Reducing cyber risks in the era of digital transformation

Sergey Soldatov

Head of Security Operations Center, R&D Security Services

ICC
International
Cybersecurity
Congress

KASPERSKY lab

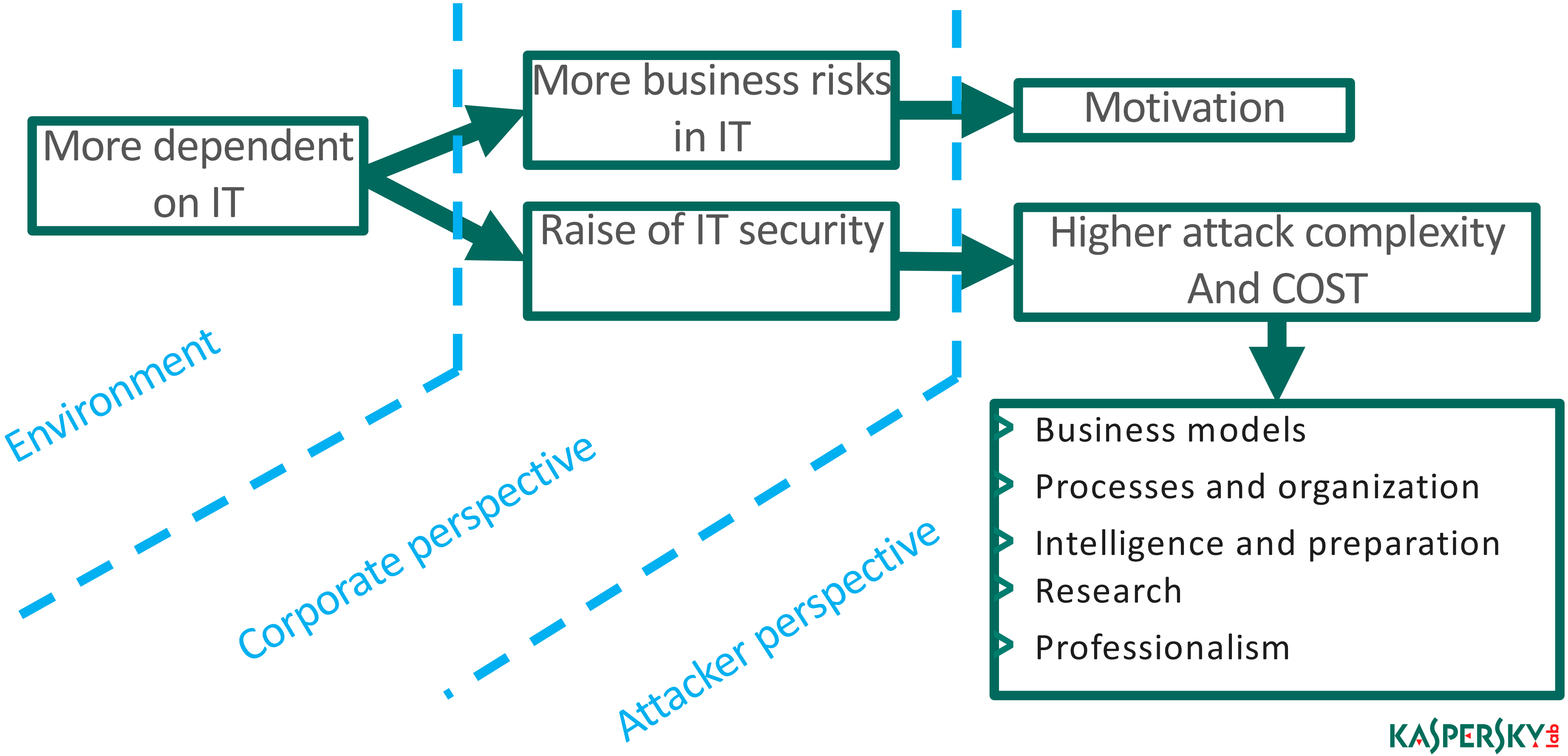
SAVING
THE WORLD
FOR 20 YEARS

WHO AM I ?

- Since 2016: Head of SOC at Kaspersky lab
  - Internal SOC
  - Commercial MDR* services
- 2012 – 2016: Chief manager at RN-Inform
  - Rosneft security services insourcing
- 2002 – 2012: TNK-BP Group
  - IT security integration into business and IT operations
  - Security controls in IT projects
  - Security operations
- 2001-2002: Software developer at RIPN
- BMSTU graduate
- CISA, CISSP
- Speaker, writer, participant, volunteer

* Managed Detection and Response

THE ERA OF DIGITAL TRANSFORMATION



More dependent on IT

More business risks in IT

Raise of IT security

Motivation

Higher attack complexity And COST

- Business models
- Processes and organization
- Intelligence and preparation
- Research
- Professionalism

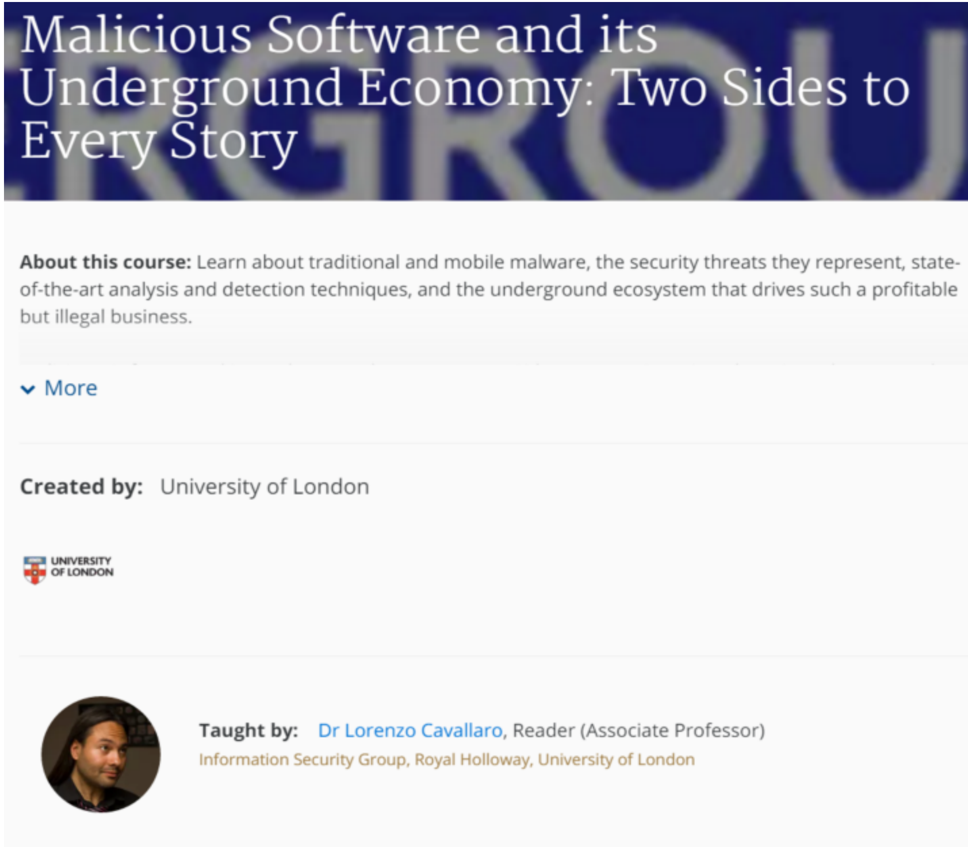
Environment

Corporate perspective

Attacker perspective

ATTACKER PERSPECTIVE

- Pentest-like
  - *“Offensive certified hackers”*
- Outsourced service
  - Profitable business
- Based on cutting edge research and approaches



Malicious Software and its Underground Economy: Two Sides to Every Story

About this course: Learn about traditional and mobile malware, the security threats they represent, state-of-the-art analysis and detection techniques, and the underground ecosystem that drives such a profitable but illegal business.

Created by: University of London

Taught by: Dr Lorenzo Cavallaro, Reader (Associate Professor)
Information Security Group, Royal Holloway, University of London

ATTACKER PERSPECTIVE

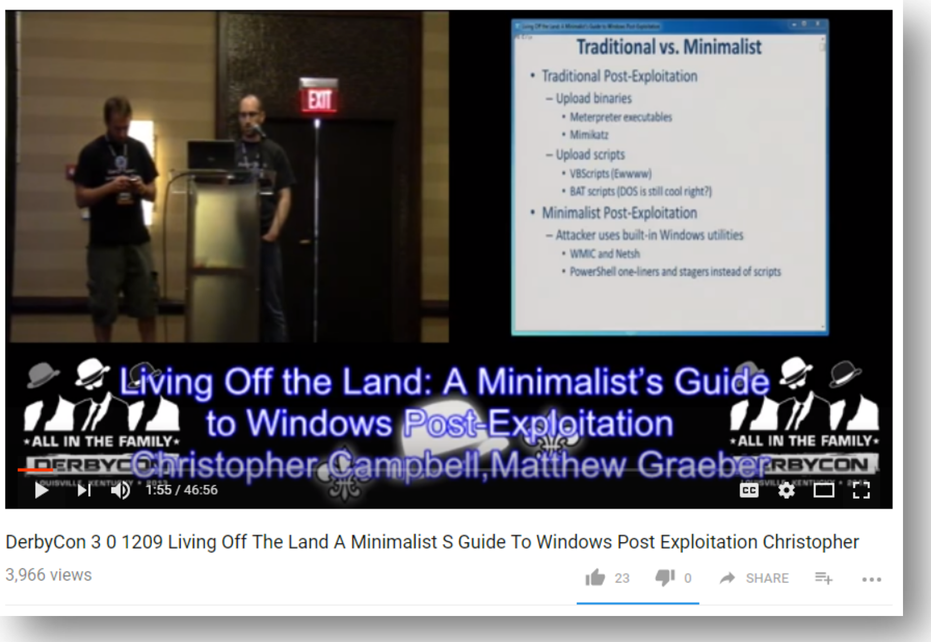
- Pentest-like
  - *“Offensive certified hackers”*
- Outsourced service
  - Profitable business
- Based on cutting edge research and approaches

- Classics
  - Anti-forensics
  - Multi-stage
- Modernity spirit:
  - File less & Malware less
  - Living off the land
  - Bring your own land
  - Off-the-shelf attack simulation toolsets
  - New mysterious TTP*

* Tactics, techniques and procedures

LIVING OFF THE LAND

- Malware-less
- Use of built-in OS tools
- In-memory only (file-less)
- Maximum use of context knowledge (make no anomalies):
  - Use tools that are already used
  - Use protocols that are already used
  - Don’t talk when the net is quiet



Traditional vs. Minimalist

- Traditional Post-Exploitation
  - Upload binaries
    - Meterpreter executables
    - Mimikatz
  - Upload scripts
    - VBScripts (Ewwww)
    - BAT scripts (DOS is still cool right?)
- Minimalist Post-Exploitation
  - Attacker uses built-in Windows utilities
    - WMIC and Netsh
    - PowerShell one-liners and stagers instead of scripts

Living Off the Land: A Minimalist’s Guide to Windows Post-Exploitation

Christopher Campbell, Matthew Graeber

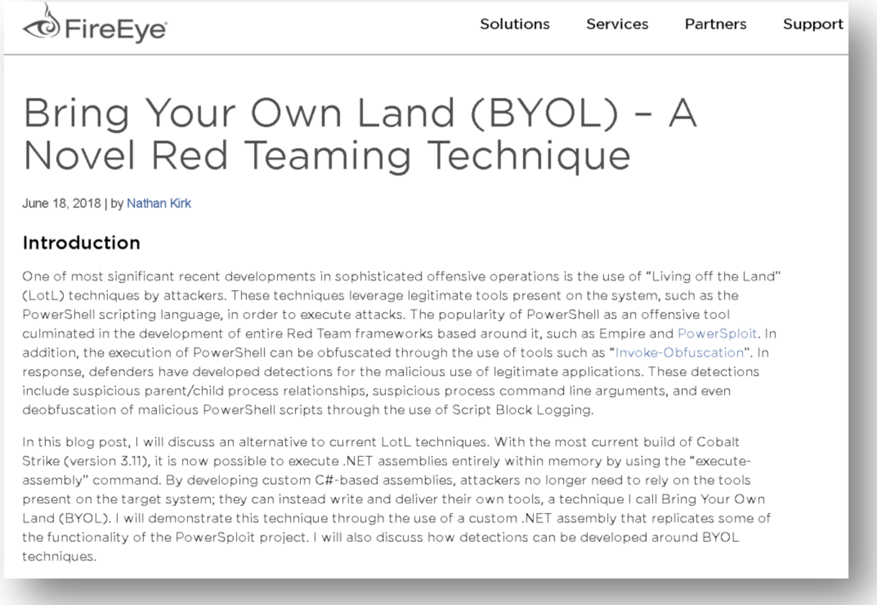
DerbyCon 3 0 1209 Living Off The Land A Minimalist S Guide To Windows Post Exploitation Christopher

3,966 views

https://www.youtube.com/watch?v=j-r6UonEkUw

BRING YOUR OWN LAND

- When PowerShell is not an option
- All requited functionality is part of specially created PE
- Malicious code is run in legitimate process memory – no suspicious parent-child relationship, no artefacts on disk
- Available in off-the-shelf adversary emulation tools (Cobalt strike)



Bring Your Own Land (BYOL) – A Novel Red Teaming Technique

June 18, 2018 | by Nathan Kirk

Introduction

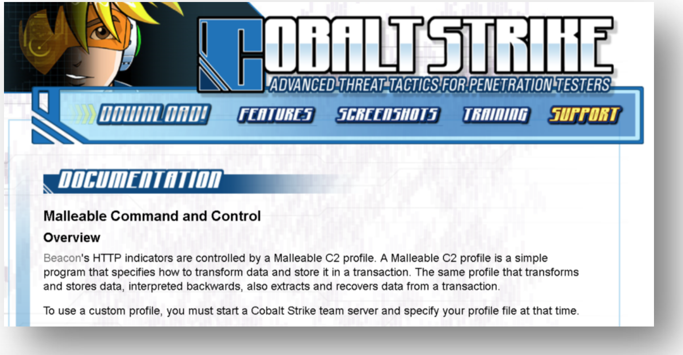
One of most significant recent developments in sophisticated offensive operations is the use of "Living off the Land" (LotL) techniques by attackers. These techniques leverage legitimate tools present on the system, such as the PowerShell scripting language, in order to execute attacks. The popularity of PowerShell as an offensive tool culminated in the development of entire Red Team frameworks based around it, such as Empire and PowerSploit. In addition, the execution of PowerShell can be obfuscated through the use of tools such as "Invoke-Obfuscation". In response, defenders have developed detections for the malicious use of legitimate applications. These detections include suspicious parent/child process relationships, suspicious process command line arguments, and even deobfuscation of malicious PowerShell scripts through the use of Script Block Logging.

