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, ...

TLP:WHITE

Agenda.

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

TLP:WHITE

Definition.

Threat intelligence

TLP:WHITE

Definition.

Threat intelligence

- Intent
- Opportunity
- Capability

TLP:WHITE

Definition.

Threat intelligence

- Product
- Process

TLP:WHITE

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

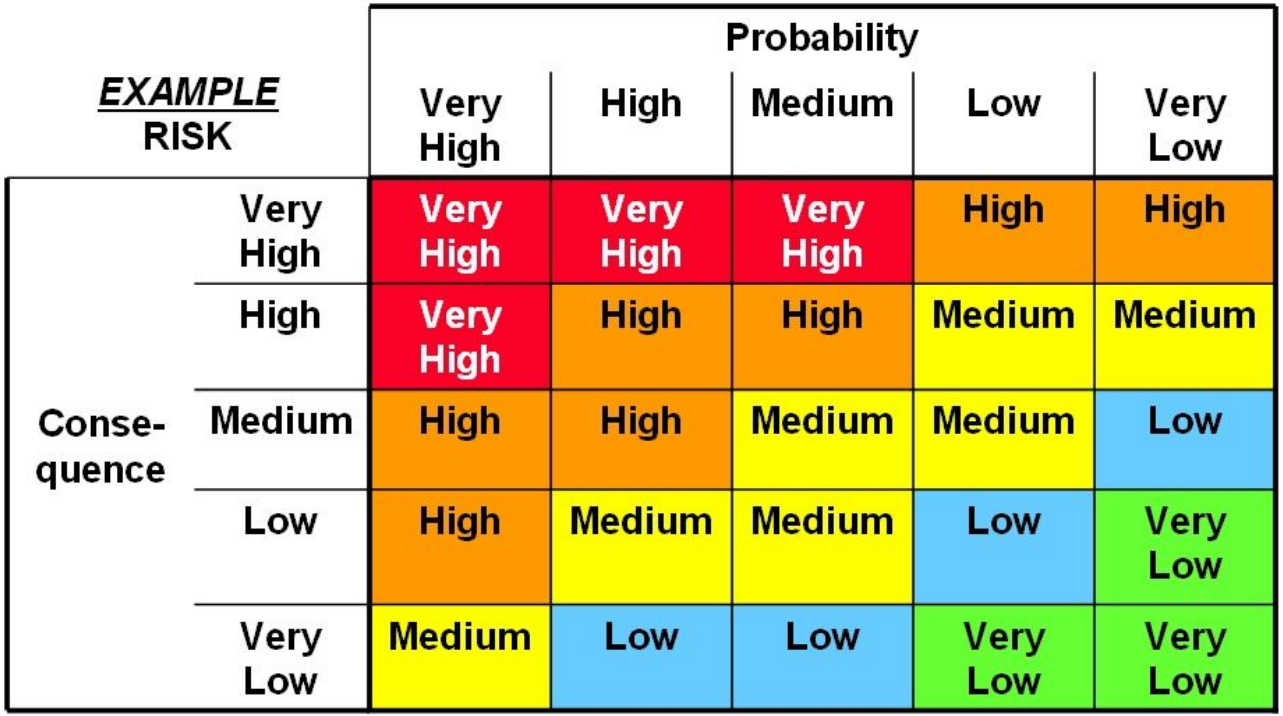
Definition.

