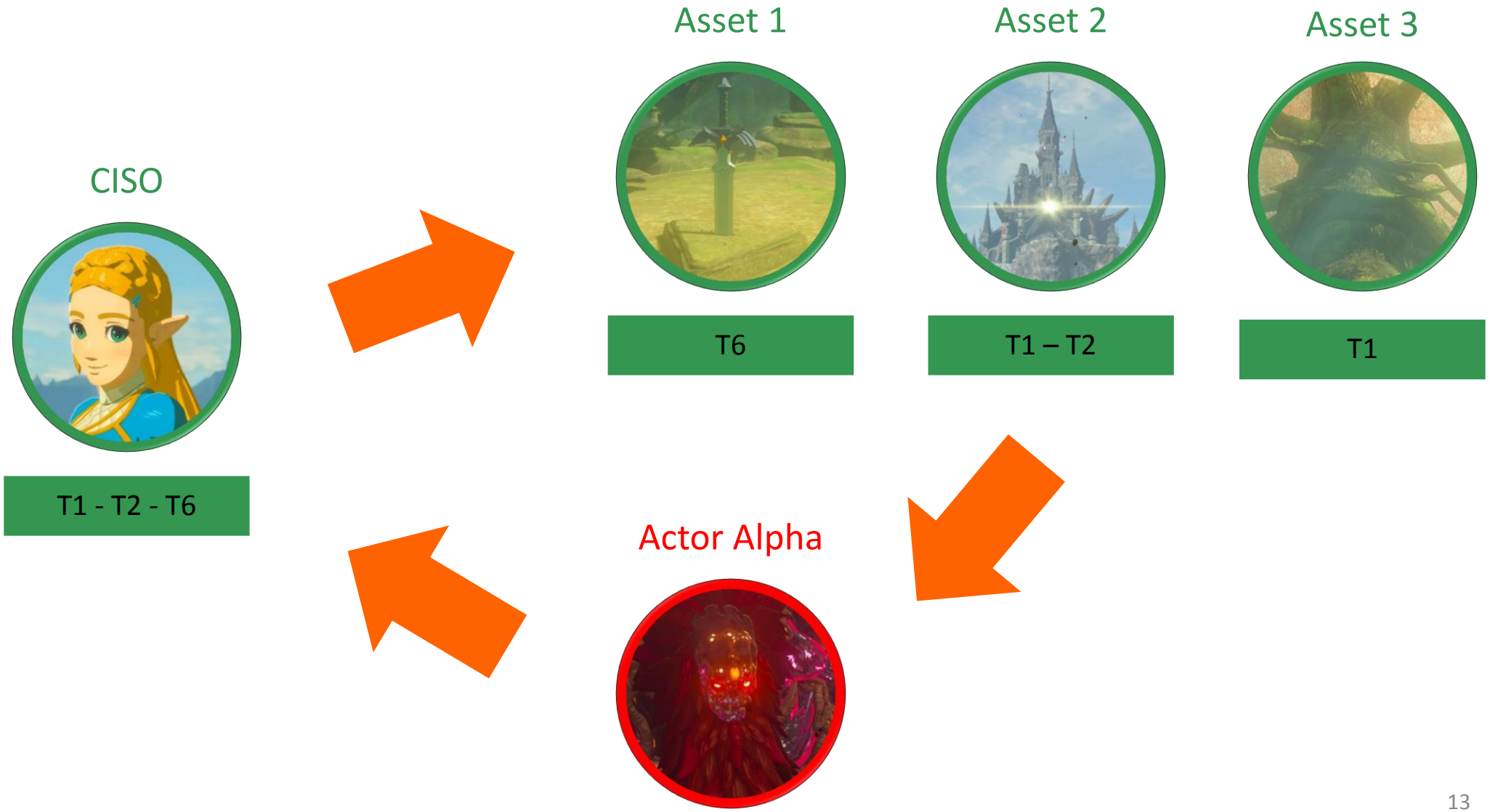
T3 – T7 – T12 – T14

Initial Access 10 Items	Execution 33 Items	Persistence 58 Items	Privilege Escalation 28 Items	Defense Evasion 63 Items	Credential Access 19 Items	Discovery 20 Items	Lateral Movement 17 Items	Collection 13 Items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Removable Media
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data Staged
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser
	Launchctl	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	Shared Webroot	Screen Capture
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Keychain	Remote System Discovery	SSH Hijacking	Video Capture
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content	
	Mshta	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Network Sniffing	System Information Discovery	Third-party Software	
	PowerShell	Dylib Hijacking	Path Interception	DLL Side-Loading	Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares	
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Windows Remote Management	
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery		
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion	Two-Factor Authentication Interception	System Service Discovery		
	Scheduled Task	Hooking	Scheduled Task	File Permissions Modification		System Time Discovery		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File System Logical Offsets				
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	Gatekeeper Bypass				
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	Hidden Files and Directories				
	Signed Script Proxy Execution	Launch Agent	Startup Items	Hidden Users				
	Source	Launch Daemon	Sudo	Hidden Window				
	Space after Filename	Launchctl	Sudo Caching	HISTCONTROL				
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Image File Execution Options Injection				
	Trap	Local Job Scheduling	Web Shell	Indicator Blocking				
	Trusted Developer Utilities	Login Item		Indicator Removal from Tools				
	User Execution	Logon Scripts		Indicator Removal on Host				
	Windows Management Instrumentation	LSASS Driver		Indirect Command Execution				
	Windows Remote Management	Modify Existing Service		Install Root Certificate				
	XSL Script Processing	Netsh Helper DLL		InstallUtil				
		New Service		Launchctl				
		Office Application Startup		LC_MAIN Hijacking				
		Path Interception		Masquerading				
		Plist Modification		Modify Registry				