In this blog post, I will discuss an alternative to current LotL techniques. With the most current build of Cobalt Strike (version 3.11), it is now possible to execute .NET assemblies entirely within memory by using the "execute-assembly" command. By developing custom C#-based assemblies, attackers no longer need to rely on the tools present on the target system; they can instead write and deliver their own tools, a technique I call Bring Your Own Land (BYOL). I will demonstrate this technique through the use of a custom .NET assembly that replicates some of the functionality of the PowerSploit project. I will also discuss how detections can be developed around BYOL techniques.

https://www.fireeye.com/blog/threat-research/2018/06/bring-your-own-land-novel-red-teaming-technique.html

AVAILABLE TOOLSETS

- Commercially supported and maintained
- Very difficult attribution
- Disguise capabilities:
  - False attribution
  - Benign activity

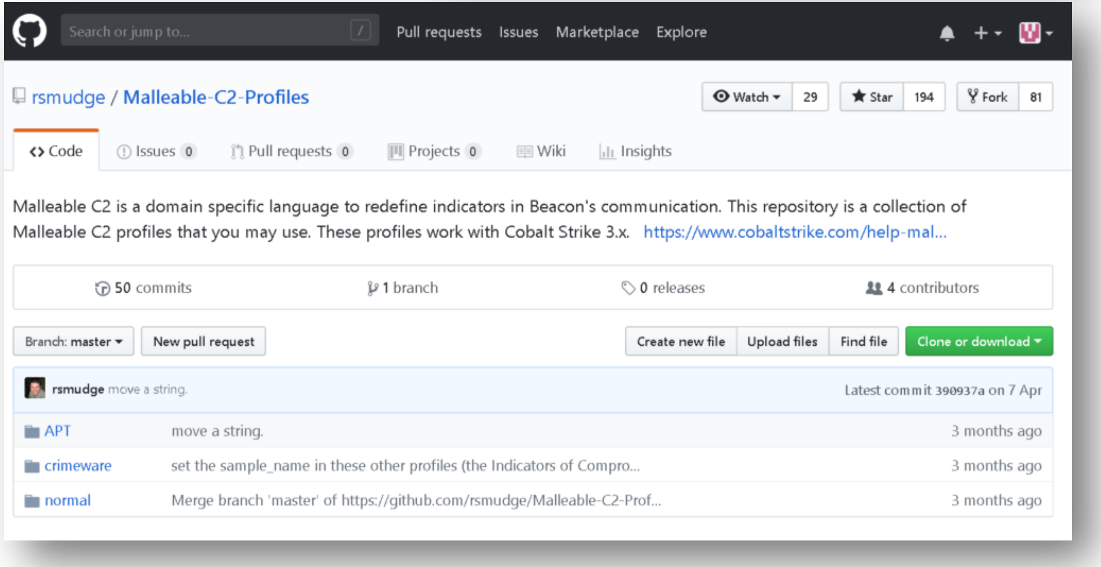


Malleable Command and Control

Overview

Beacon's HTTP indicators are controlled by a Malleable C2 profile. A Malleable C2 profile is a simple program that specifies how to transform data and store it in a transaction. The same profile that transforms and stores data, interpreted backwards, also extracts and recovers data from a transaction.

To use a custom profile, you must start a Cobalt Strike team server and specify your profile file at that time.



rsmudge / Malleable-C2-Profiles

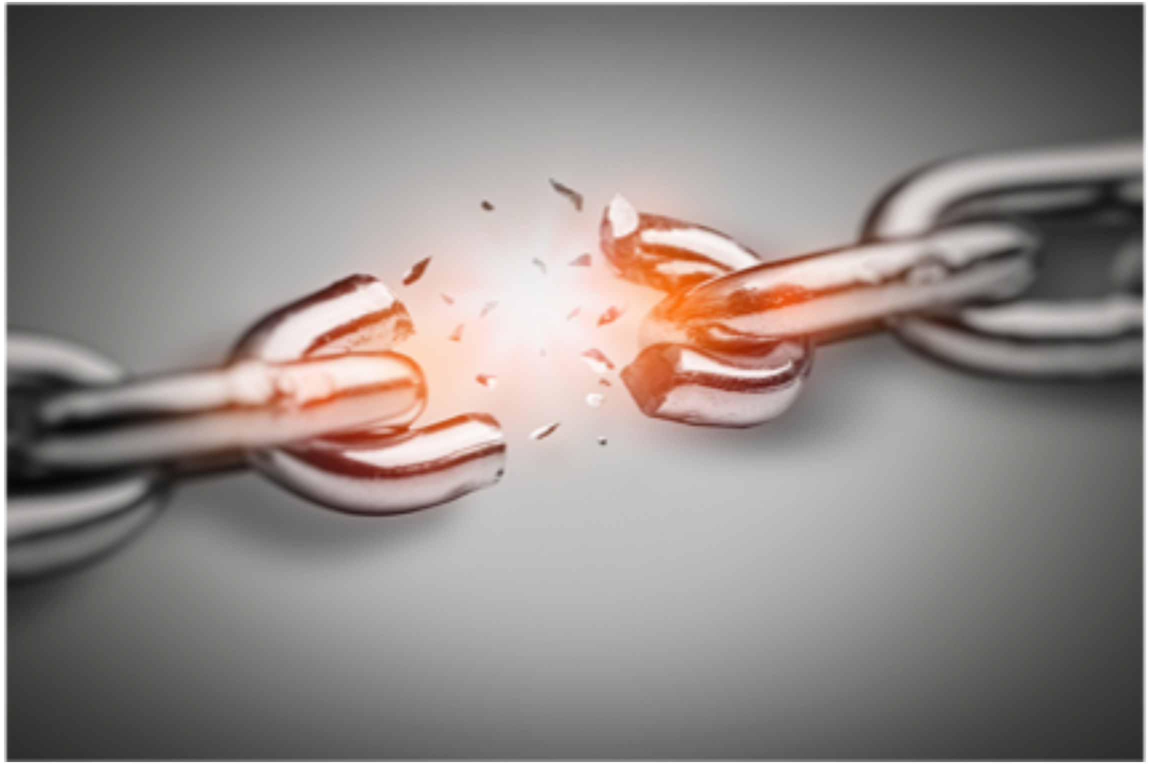
Malleable C2 is a domain specific language to redefine indicators in Beacon's communication. This repository is a collection of Malleable C2 profiles that you may use. These profiles work with Cobalt Strike 3.x. https://www.cobaltstrike.com/help-mal...

50 commits | 1 branch | 0 releases | 4 contributors

rsmudge move a string. | Latest commit 390937a on 7 Apr

APT	move a string.	3 months ago
crimeware	set the sample_name in these other profiles (the Indicators of Compro...	3 months ago
normal	Merge branch 'master' of https://github.com/rsmudge/Malleable-C2-Prof...	3 months ago

ATTACKER ALWAYS ATTACKS THE WEAKEST LINK

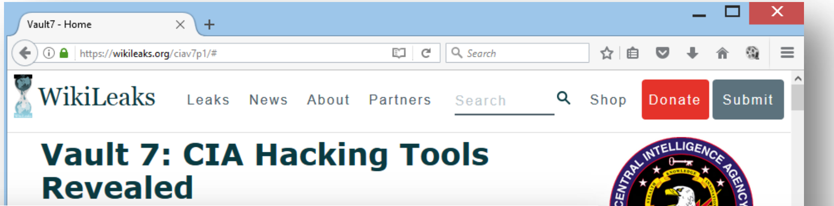


http://reply-to-all.blogspot.com/2018/04/blog-post.html

…AND CYBER WEAPON FOR ALL!

- The resources of the attacker are limitless!

- Prevention
- Detection → **Threat hunting**
- **Response**

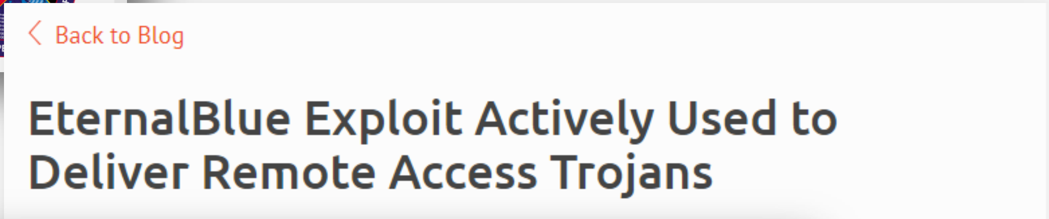


Vault 7: CIA Hacking Tools Revealed

USENIX Enigma 2016 - NSA TAO Chief on Disrupting Nation State Hackers

108,293 views

USENIX Enigma Conference
Published on Jan 28, 2016



EternalBlue Exploit Actively Used to Deliver Remote Access Trojans

threat actors have
lware is not a
one is a remote
heir computers for

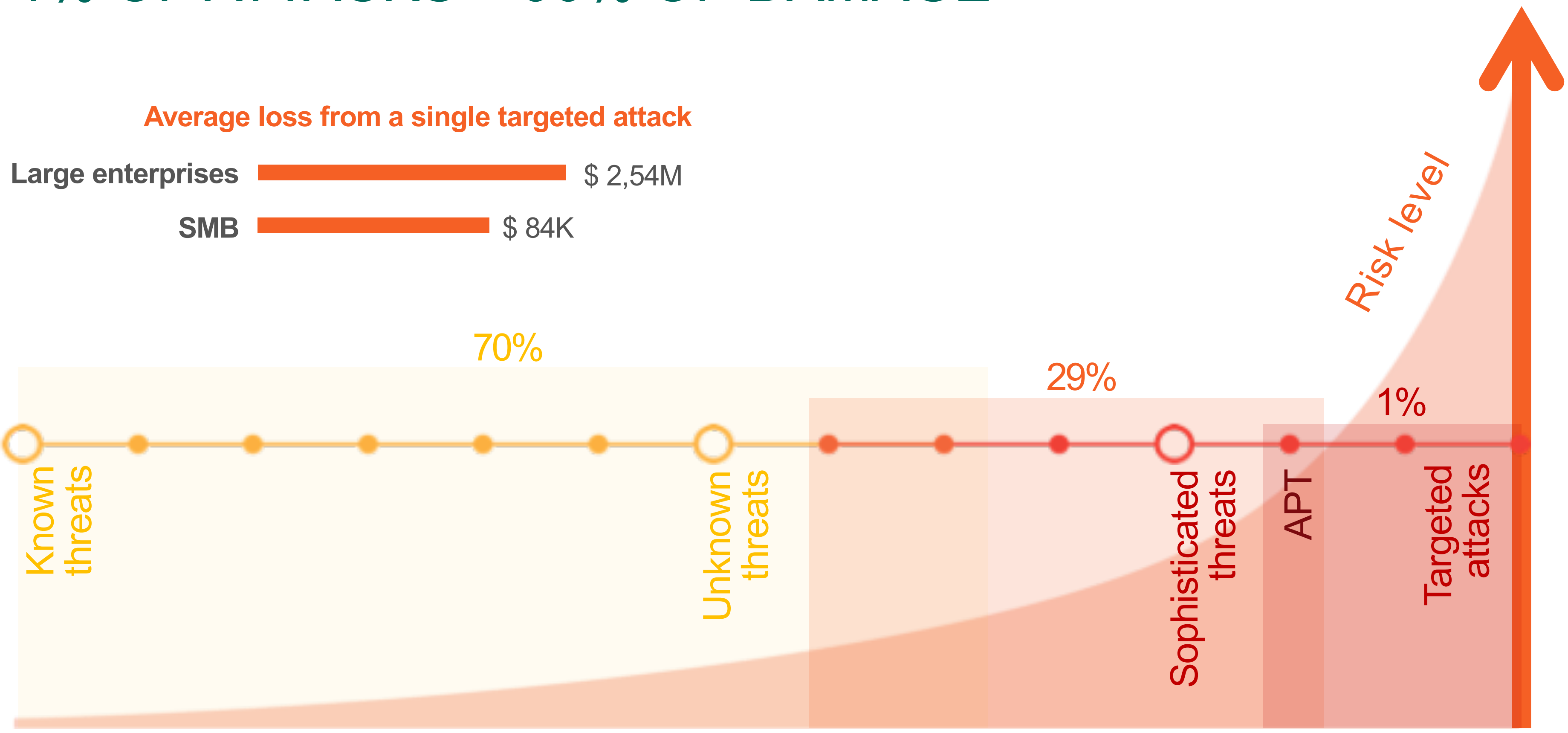
WannaCry ransomware used in widespread attacks all over the world

By GReAT on May 12, 2017. 5:30 pm

Earlier today, our products detected and successfully blocked a large number of ransomware attacks around the world. In these attacks, data is encrypted with the extension “.WCRY” added to the filenames

KASPERSKY lab

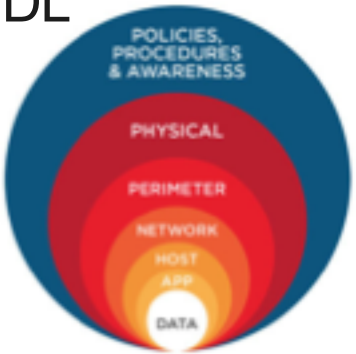
1% OF ATTACKS – 90% OF DAMAGE

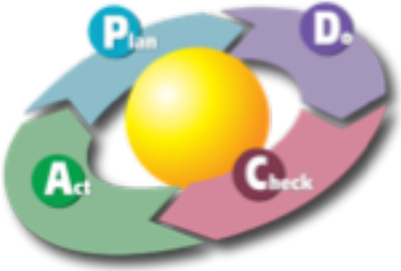


* According to Kaspersky lab and B2B international research “Enterprise information security”. Average damage from single targeted attack, including direct losses and indirect costs of restoration after the attack.