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

Sun Tzu, The Art of War

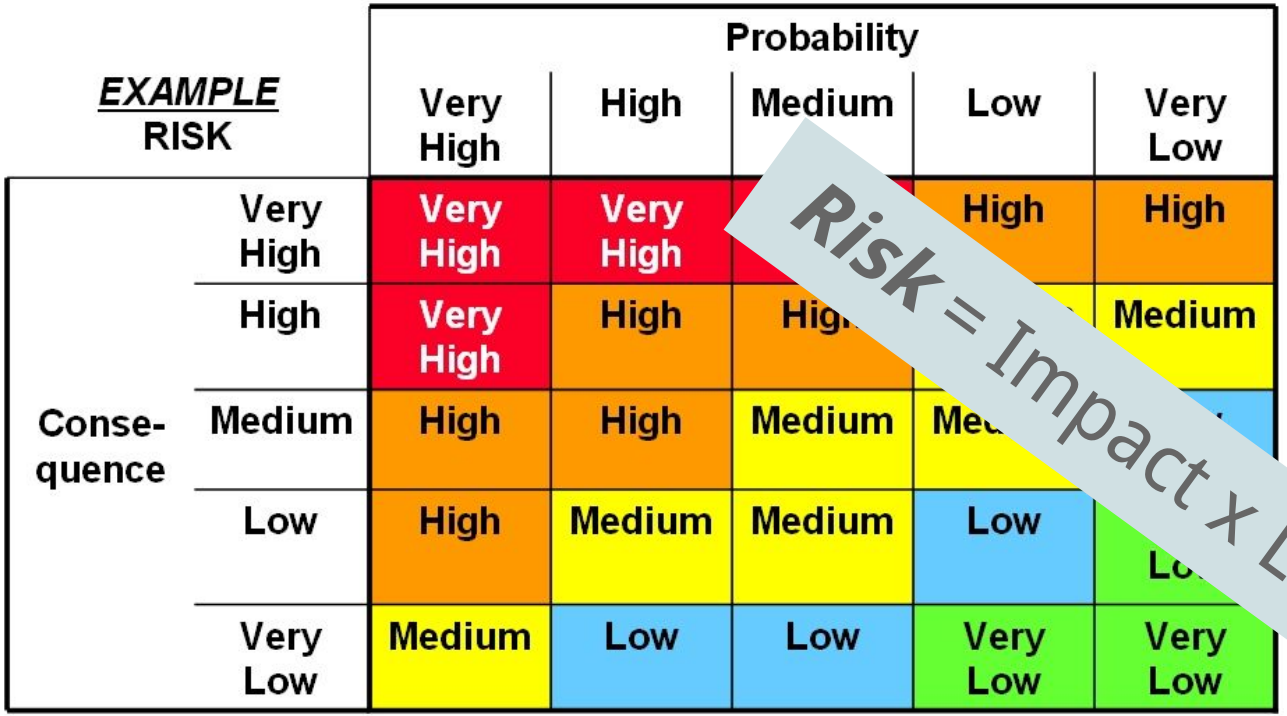
TLP:WHITE

Risk vs threat-based approach.



EXAMPLE 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.