Organically linked to

Stakeholders
Sources
Products
Mitigations

Levelling up the Stakeholder relation



The Sources and the Products

CISO

T1 - T2 - T6

Source 1

T1 – T4

Source 2

T3 – T6 – T10

Source 3

T5 – T7

OSINT

T2

Closed Group

T9

Landscape

T1 – T4

Flash

T3 – T8

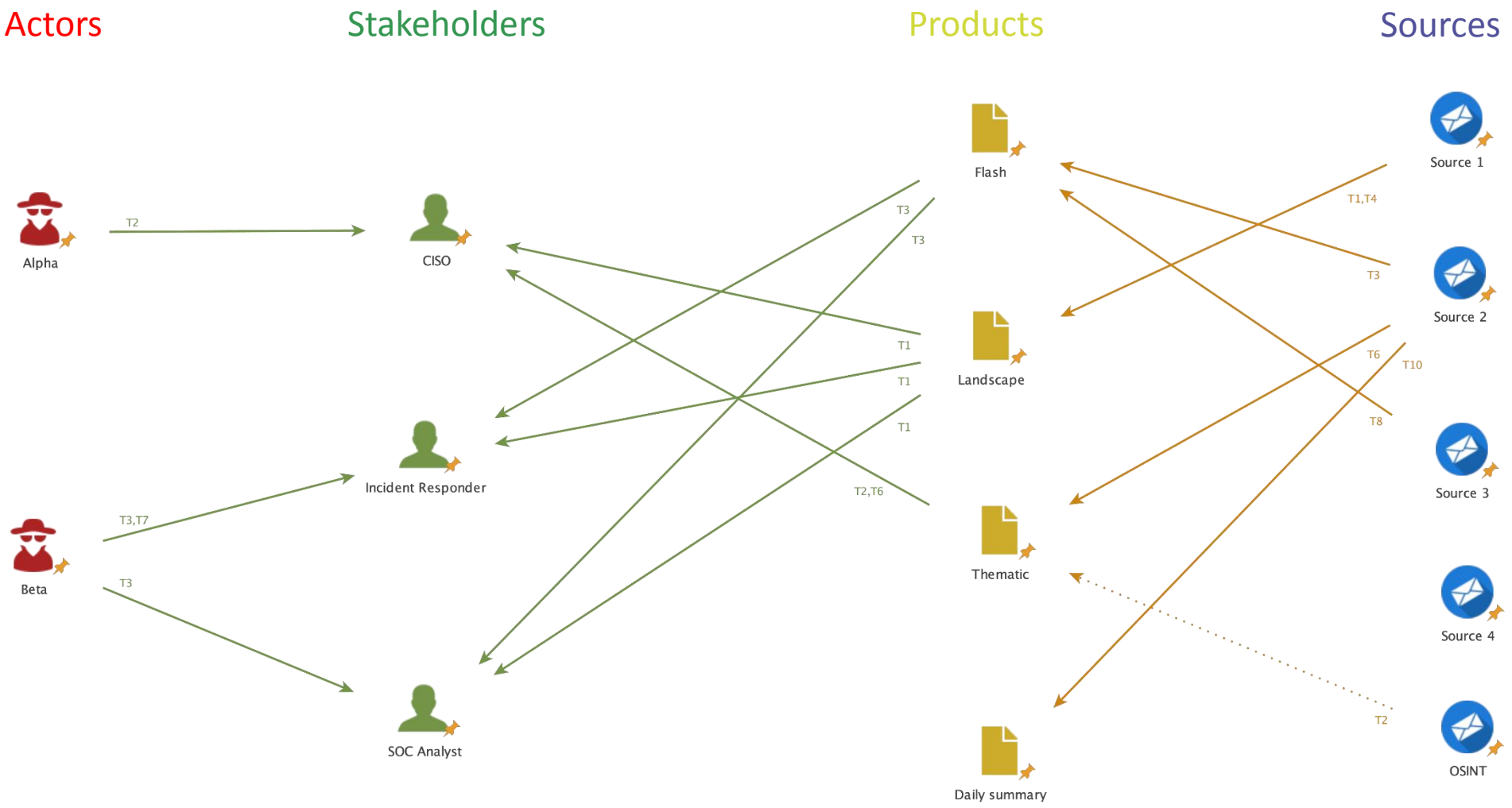
Thematic

T2 – T6

Daily summary

T10

The big picture



Source coverage

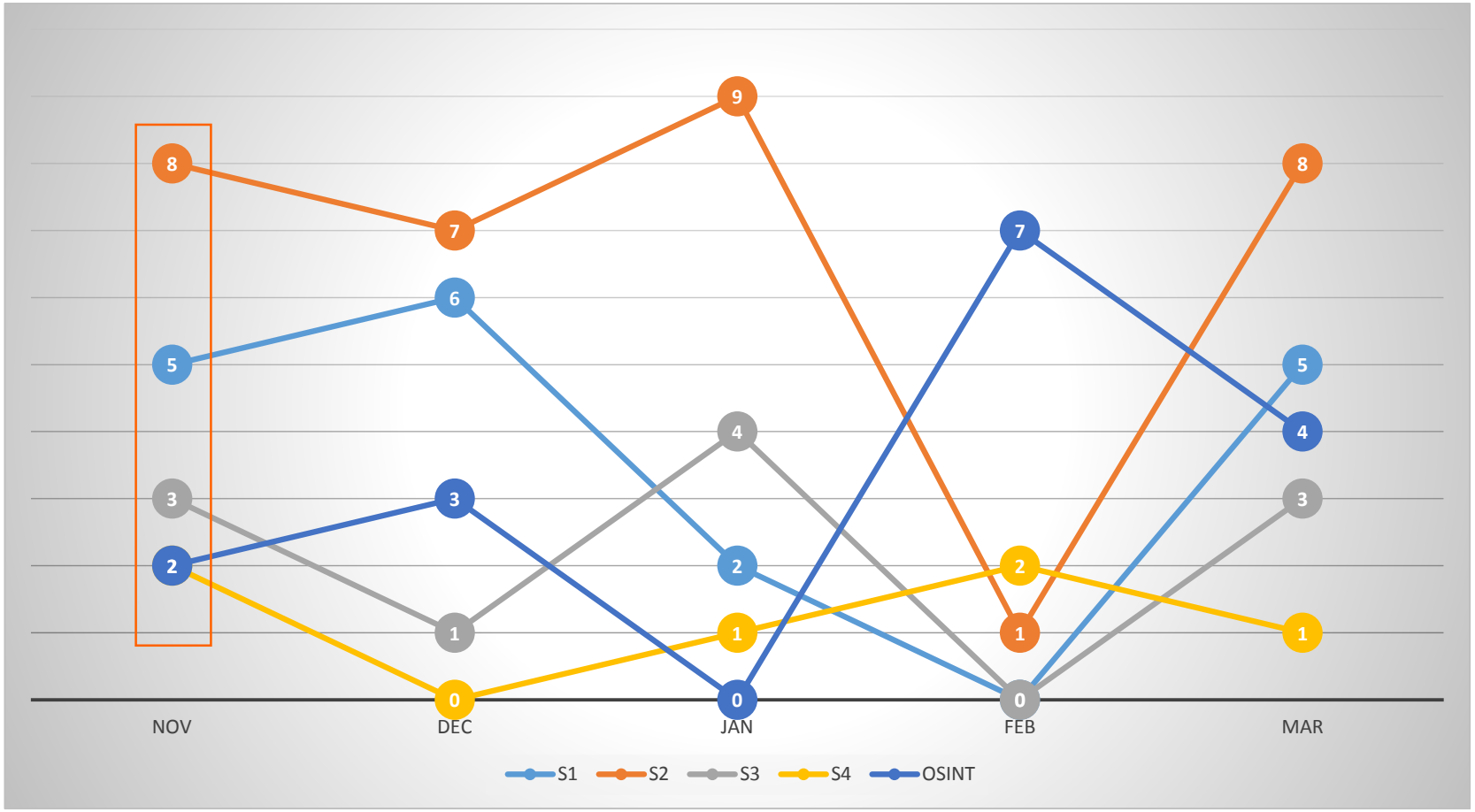
Source	Stakeholder c.	Actor c.	Usage	AVG RFI score (1-10)	Score
S1	3	1	1	9	5 (14)
S2	3	2	3	4	8 (12)
S3	0	2	1	8	3 (11)
S4	1	1	0	6	2 (8)
OSINT	1	0	1	N/A	2