THREAT LANDSCAPE OUTRO

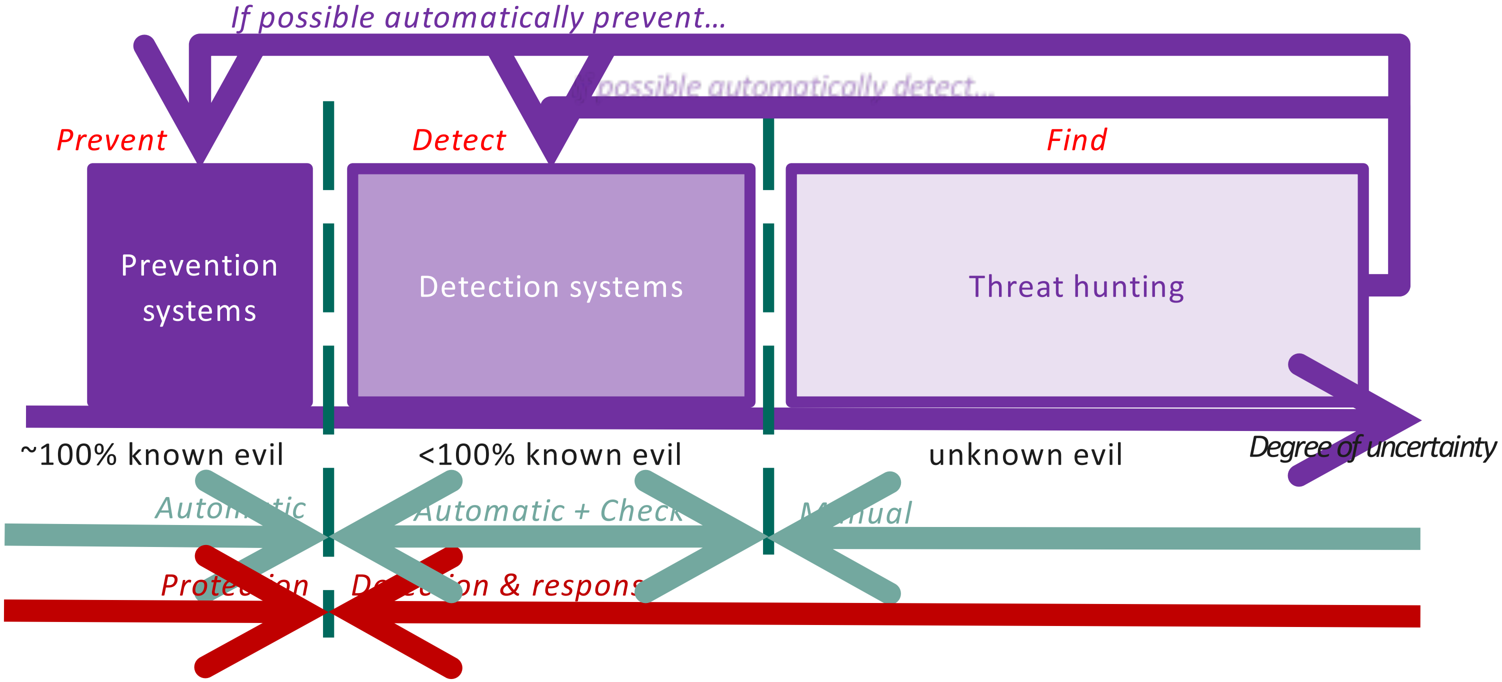
- Layers:
  - By approach: Prevent → Detect → Hunt
  - By technology: Entities → Behavior → Statistics → ML → DL
  - By Kill Chain: Pre-breach → Post-breach
  - By decision maker: Sensor → Cloud → Human
  - By media: Endpoint → Network
- Cycles:
  - Threat intel → Detect → Practice → Threat intel
  - Hunt → Detect → Hunt





LAYERS

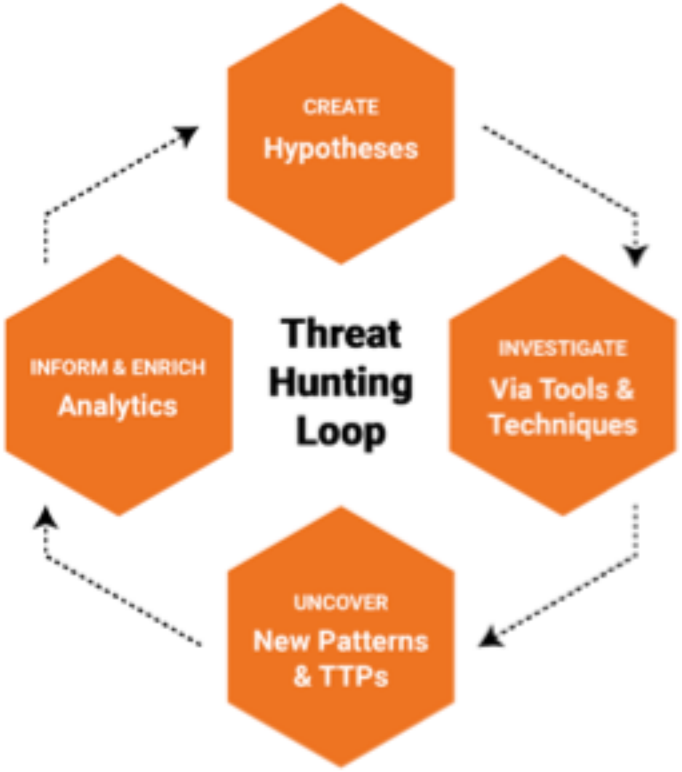
APPROACH LAYERS: PREVENT → DETECT → HUNT



http://reply-to-all.blogspot.com/2017/11/epp-edr.html

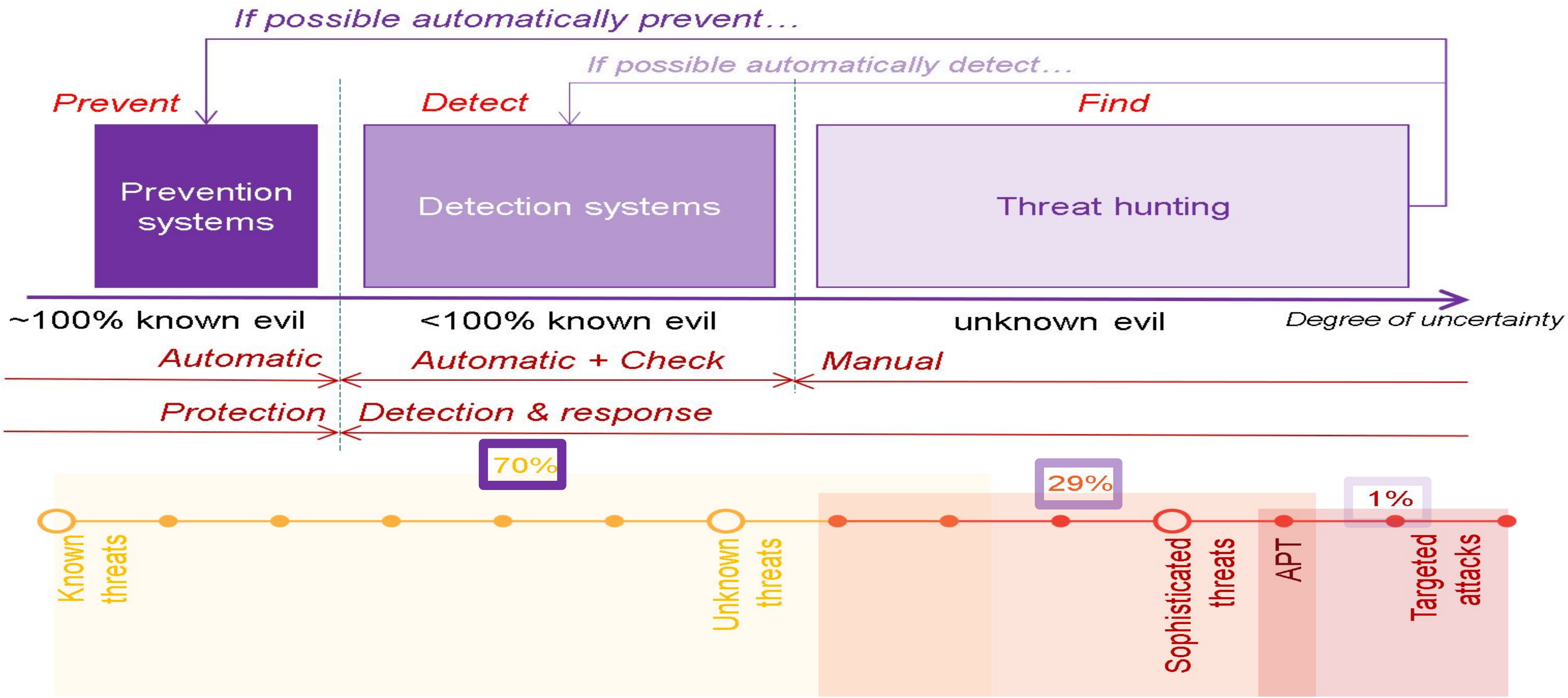
THREAT HUNTING

Cyber threat hunting is the practice of searching iteratively through data to detect advanced threats that evade traditional security solutions.



https://sqrrl.com/solutions/cyber-threat-hunting/

PROTECTION STRATEGY – WAYS OF RETREAT

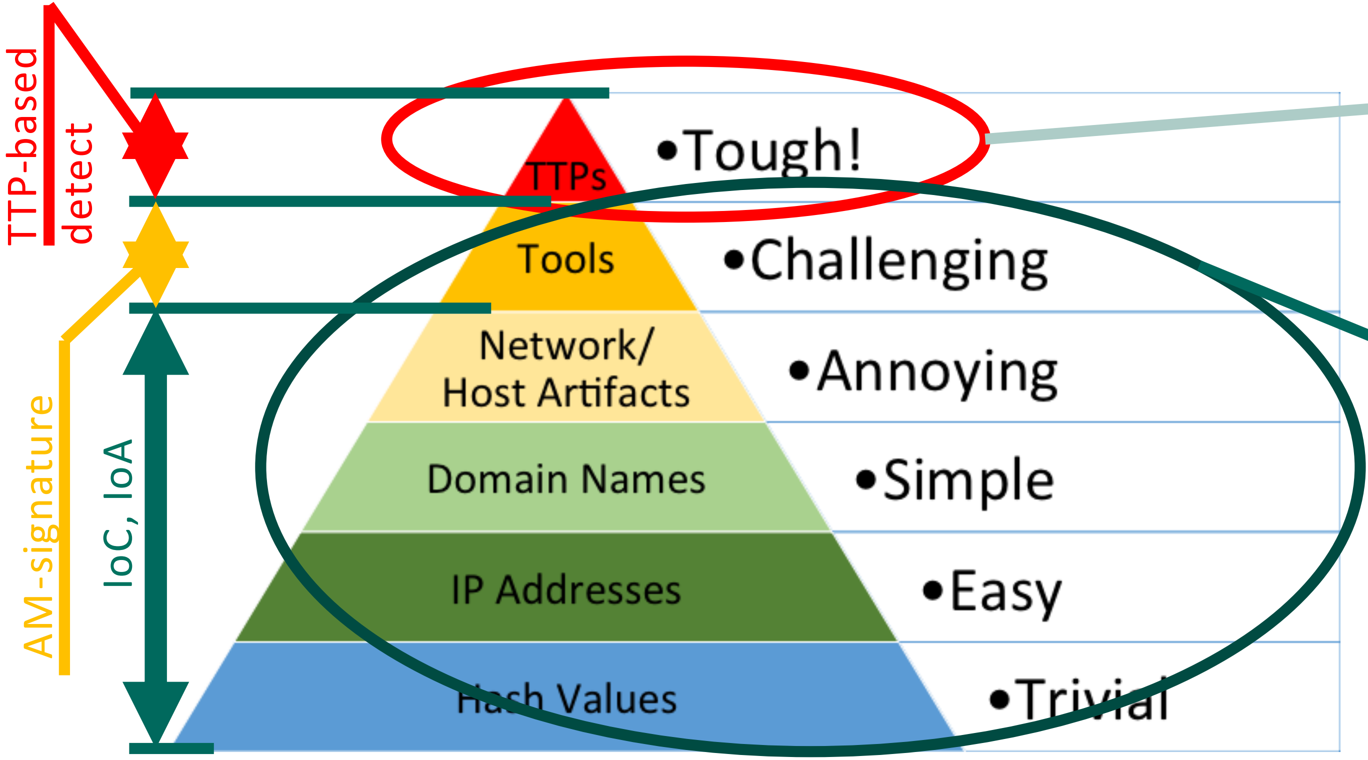


DETECT LAYERS: ANTI-MALWARE & SANDBOX

	Endpoint AM-engine (AM)	Sandbox (SB)
Advantages	- **Real environment** - Real user activity - Unlimited processing time	- **No performance limitations** - Low impact from True Positive
Disadvantages	- **Performance Limitations** - Big impact from True Positive	- **Artificial environment** - Emulated user activity (required actions may not be fulfilled) - Limited processing time

- Different technologies works with different effectiveness and efficiency against different attacks
- AM and SB complement each other to better cumulative detection rate