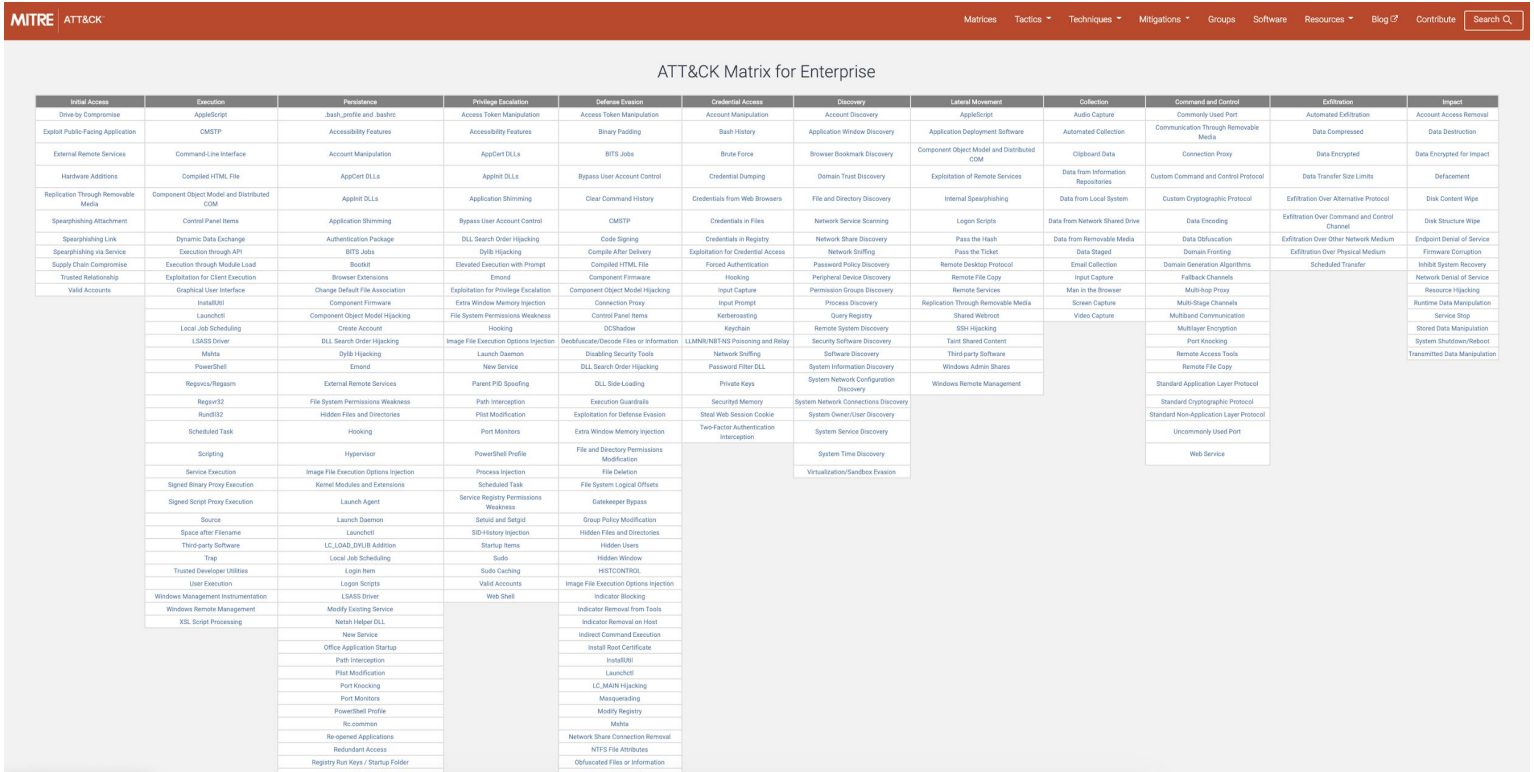


EXAMPLE RISK		Probability				
		Very High	High	Medium	Low	Very Low
Conse-quence	Very High	Very High	Very High		High	High
	High	Very High	High			Medium
	Medium	High	High	Medium		
	Low	High	Medium	Medium	Low	
	Very Low	Medium	Low	Low	Very Low	Very Low

