



# Building an intelligence-driven organization

---

*Anastasios Pingios*

4 May 2020

*FIRST Cyber Threat Intelligence Webinar Series*

**TLP:WHITE**

# Disclaimer.



*All opinions expressed are my own,  
and do not represent my employer.*

**TLP:WHITE**

# About.



- Principal Security Engineer at Booking.com
- Contributor at MITRE ATT&CK framework
- @xorlgr
- SANS GCTI, RecordedFuture Geopolitical Analyst, Bellingcat OSINT, ISS OSINT, ...

# Agenda.



- Definition
- Risk versus threat-based approach
- The 5 phases

# Definition.



# Threat intelligence

TLP:WHITE

# Definition.



# Threat intelligence

- Intent
- Opportunity
- Capability

**TLP:WHITE**

# Definition.



# Threat intelligence

---

- Product
- Process

# Definition.



# Threat intelligence



- Product
- Process

TLP:WHITE



# Definition.



*If you know the enemy and know yourself, you need not fear the result of a hundred battles.*

*Sun Tzu, The Art of War*

**TLP:WHITE**



# Definition.



*If you **know the enemy** and know yourself, you need not fear the result of a hundred battles.*

*Sun Tzu, The Art of War*

TLP:WHITE



# Risk vs threat-based approach.



<u>EXAMPLE</u> RISK		Probability				
		Very High	High	Medium	Low	Very Low
Conse- quence	Very High	Very High	Very High	Very High	High	High
	High	Very High	High	High	Medium	Medium
	Medium	High	High	Medium	Medium	Low
	Low	High	Medium	Medium	Low	Very Low
	Very Low	Medium	Low	Low	Very Low	Very Low

# Risk vs threat-based approach.



<u>EXAMPLE RISK</u>		Probability				
		Very High	High	Medium	Low	Very Low
Consequence	Very High	Very High	Very High	High	High	High
	High	Very High	High	High	Medium	Medium
	Medium	High	High	Medium	Medium	Low
	Low	High	Medium	Medium	Low	Low
	Very Low	Medium	Low	Low	Very Low	Very Low

*Risk = Impact x Likelihood*

# Risk vs threat-based approach.



## ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Application Log	Jobs, Profiles and Scripts	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppLog	Auth Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMS/FTP	Accessibility Features	Accessibility Features	Binary Padding	Batch History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	Applet DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	Applet DLLs	Applet DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	Applet DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMS/FTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Spraying	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Traited Relationship	Exploitation for Client Execution	Browser Extensions	Emrod	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels	Resource Hijacking	Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Group Discovery	Remote Services	Main in the Browser	Multi-App Proxy	Runtime Data Manipulation	Resource Hijacking
	Installable	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels	Service Stop	Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Quarry Registry	Shared Webroot	Video Capture	Multi-Stage Communication	Service Stop	Stored Data Manipulation
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multi-Stage Encryption	System Shutdown/Reboot	Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	deobfuscate/Decode Files or Information	LLMNR/NLNR Poisoning and Relay	Security Software Discovery	Tampered Content		Port Knocking	System Shutdown/Reboot	Transmitted Data Manipulation
	Malsp	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		
	PowerShell	Emrod	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Repos/Regasm	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness	Path Interception	Execution Guardrails	Security Sessions	System Network Connections Discovery			Standard Cryptographic Protocol		
	RunSMB	Hidden Files and Directories	File Modification	Exploitation for Defense Evasion	Steal Web Session Cookie	System Owner/User Discovery			Standard Non-Application Layer Protocol		
	Scheduled Task	Hooking	Port Monitors	Extra Window Memory Injection	Two-Factor Authentication Interception	System Service Discovery			Uncommonly Used Port		
	Scripting	Hypervisor	PowerShell Profile	File and Directory Permissions Modification		System Time Discovery					
	Service Execution	Image File Execution Options Injection	Process Injection	File Deletion		Virtualization/Sandbox Evasion					
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Scheduled Task	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Service Registry Permissions Weakness	Gatekeeper Bypass							
	Source	Send and Setgid	Group Policy Modification								
	Space after Filename	Launchctl	SID-History Injection	Hidden Files and Directories							
	Third-party Software	IC.MSAS.JPCLB Addition	Startup Items	Hidden Users							
	Trap	Local Job Scheduling	Subs	Hidden Window							
	Traited Developer Utilities	Login Item	Subs Caching	HSTCONTROL							
	User Execution	Logon Scripts	Valid Accounts	Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver	Web Shell	Indicator Blocking							
	Windows Remote Management	Modify Existing Service	Network Helper DLL	Indicator Removal from Tools							
	XSL Script Processing	New Service	Office Application Startup	Indicator Removal on Host							
		Path Interception	Install Root Certificate	Indirect Command Execution							
		File Modification	InstallJBI								
		Port Knocking	Launchctl								
		Port Monitors	IC.MSAS.JPCLB Hijacking								
		PowerShell Profile	Masquerading								
		Re common	Modify Registry								
		Re-opened Applications	Malsp								
		Redundant Accounts	Network Share Connection Removal								
		Registry Run Keys / Startup Folder	NTFS File Attributes								
			Obfuscated Files or Information								