DETECT LAYERS: DAVID BIANCO'S PYRAMID OF PAIN

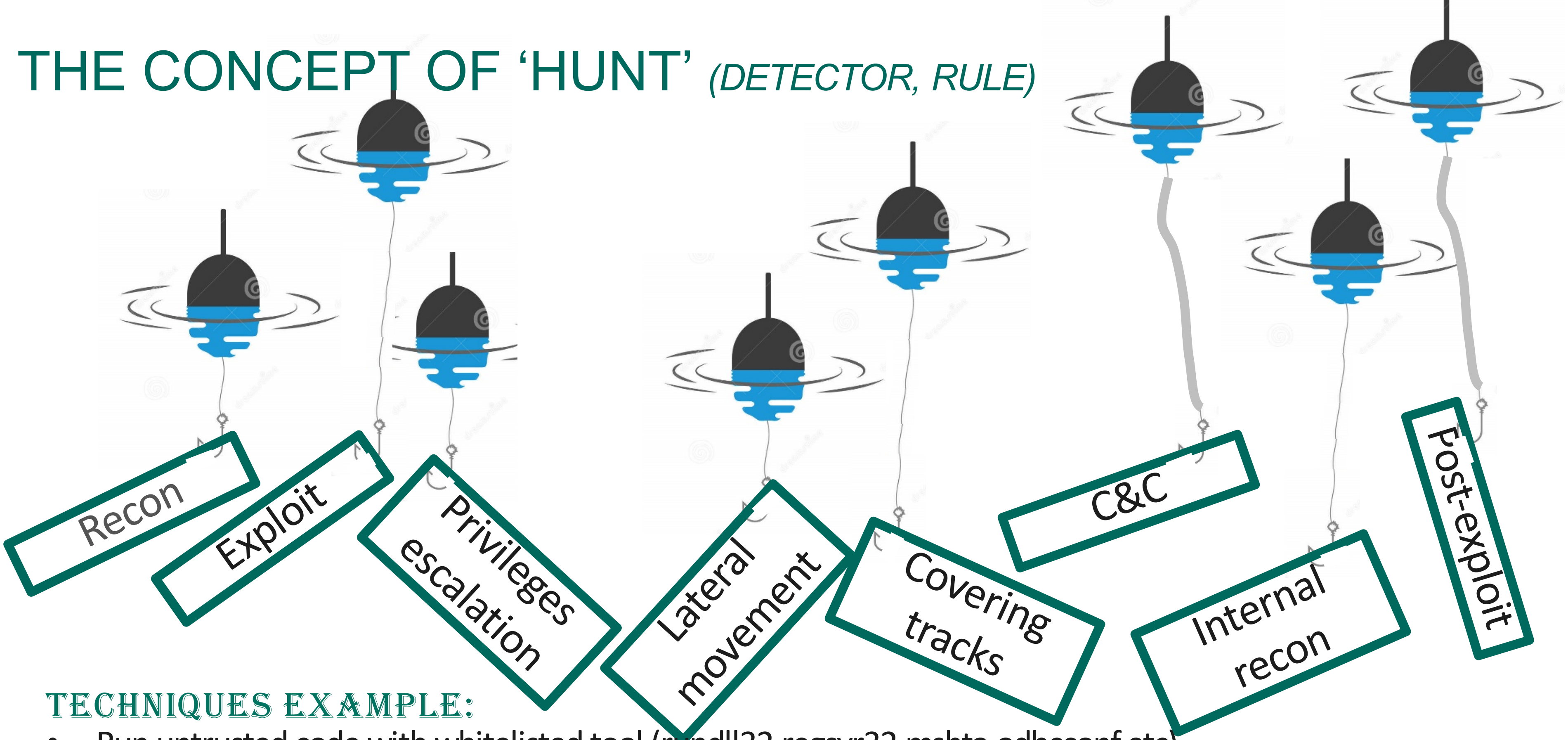


Human Analyst required

Commodity Prevention/Detection tools capabilities (can be done automatically)

http://detect-respond.blogspot.ru/2013/03/the-pyramid-of-pain.html

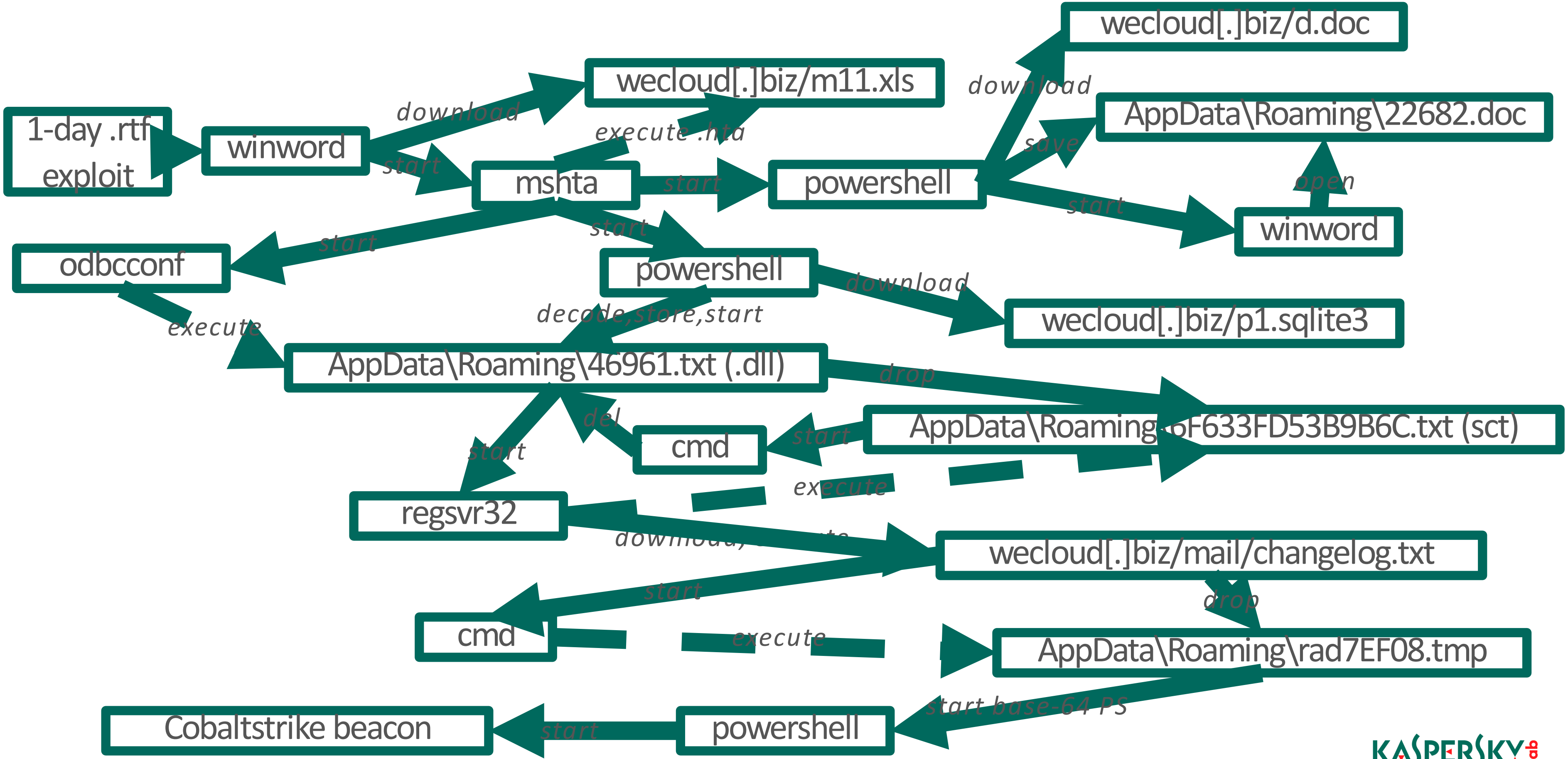
THE CONCEPT OF 'HUNT' *(DETECTOR, RULE)*



TECHNIQUES EXAMPLE:

- Run untrusted code with whitelisted tool (rundll32,regsvr32,mshta,odbcconf,etc)
- Office app spawns cmd/powershell/etc
- Access to paste service from non-browsers
- …

REAL ATTACK (SIMPLIFIED)



1-day .rtf exploit

winword

wecloud[.]biz/m11.xls

mshta

powershell

wecloud[.]biz/d.doc

AppData\Roaming\22682.doc

winword

odbcconf

powershell

wecloud[.]biz/p1.sqlite3

AppData\Roaming\46961.txt (.dll)

AppData\Roaming\6F633FD53B9B6C.txt (sct)

cmd

regsvr32

wecloud[.]biz/mail/changelog.txt

cmd

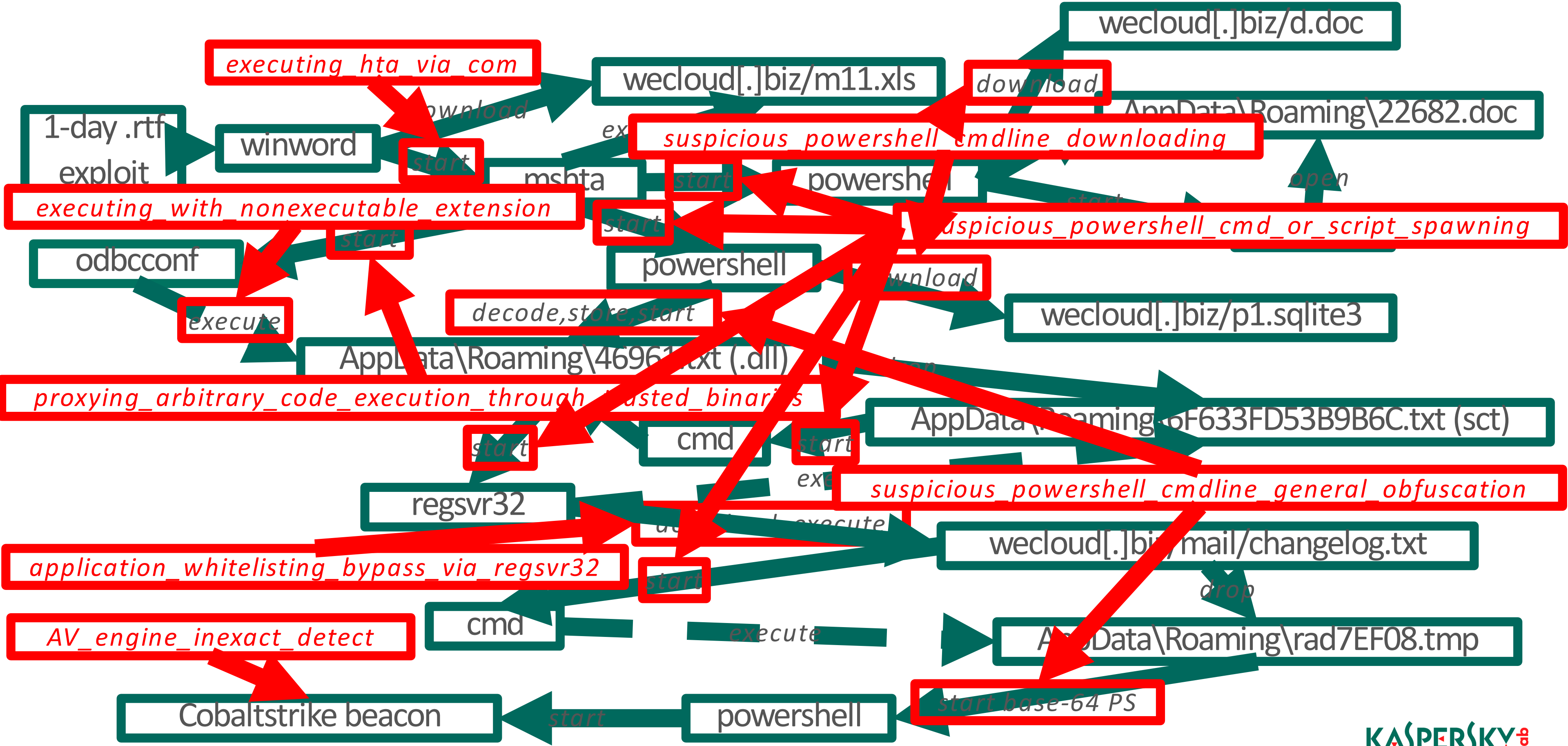
AppData\Roaming\rad7EF08.tmp

Cobaltstrike beacon

powershell

KASPERSKY lab

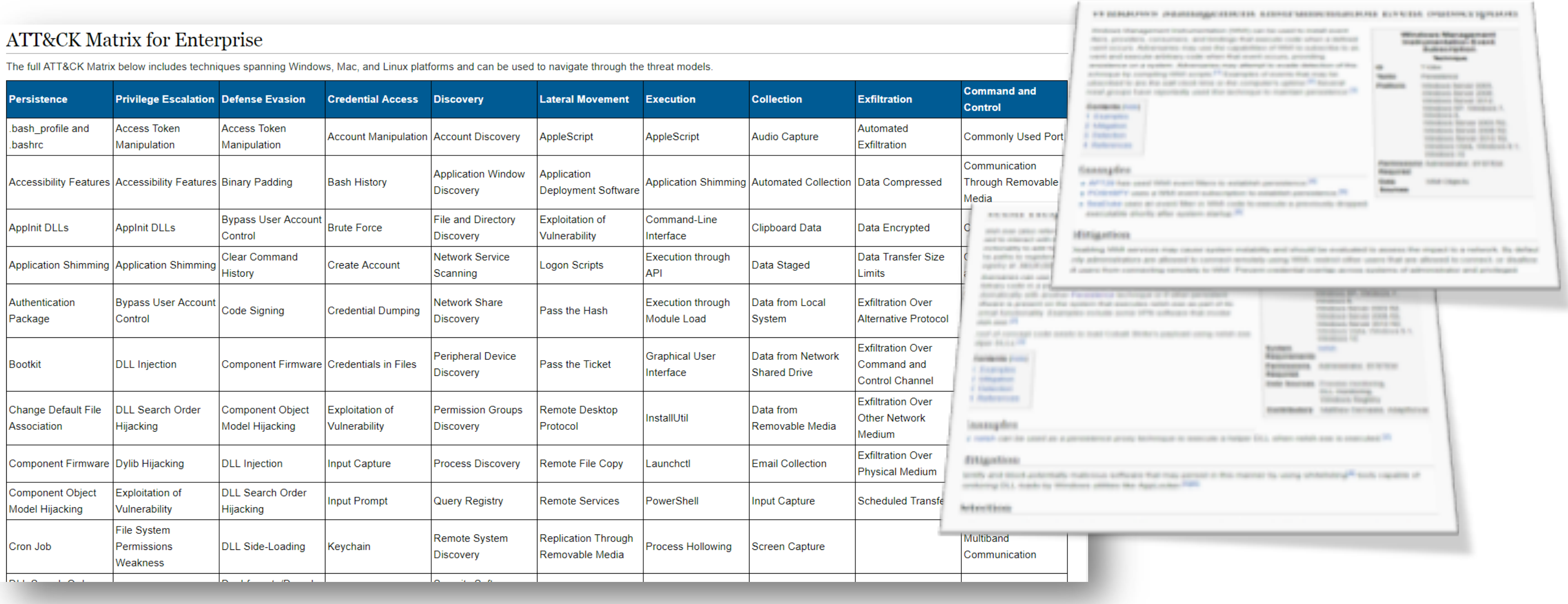
TTP-BASED DETECTS



executing_hta_via_com
wecloud[.]biz/d.doc
wecloud[.]biz/m11.xls
download
1-day .rtf exploit
winword
download
AppData\Roaming\22682.doc
ex
suspicious_powershell_cmdline_downloading
start
mshta
start
powershell
open
executing_with_nonexecutable_extension
start
start
suspicious_powershell_cmd_or_script_spawning
odbcconf
powershell
download
execute
decode,store,start
wecloud[.]biz/p1.sqlite3
AppData\Roaming\46961.txt (.dll)
proxying_arbitrary_code_execution_through_trusted_binaries
AppData\Roaming\6F633FD53B9B6C.txt (sct)
start
cmd
start
ex
suspicious_powershell_cmdline_general_obfuscation
regsvr32
execute
wecloud[.]biz/mail/changelog.txt
application_whitelisting_bypass_via_regsvr32
start
drop
cmd
execute
AV_engine_inexact_detect
AppData\Roaming\rad7EF08.tmp
start base-64 PS
Cobaltstrike beacon
start
powershell