Risk = Impact x Likelihood

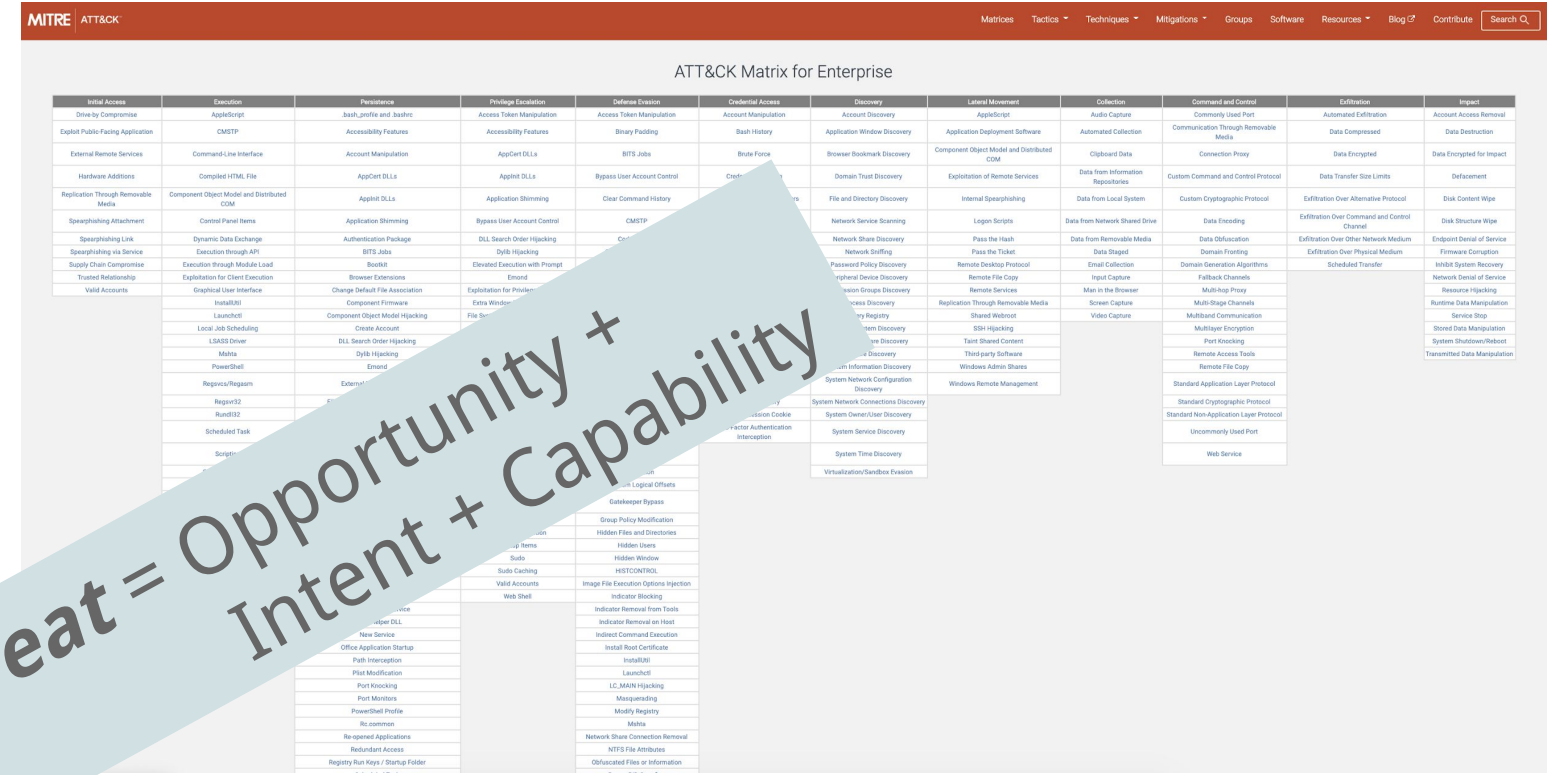
TLP:WHITE

Risk vs threat-based approach.



TLP:WHITE

Risk vs threat-based approach.



TLP:WHITE

Risk vs threat-based approach.