METRIC

Number in brackets include avg RFI score for the source. RFI score represent the opinion of the analyst.

Source value

Overall



Different angle

By Stakeholder Coverage

S2 S1 S4 OS S3

By Actor Coverage

S2 S3 S1 S4 OS

RFI feedback not included; Example data

Product quality

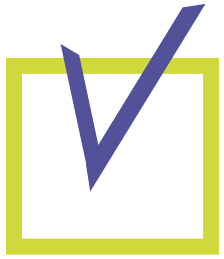
Product	Stakeholder covered	Actor covered	Source used
Flash	1	1	S2, S3
Landscape	3	2	S1
Thematic	3	0	S2, OSINT
Daily summary	0	1	S2

Combine to actual feedback
= **Product quality**

Product	Stakeholder c.	Actor c.	Feedback (1-10)	Score
Flash	1	1	8	**10**

METRIC

Level up the team



Number of technique never covered by a product

METRIC

Number of covered tactics/techniques for an actor

METRIC

Threat = Capability + Intent + **Coverage**


Takeaways

Because metrics matter

Theme	Metric	Implementation complexity	Added value	Audience
Stakeholders	Number of stakeholders on boarded (formally/informally)	low	low	Program sponsor
	Number of intel requirements	medium	medium	Management
	Number of unique intel requirements	medium	medium	Management
	Number of issued products per stakeholder	low	medium	Management
	Number of products within deadline	low	low	Management
	Number of products meeting the initial scope	low	low	Team
	Number of incoming RFI per stakeholder	low	high	Team
	Average score per stakeholder (e.g. success/fail)	medium	high	Program sponsor

Because metrics matter

Theme	Metric	Implementation complexity	Added value	Audience
Products	Number of issued products not linked to a requirement	high	medium	Management
	Number of products issued per requirement	high	high	Management
	Number of requirements without a product	high	high	Management
	Number of issued products per intelligence level (operational, tactical and strategic)	low	medium	Team
	Number of IoC per ATT&CK tactic (via Feed)	high	medium	Team
	Number of IoC per ATT&CK technique (via Feed)	high	medium	Team
	Number of IoC per requirement (via Feed)	high	medium	Team
	Number per issued product type and average score	medium	low	Program sponsor
Intel sources	Number of requirements satisfied by a source	high	medium	Management
	Number of products making use of a source (which sources are used the most)	low	high	Management
	Average score of outgoing RFIs per source	low	high	Management

Because metrics matter

Theme	Metric	Implementation complexity	Added value	Audience
Team	Number of alerts handled	low	low	Management
	Average saving thanks to met requirement	medium	medium	Management
	Average time taken to create a report/product (report cycle - days)	low	low	Team
	Number of actors on the watch list	low	low	Program sponsor
	Number of actors on the watch list per actor sophistication	low	low	Management
	Number of actors on the watch list per actor label	low	low	Management
	Number of incidents/action taken created directly from product	high	high	Program sponsor

Final thoughts

- Use your TIP + reporting
- Clear set of stakeholders' requirements
- Not always a good fit
- Valuable measurable data

Not a silver bullet…but still a bullet!