# Risk vs threat-based approach.



## *Risk-based*

- Covers all cases
- Well known
- Standardized

## *Threat-based*

- Very specific
- Applicable to all levels
- Proactive security

# Why?



**TLP:WHITE**

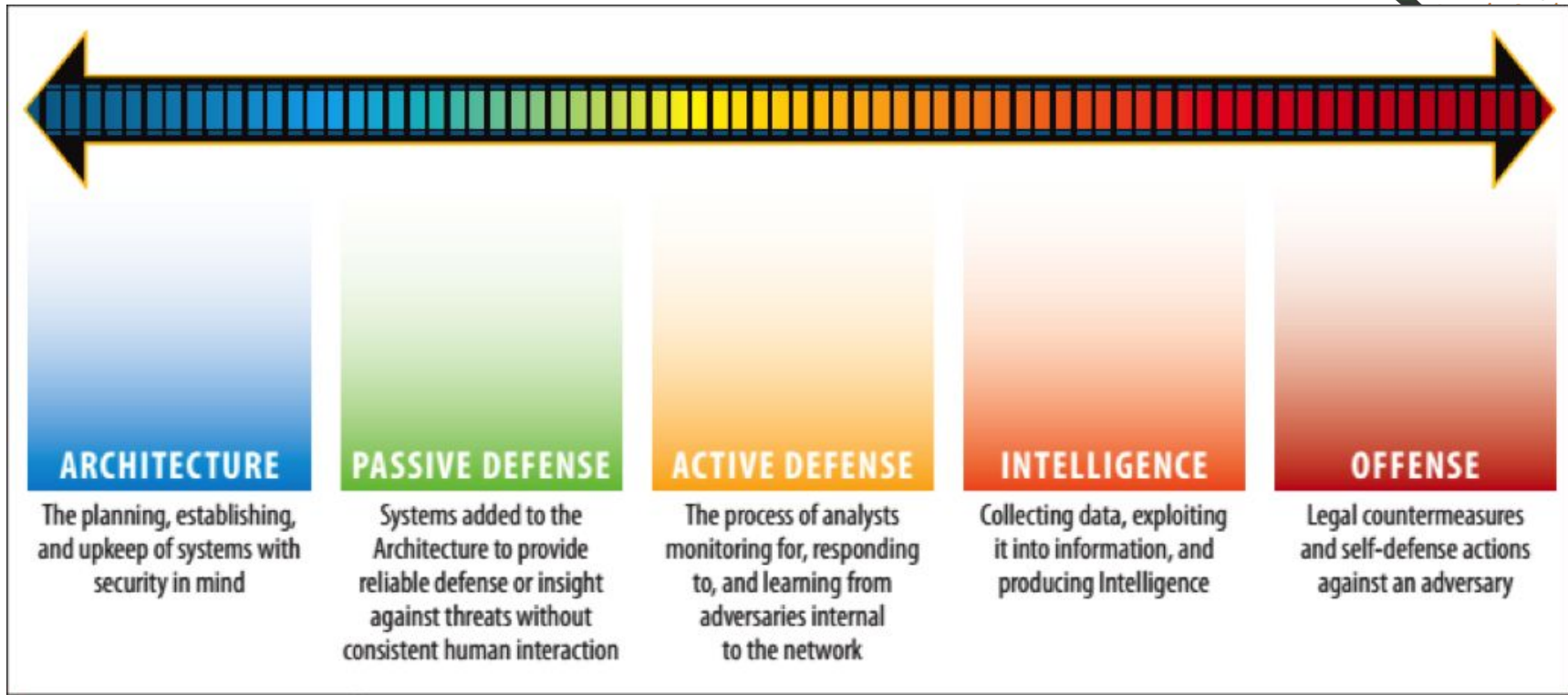


# Why?



TLP:WHITE

# Why?



The Sliding Scale of Cyber Security  
Robert M. Lee - September 2015

# Phase 1: The beginning.



- Typically on spare-time
- No Intelligence Requirements? Start small
- Analysis on past incidents
- Build campaigns & threat actor profiles
- Develop simple products and get lots of **feedback**  
(WARNING: DO NOT MAKE THIS AN ECHO CHAMBER)