KASPERSKY lab

MITRE ATT&CK: ADVERSARIAL TACTICS, TECHNIQUES & COMMON KNOWLEDGE



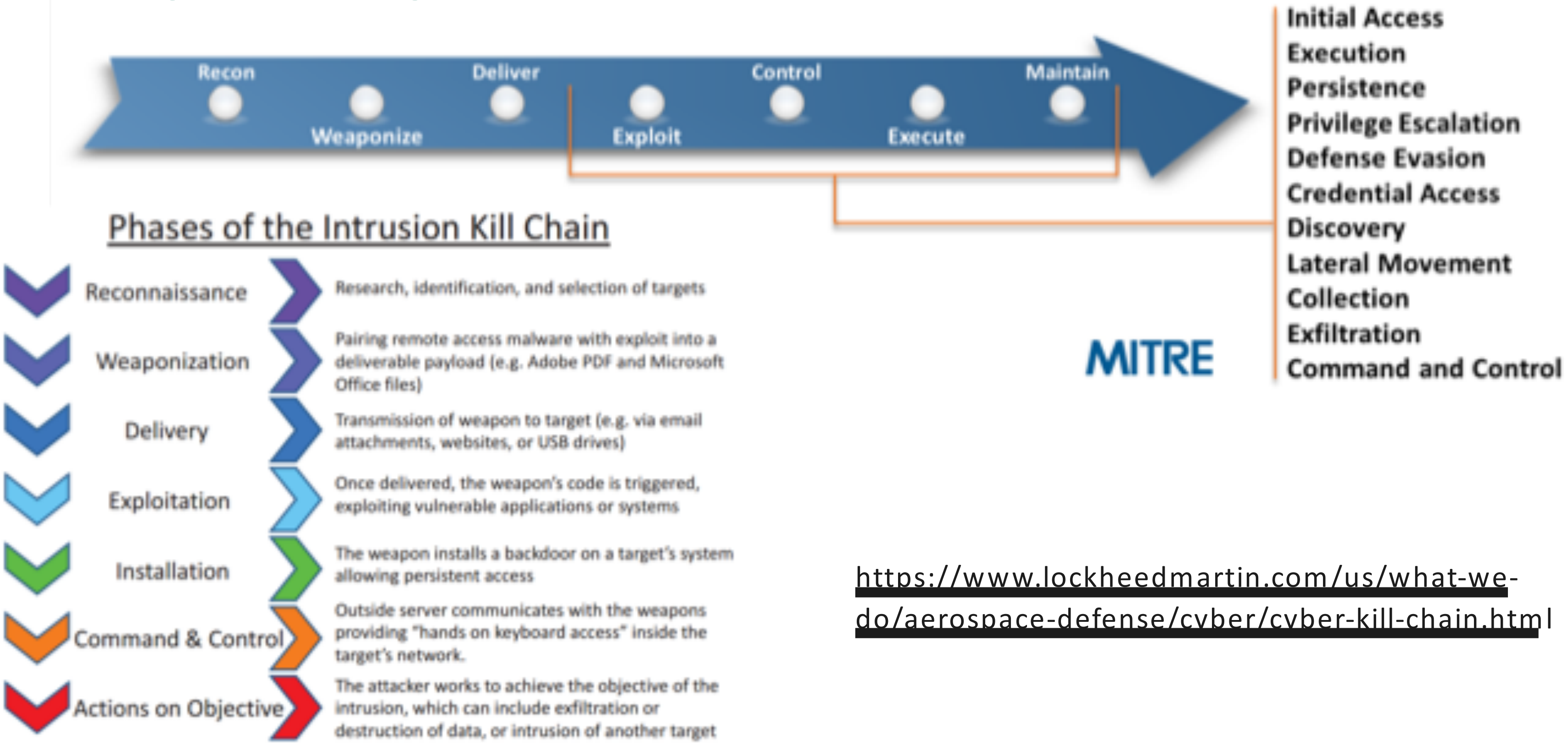
ATT&CK Matrix for Enterprise

The full ATT&CK Matrix below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the threat models.

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Application Shimming	Automated Collection	Data Compressed	Communication Through Removable Media
AppInit DLLs	AppInit DLLs	Bypass User Account Control	Brute Force	File and Directory Discovery	Exploitation of Vulnerability	Command-Line Interface	Clipboard Data	Data Encrypted	C
Application Shimming	Application Shimming	Clear Command History	Create Account	Network Service Scanning	Logon Scripts	Execution through API	Data Staged	Data Transfer Size Limits	C
Authentication Package	Bypass User Account Control	Code Signing	Credential Dumping	Network Share Discovery	Pass the Hash	Execution through Module Load	Data from Local System	Exfiltration Over Alternative Protocol	
Bootkit	DLL Injection	Component Firmware	Credentials in Files	Peripheral Device Discovery	Pass the Ticket	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	
Change Default File Association	DLL Search Order Hijacking	Component Object Model Hijacking	Exploitation of Vulnerability	Permission Groups Discovery	Remote Desktop Protocol	InstallUtil	Data from Removable Media	Exfiltration Over Other Network Medium	
Component Firmware	Dylib Hijacking	DLL Injection	Input Capture	Process Discovery	Remote File Copy	Launchctl	Email Collection	Exfiltration Over Physical Medium	
Component Object Model Hijacking	Exploitation of Vulnerability	DLL Search Order Hijacking	Input Prompt	Query Registry	Remote Services	PowerShell	Input Capture	Scheduled Transfe	
Cron Job	File System Permissions Weakness	DLL Side-Loading	Keychain	Remote System Discovery	Replication Through Removable Media	Process Hollowing	Screen Capture		Multiband Communication

https://attack.mitre.org/wiki/Main_Page

ATTACK KILL CHAIN



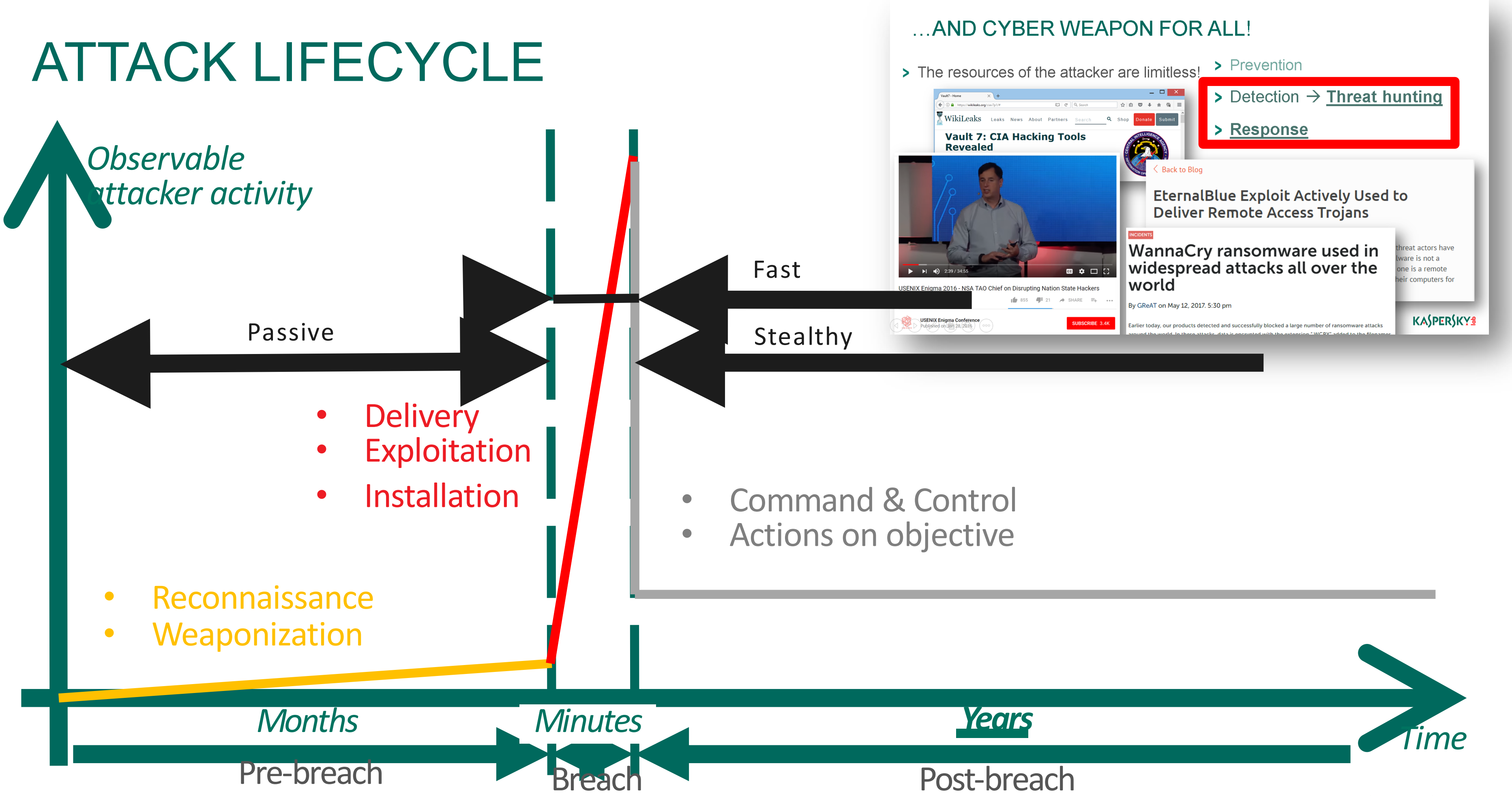
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control

Phases of the Intrusion Kill Chain

Reconnaissance	Research, identification, and selection of targets
Weaponization	Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)
Delivery	Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)
Exploitation	Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems
Installation	The weapon installs a backdoor on a target's system allowing persistent access
Command & Control	Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network.
Actions on Objective	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

ATTACK LIFECYCLE



Observable attacker activity

Passive

Fast

Stealthy

- Delivery
- Exploitation
- Installation

- Command & Control
- Actions on objective

- Reconnaissance
- Weaponization

Months

Minutes

Years

Time

Pre-breach

Breach

Post-breach

…AND CYBER WEAPON FOR ALL!

- The resources of the attacker are limitless!

- Prevention
- Detection → Threat hunting
- Response

WikiLeaks

Vault 7: CIA Hacking Tools Revealed

USENIX Enigma 2016 - NSA TAO Chief on Disrupting Nation State Hackers

USENIX Enigma Conference

Back to Blog

EternalBlue Exploit Actively Used to Deliver Remote Access Trojans

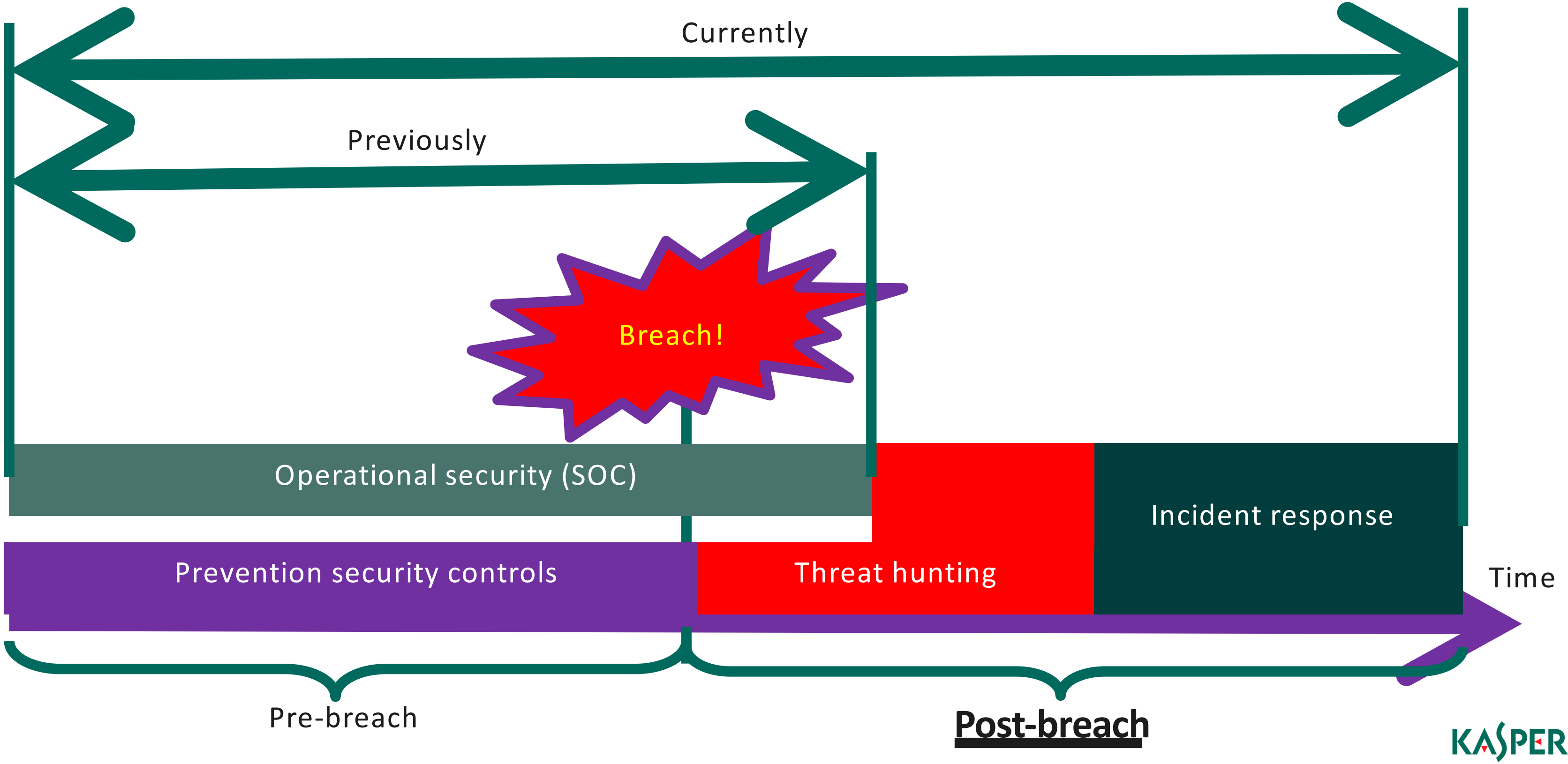
INCIDENTS

WannaCry ransomware used in widespread attacks all over the world

By GReAT on May 12, 2017. 5:30 pm

Earlier today, our products detected and successfully blocked a large number of ransomware attacks