Risk-based

- Covers all cases
- Well known
- Standardized

Threat-based

- Very specific
- Applicable to all levels
- Proactive security

TLP:WHITE

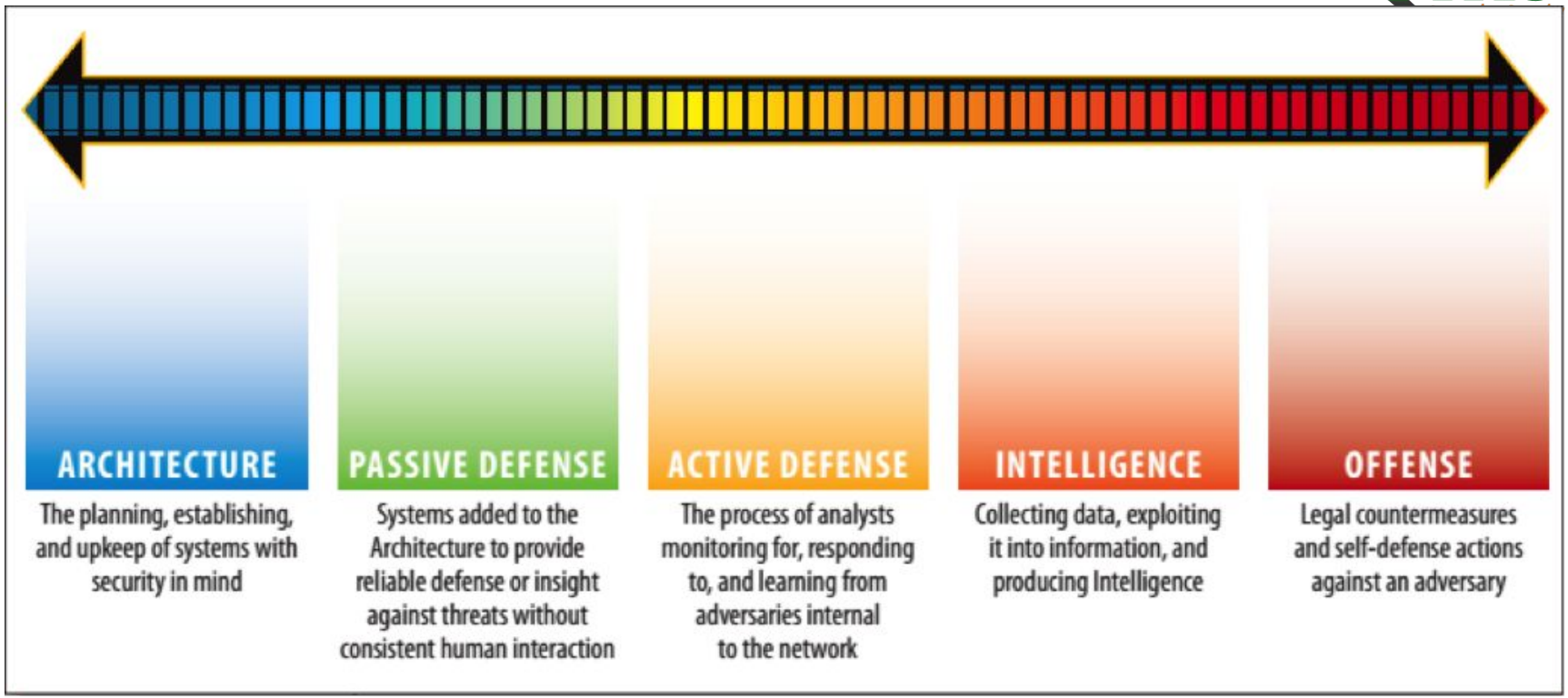
Why?