# Phase 1: The beginning.



<p><b>Products</b></p> <ul style="list-style-type: none"><li>● Past campaigns</li><li>● Past threat actor profiles</li></ul>
<p><b>Customers</b></p> <ul style="list-style-type: none"><li>● Cyber-security team(s)</li><li>● Cyber-security leadership</li></ul>
<p><b>KPIs</b></p> <ul style="list-style-type: none"><li>● Consistency of products</li><li>● Incidents analyzed</li></ul>

# Phase 2: External threats.



- Map identified threat actors/groups to external ones
- Track their activities and proactively deploy controls
- Develop processes and focus on quality
- Start measuring key indicators
- Share success stories / develop good reputation

# Phase 2: External threats.



<h3>Products</h3> <ul style="list-style-type: none"><li>• Actor/campaign tracking</li><li>• External/internal mapping</li></ul>
<h3>Customers</h3> <ul style="list-style-type: none"><li>• Cyber-security team(s)</li><li>• Cyber-security leadership</li></ul>
<h3>KPIs</h3> <ul style="list-style-type: none"><li>• Incident response from TI</li><li>• False positive/negative rate</li></ul>

# Phase 3: Formal CTI function.



- Clear mission, vision, and purpose
- Goal-driven intelligence - be a force multiplier
- Quality over quantity!
- Start offering intelligence products for all levels (strategic, tactical, and operational) based on PIRs
- Formal team KPIs

# Phase 3: Formal CTI function.



<p><b>Products</b></p> <ul style="list-style-type: none"><li>• Support for RFIs</li><li>• Regular threat updates</li></ul>
<p><b>Customers</b></p> <ul style="list-style-type: none"><li>• Cyber-security team(s)</li><li>• Cyber-security leadership</li></ul>
<p><b>KPIs</b></p> <ul style="list-style-type: none"><li>• Response time on RFIs</li><li>• Quality of products</li></ul>

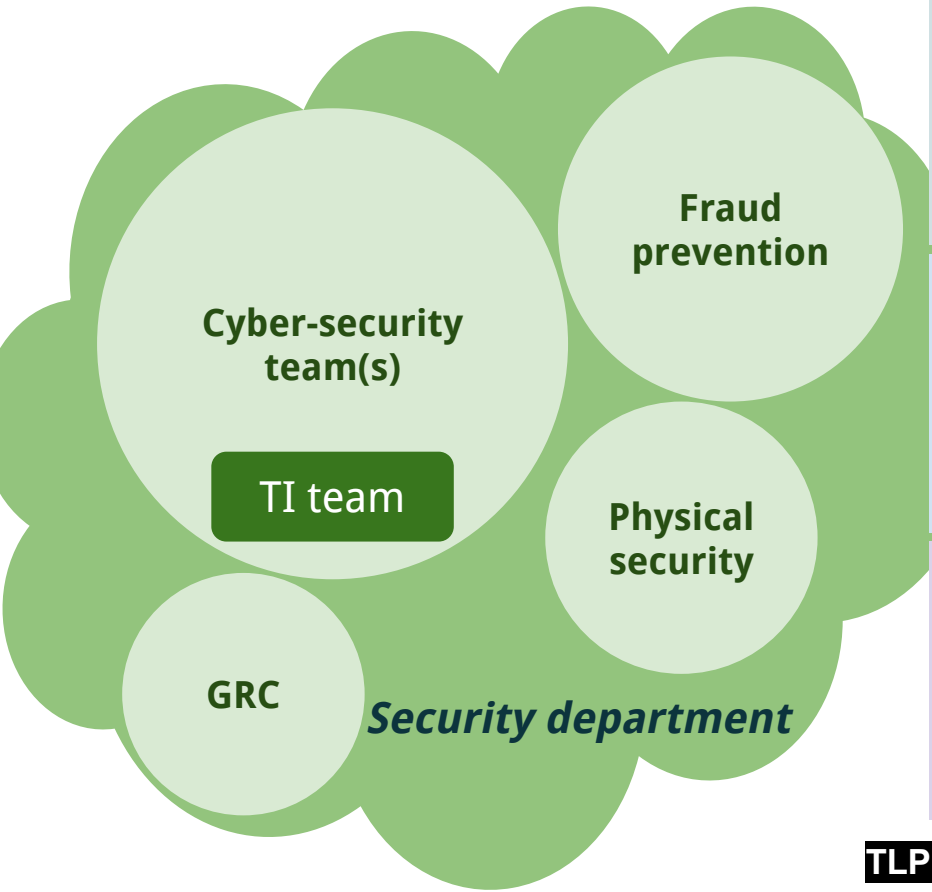


# Phase 4: Intelligence-driven security.



- Expand beyond cyber
- Provide intelligence services to all security teams
- Find links between threats from different domains
- Holistic intelligence reporting