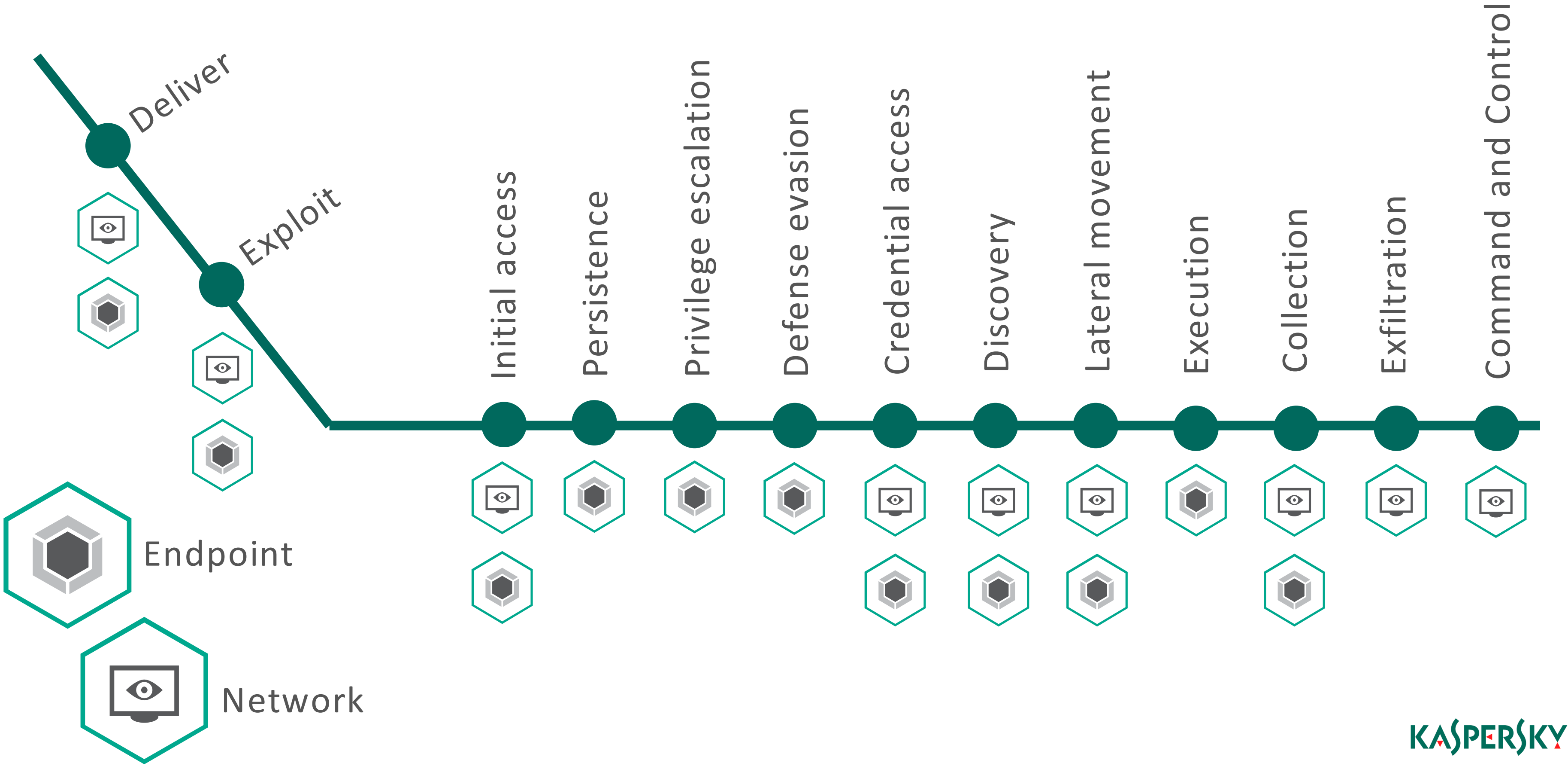
ATTACK KILL CHAIN COVERAGE: PRE-BREACH AND POST-BREACH SCENARIOS



POST-BREACH: MITRE ATT&CK COVERAGE

- **Consumer**: the most appropriate way to assess EDR/MDR
- **Vendor/Provider**: Self-assessment for current capabilities and improvement planning

MEDIA COVERAGE



Deliver

Exploit

Initial access

Persistence

Privilege escalation

Defense evasion

Credential access

Discovery

Lateral movement

Execution

Collection

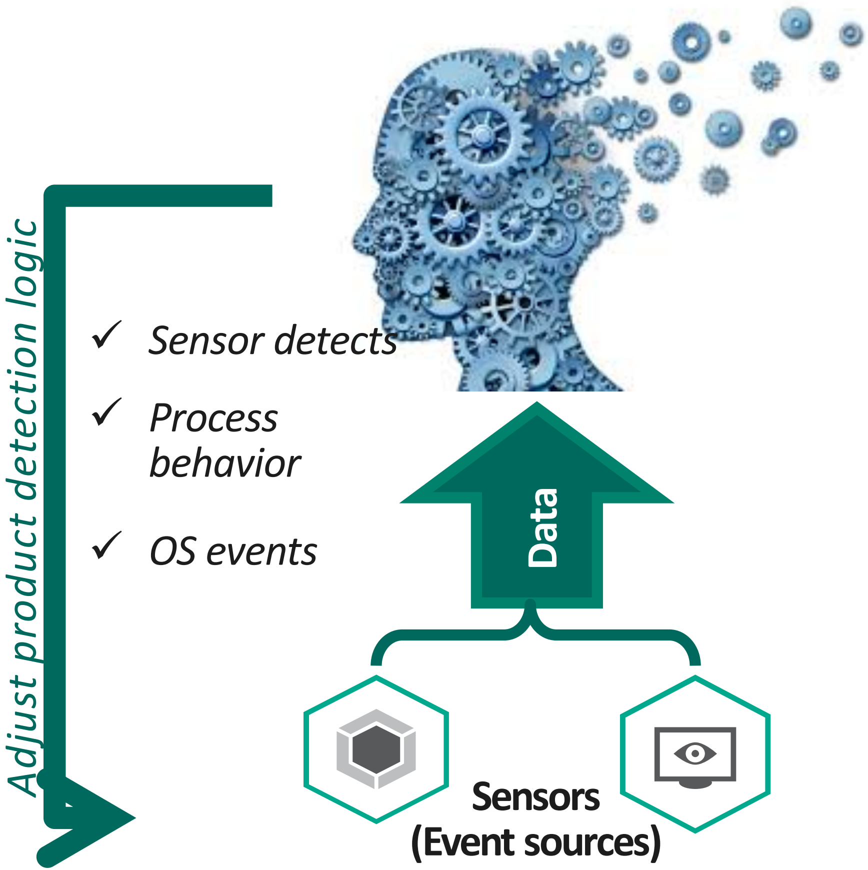
Exfiltration

Command and Control

Endpoint

Network

LEVELS OF DECISION MAKING



- ✓ *Sensor detects*
- ✓ *Process behavior*
- ✓ *OS events*

Sensors (Event sources)

Human analyst work, Threat hunting:

- ✓ Check behavior hypotheses about attacker
- ✓ Situational awareness
- ✓ Investigate borderline cases
- ✓ Overall process improvement

Macro correlation, TTP-based detection logic:

- ✓ All **TTP** knowledge:
  - ✓ Internal research
  - ✓ MITRE ATT&CK
  - ✓ Security assessment/Red teaming
  - ✓ Incident response practice
  - ✓ Monitoring practice

Cloud

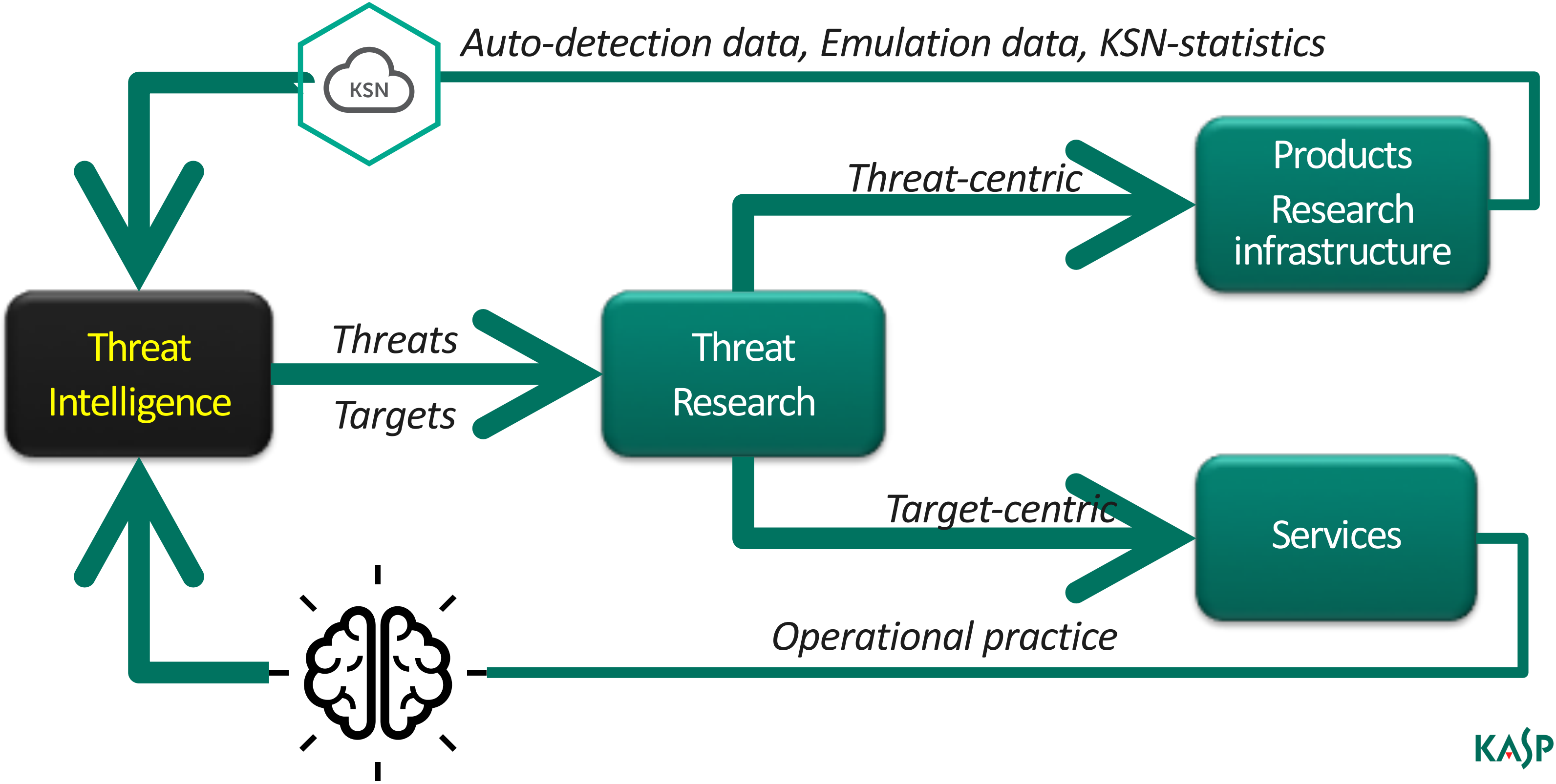
Micro correlation on sensor level:

- ✓ All sensor detection technologies
- ✓ Reputation (cloud)

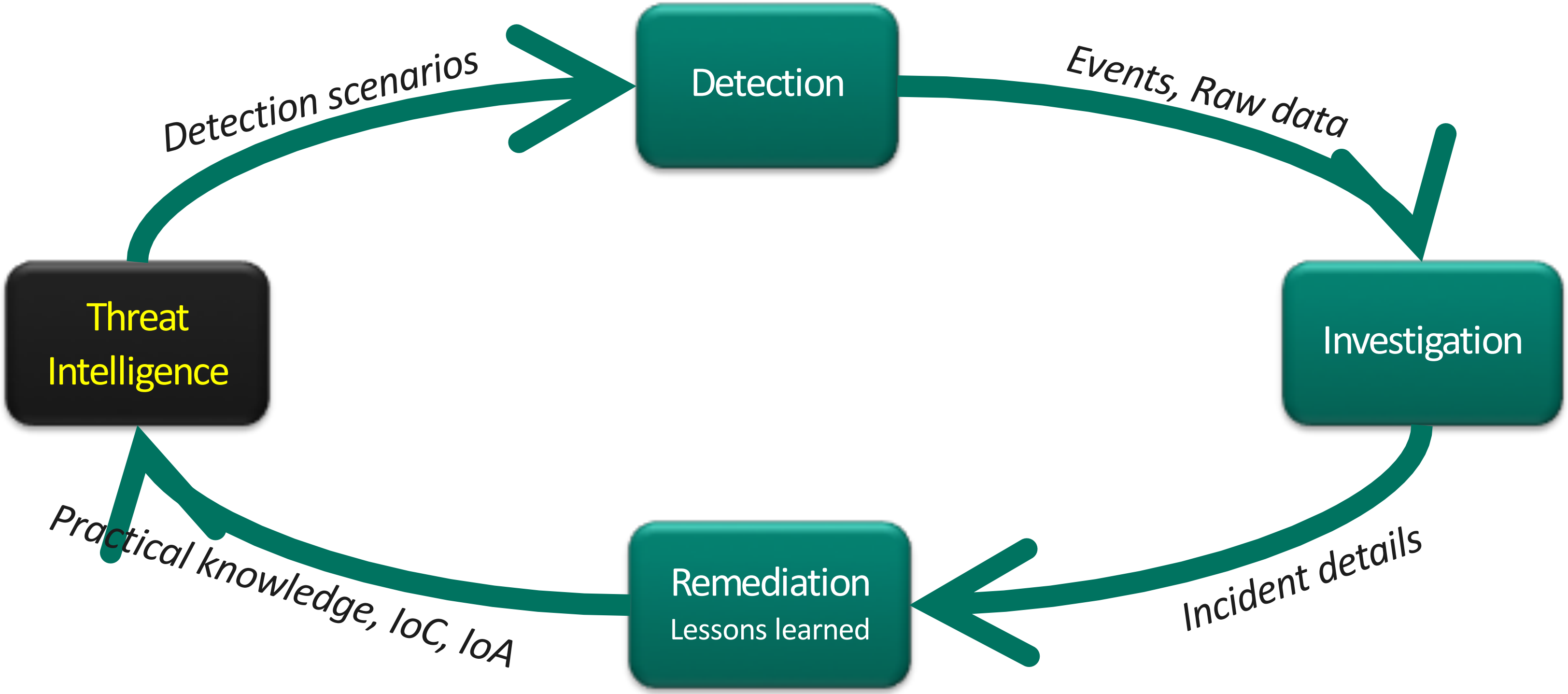
Products

CYCLES

THREAT INTELLIGENCE CYCLE FOR CONSTANT IMPROVEMENT



SECURITY OPERATIONS CYCLE (SIMPLIFIED)