TLP:WHITE

Why?

TLP:WHITE

Why?



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

TLP:WHITE

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)

TLP:WHITE

Phase 1: The beginning.

Cyber-security team(s)

TI “team”

Products

- Past campaigns
- Past threat actor profiles

Customers

- Cyber-security team(s)
- Cyber-security leadership

KPIs

- Consistency of products
- Incidents analyzed

TLP:WHITE

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.

Products

- Actor/campaign tracking
- External/internal mapping

Customers

- Cyber-security team(s)
- Cyber-security leadership

KPIs

- Incident response from TI
- False positive/negative rate

TLP:WHITE

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

TLP:WHITE

Phase 3: Formal CTI function.

Products

- Support for RFIs
- Regular threat updates

Customers

- Cyber-security team(s)
- Cyber-security leadership

KPIs

- Response time on RFIs
- Quality of products

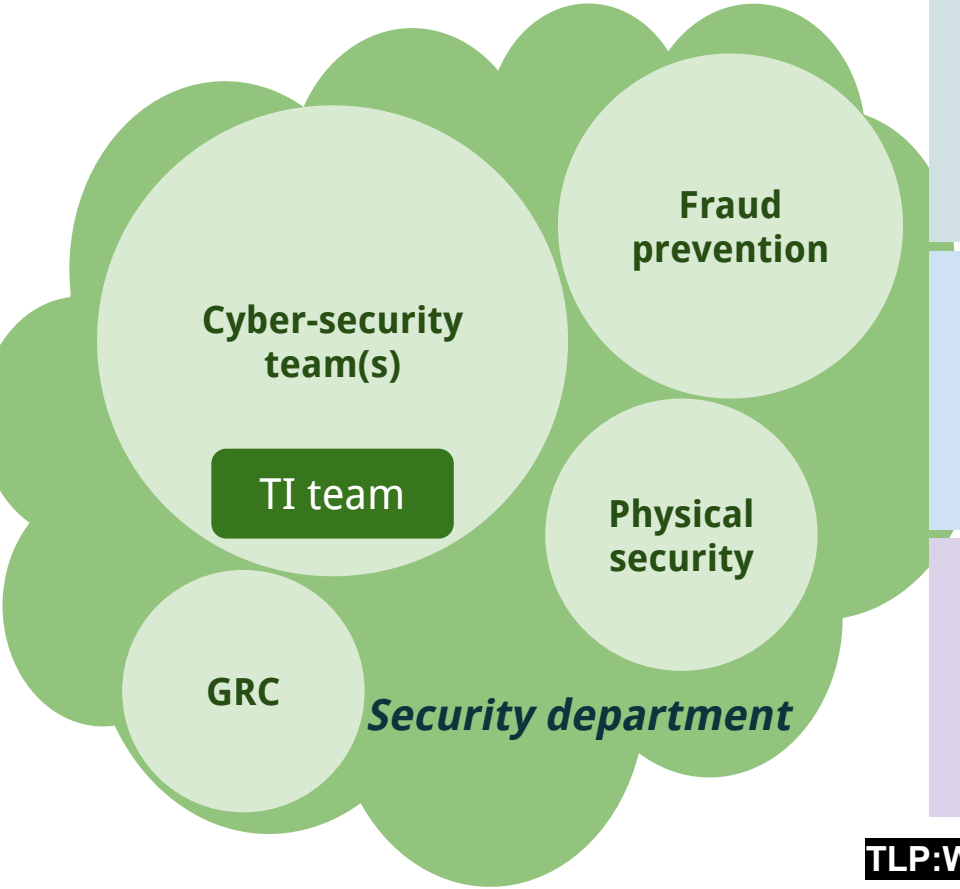
TLP:WHITE

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

TLP:WHITE

Phase 4: Intelligence-driven security.



Products

- Analytical support
- Multi-domain intelligence

Customers

- All security teams
- Security leadership

KPIs

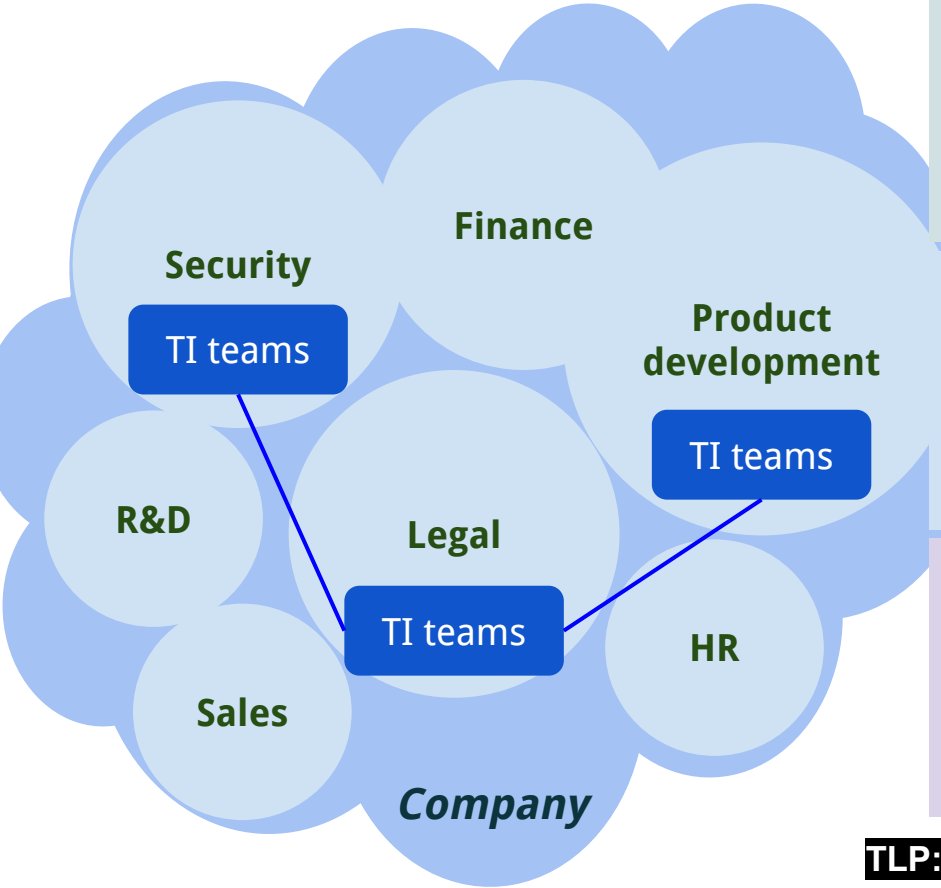
- Metrics of proactive actions
- Teams utilizing TI resources

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

Risk-based

Phase 5: Intelligence-driven organization

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