# Phase 4: Intelligence-driven security.



**Products**

- Analytical support
- Multi-domain intelligence

**Customers**

- All security teams
- Security leadership

**KPIs**

- Metrics of proactive actions
- Teams utilizing TI resources

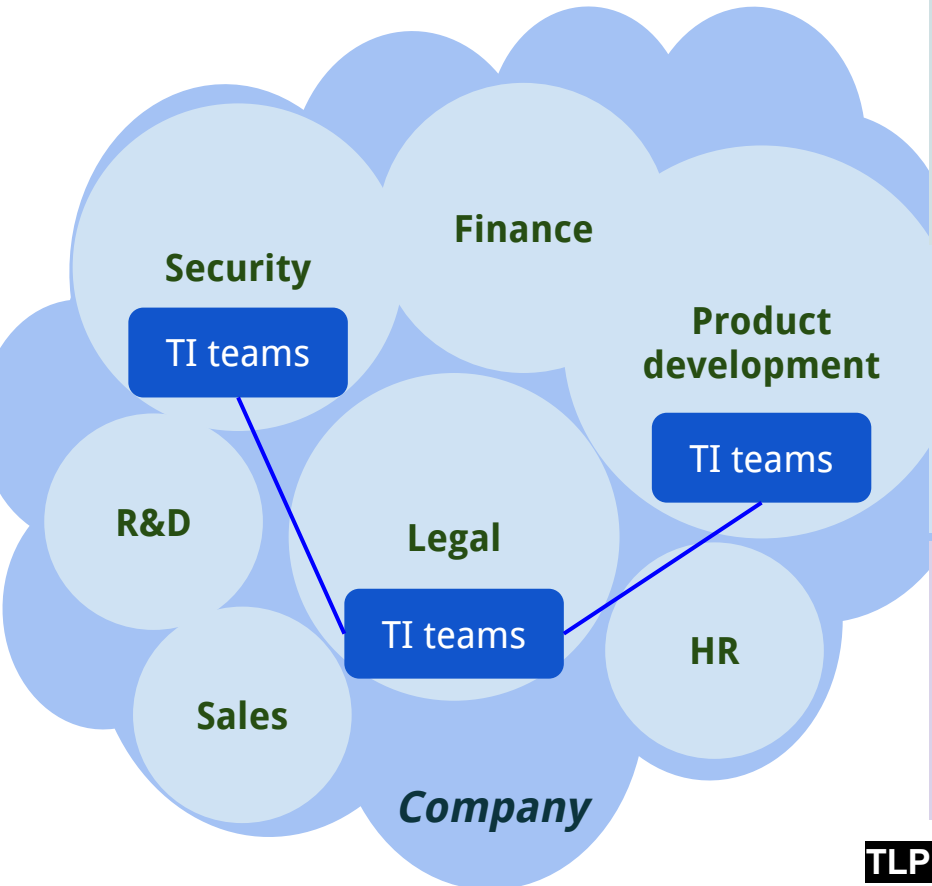
**TLP:WHITE**

# Phase 5: Intelligence-driven organization.



- Natural progression
- Build and train specialized intelligence teams
- Moving to the “left side of the boom” collectively
- Wider adoption of threat-based prioritization
- Create an internal intelligence community

# Phase 5: Intelligence-driven organization.



**Products**

- Analytical support
- Domain specific RFIs

**Customers**

- All company teams
- All company leadership

**KPIs**

- Per domain KPIs
- Deviations from standards

TLP:WHITE

# Summary.



Threat-based

**Phase 5: Intelligence-driven organization**

Risk-based

**Phase 4: Intelligence-driven security**

**Phase 3: Formal CTI function**

**Phase 2: External threats**

**Phase 1: Beginning**

**TLP:WHITE**

# References.



- Conducting Risk Assessments, NIST 800-30
- MITRE ATT&CK framework
- The Sliding Scale of Cyber Security, Robert M. Lee - September 2015
- Left of boom: Do we actually do this?, Anastasios (xorl) Pingios - December 2019

 @xorlgr

 Anastasios Pingios

**TLP:WHITE**