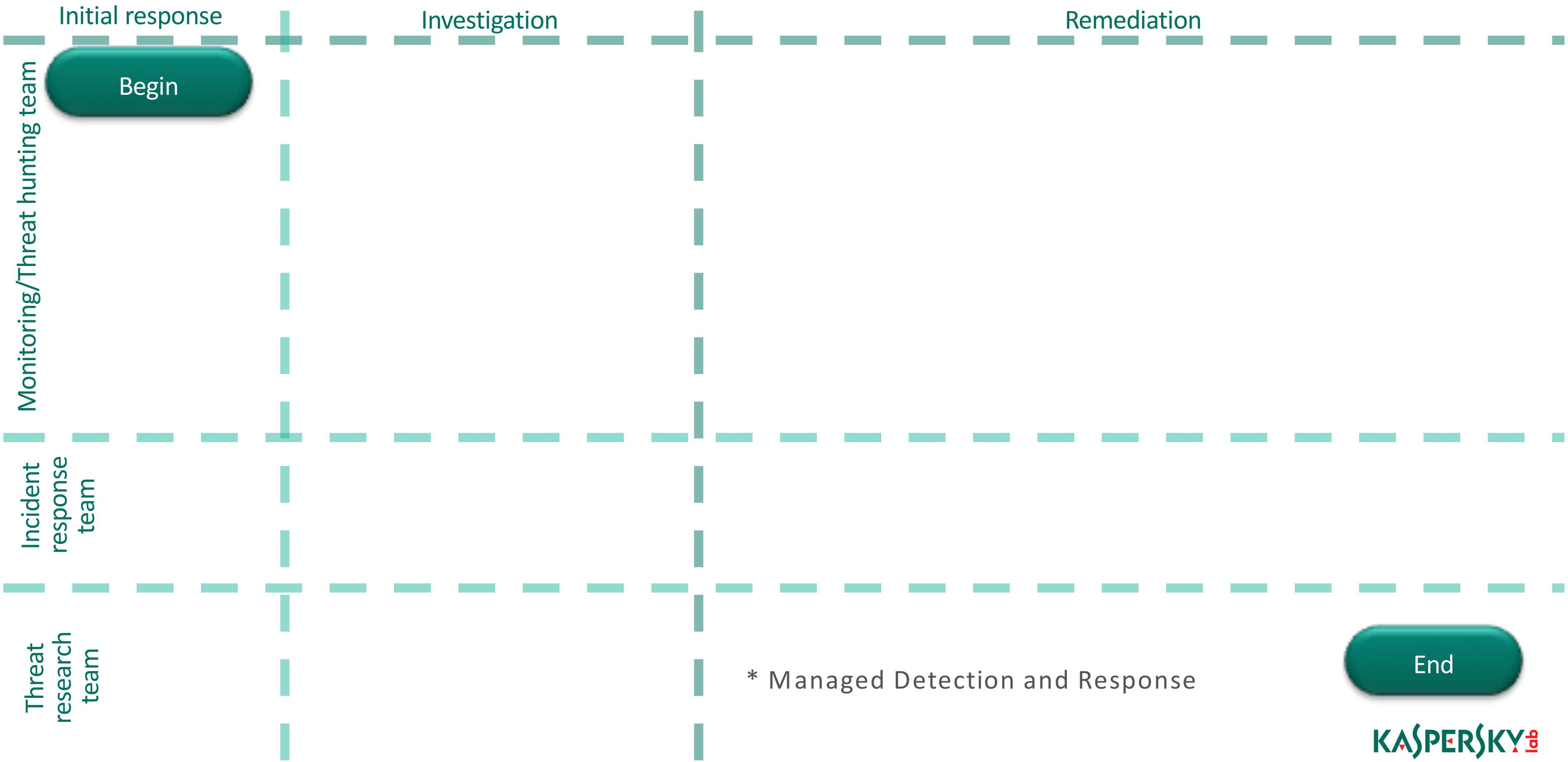


OFF-TOPIC: WHAT IS TI AND FOR WHOM IT MATTERS

	IT Roles	Tasks	Problems	Value of TI
Tactical level	Network operation center (NOC)	Feed indicators to security products	Bad indicators cause FP	Validate and prioritize indicators
	Security operations center (SOC)	Monitor, triage	Too many alerts to investigate (+ FN)	Prioritize alerts
	Infrastructure operations (IT)	Patch vulnerable systems	Difficult to prioritize patches	Prioritize patches
Operational level	IR Team	Remediate Determine details of attacks Hunt for additional breaches	Time-consuming to reconstruct attack from initial indicators	Provide context to reconstruct attack quickly
	SOC Team		Difficult to identify additional breaches	Provide data for threat hunting
Strategic level	CISO	Allocate resources	No clear priorities for investment	Priorities based on risks and likely attacks
	CIO	Communicate to executives	Executives don’t understand tech	Explain adversary in terms of impact

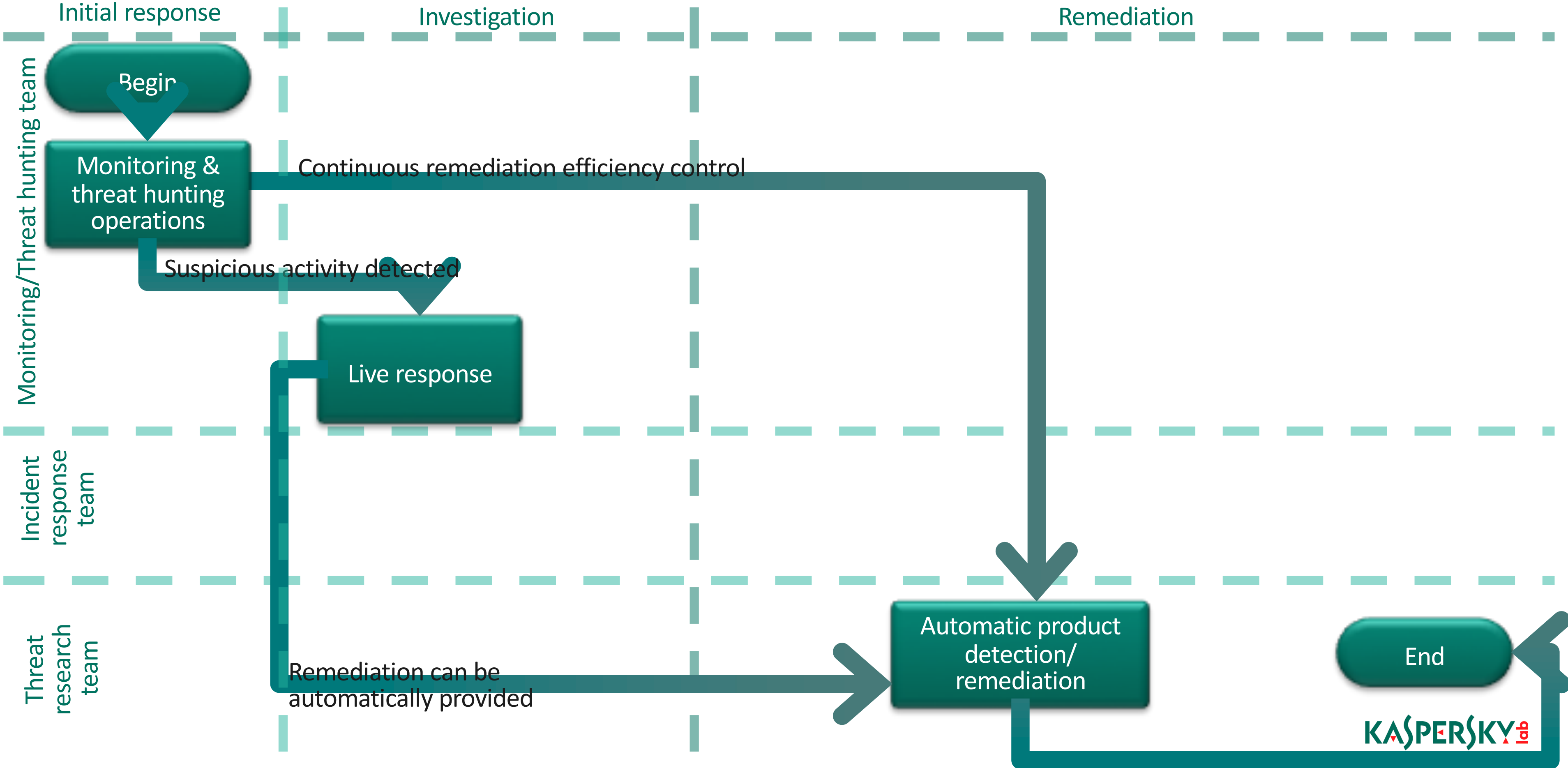
Source: John Friedman, Mark Bouchard, CISSP. Definitive Guide to Cyber Threat Intelligence. CyberEdge Group, LLC, 2015

INCIDENT RESPONSE IN MDR*



* Managed Detection and Response

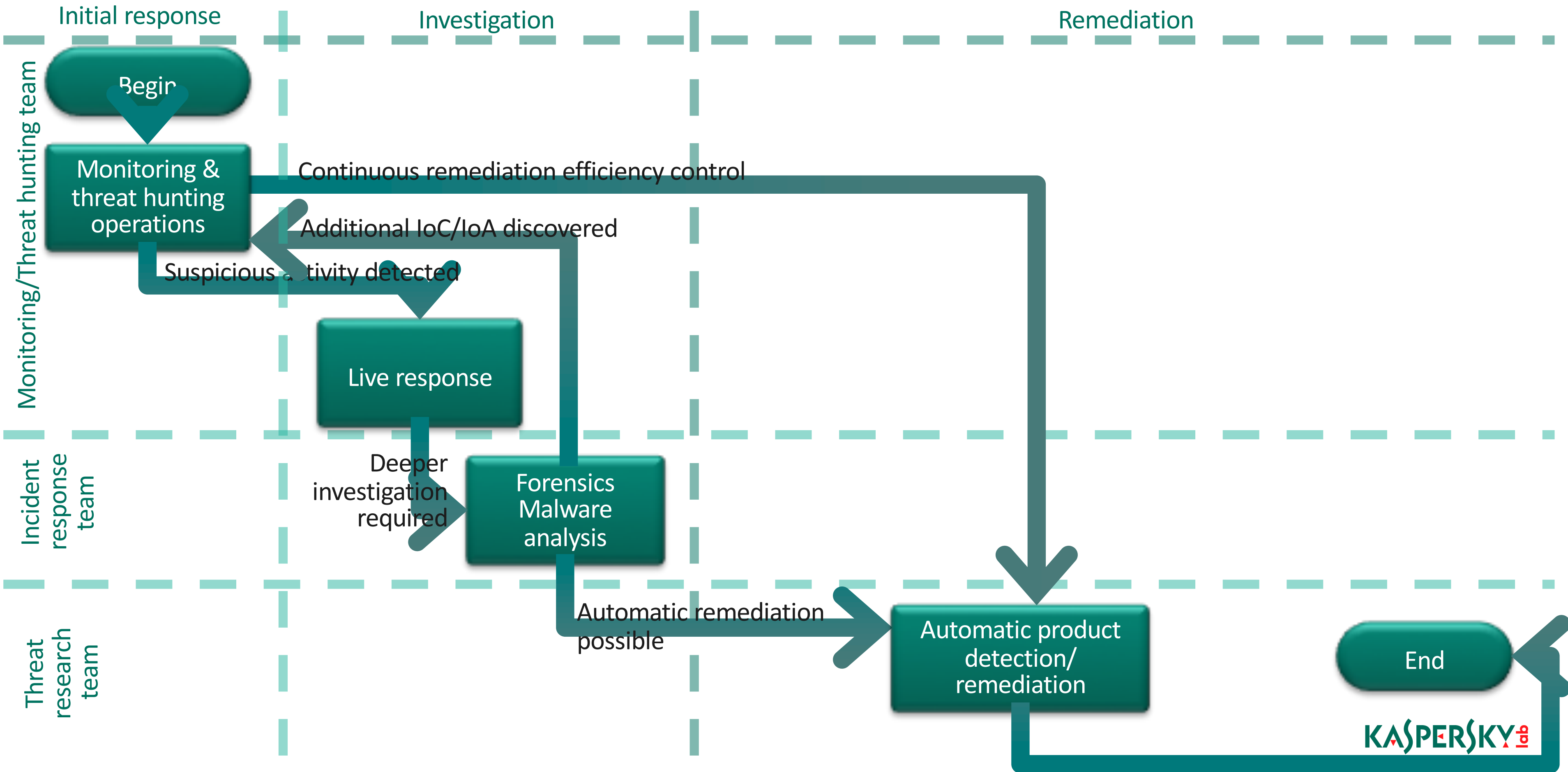
INCIDENT RESPONSE IN MDR



Initial response
Investigation
Remediation
Monitoring/Threat hunting team
Incident response team
Threat research team
Begin
Monitoring & threat hunting operations
Continuous remediation efficiency control
Suspicious activity detected
Live response
Remediation can be automatically provided
Automatic product detection/ remediation
End

KASPERSKY lab

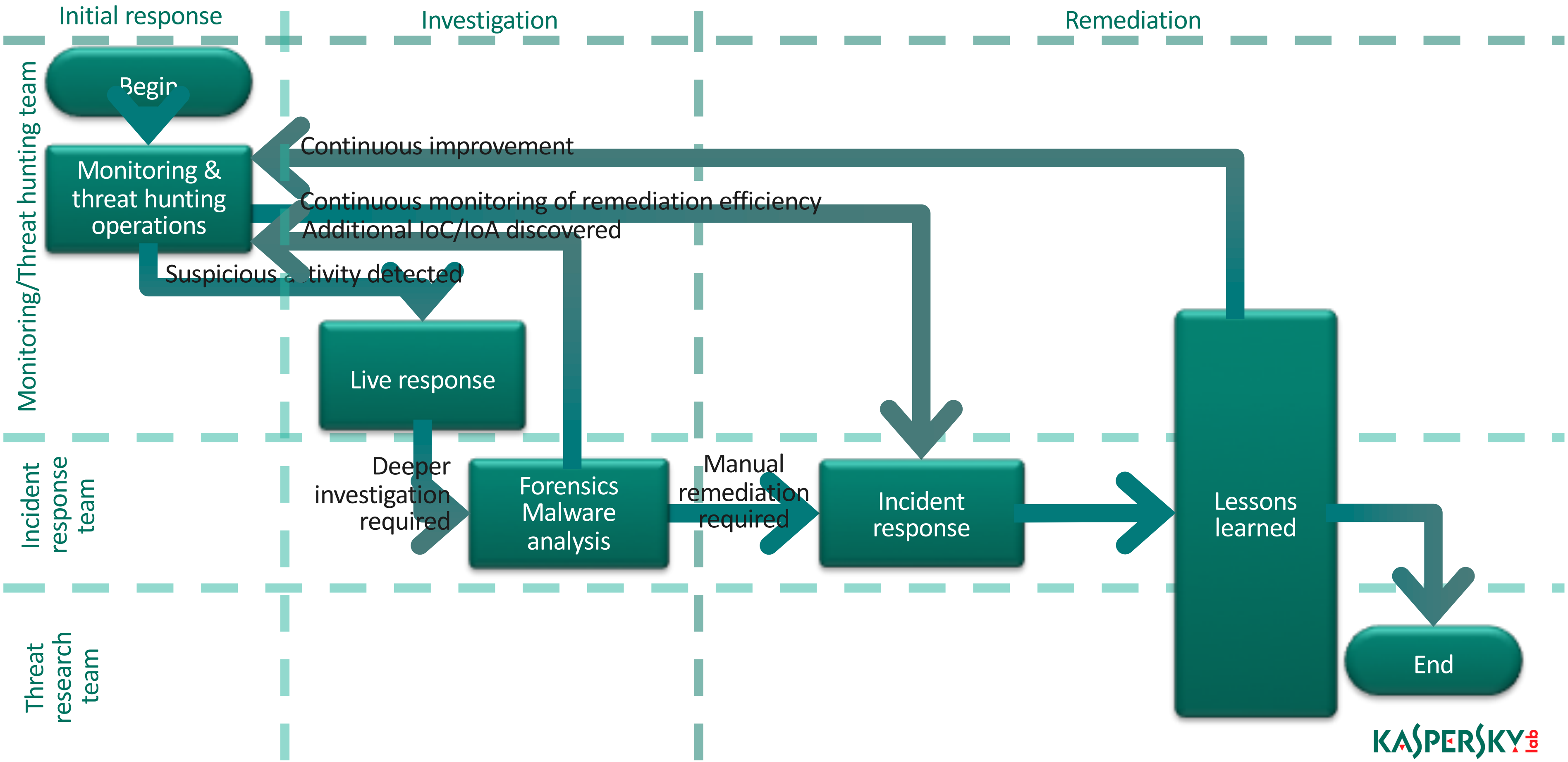
INCIDENT RESPONSE IN MDR



Initial response
Investigation
Remediation
Monitoring/Threat hunting team
Incident response team
Threat research team
Begin
Monitoring & threat hunting operations
Continuous remediation efficiency control
Additional IoC/IoA discovered
Suspicious activity detected
Live response
Deeper investigation required
Forensics Malware analysis
Automatic remediation possible
Automatic product detection/ remediation
End

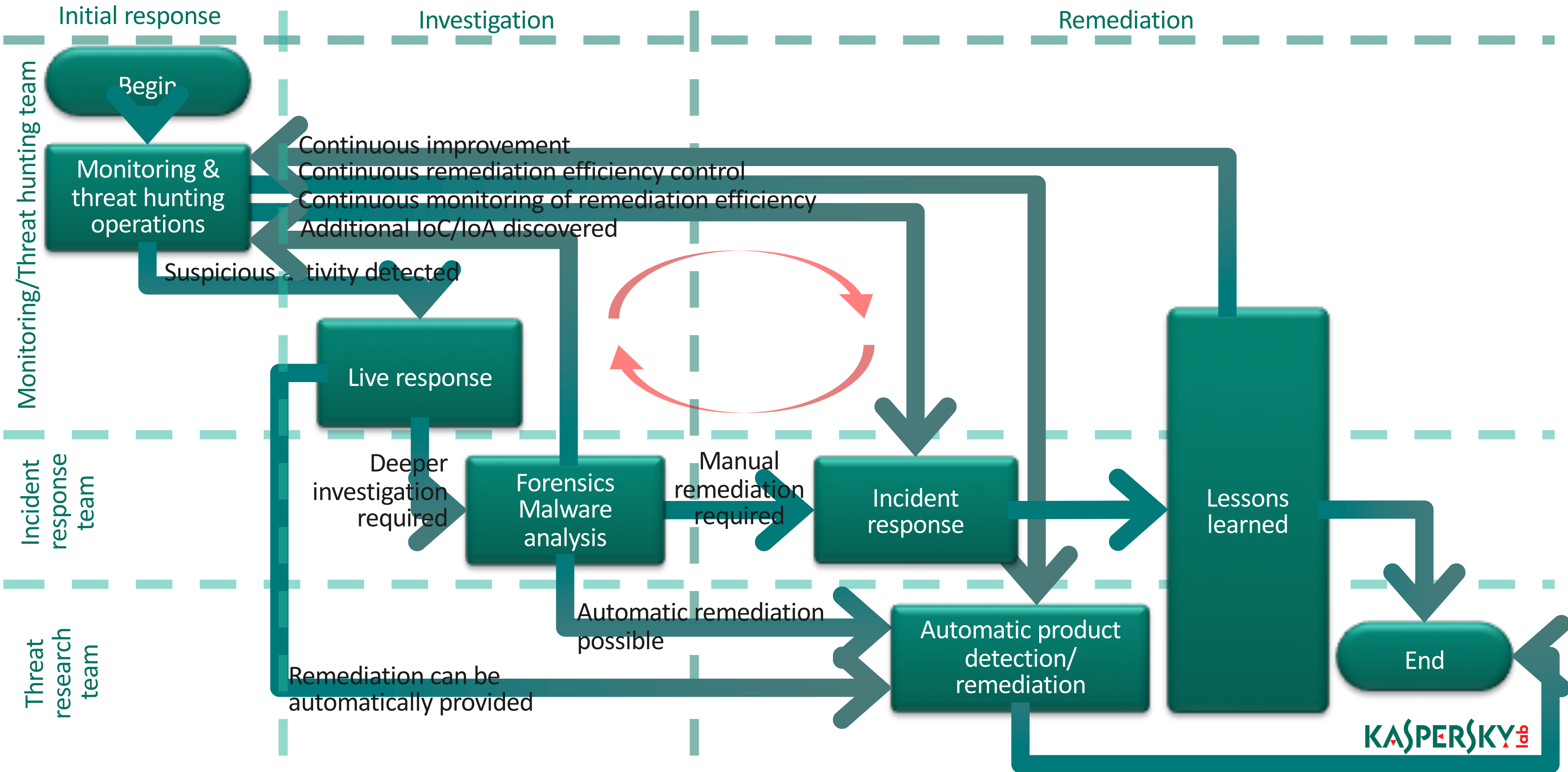
KASPERSKY lab

INCIDENT RESPONSE IN MDR


Initial response
Investigation
Remediation
Monitoring/Threat hunting team
Incident response team
Threat research team
Begin
Monitoring & threat hunting operations
Continuous improvement
Continuous monitoring of remediation efficiency
Additional IoC/IoA discovered
Suspicious activity detected
Live response
Deeper investigation required
Forensics Malware analysis
Manual remediation required
Incident response
Lessons learned
End

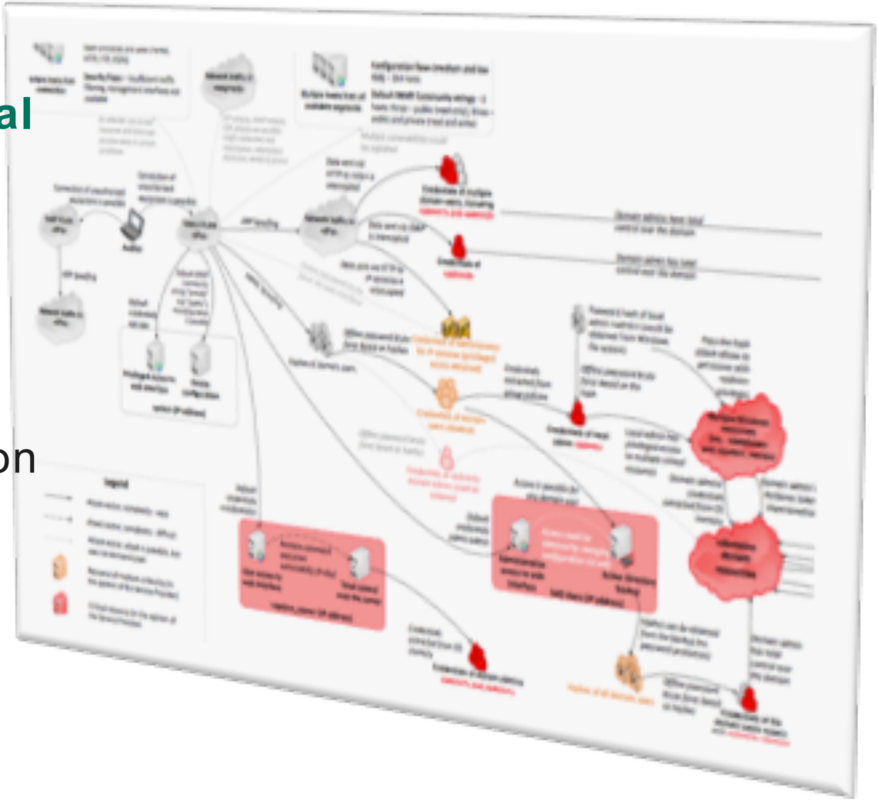
KASPERSKY lab

INCIDENT RESPONSE IN MDR

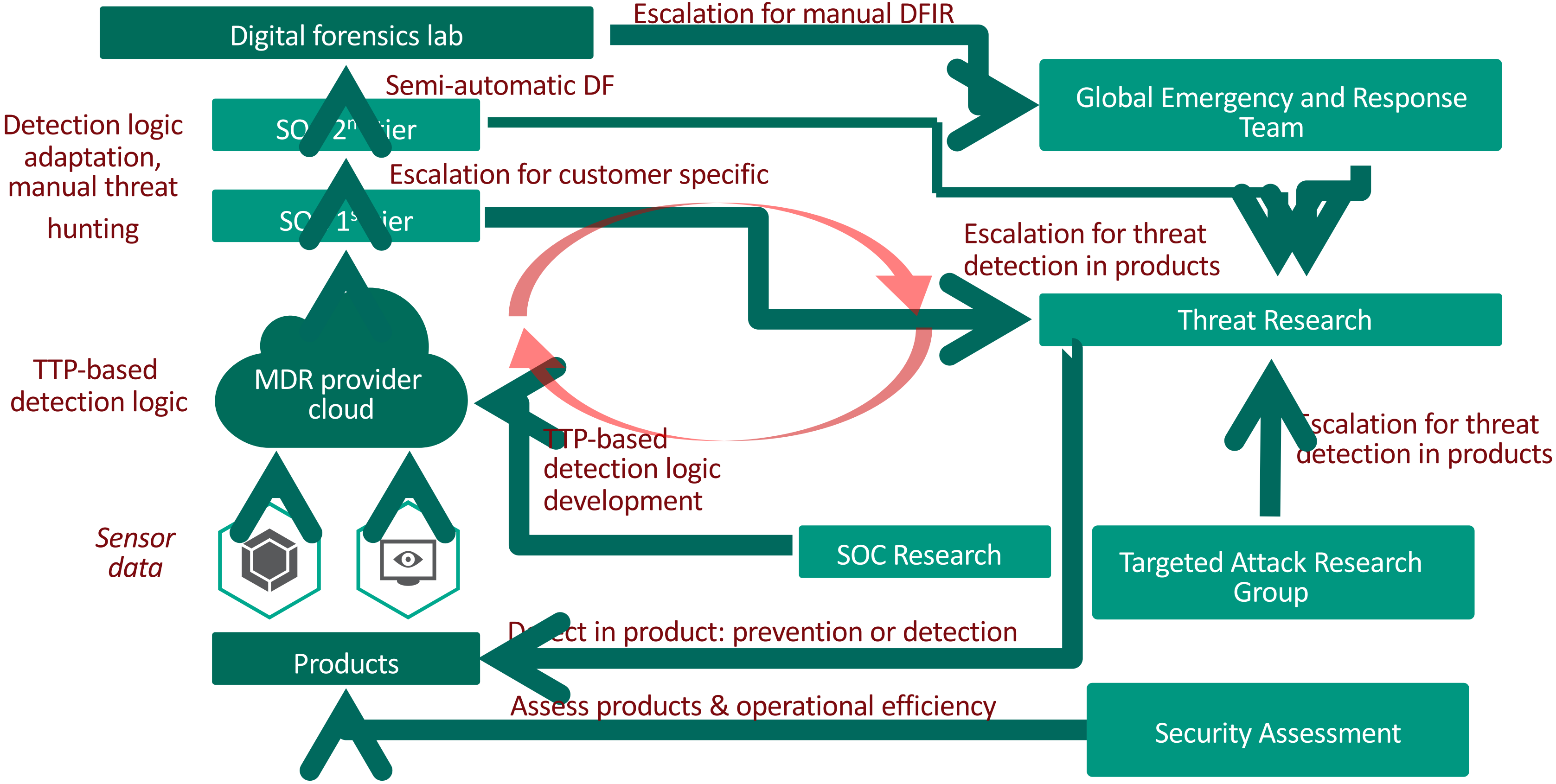

Initial response
Investigation
Remediation
Monitoring/Threat hunting team
Incident response team
Threat research team
Begin
Monitoring & threat hunting operations
Continuous improvement
Continuous remediation efficiency control
Continuous monitoring of remediation efficiency
Additional IoC/IoA discovered
Suspicious activity detected
Live response
Deeper investigation required
Forensics Malware analysis
Manual remediation required
Incident response
Lessons learned
Automatic remediation possible
Remediation can be automatically provided
Automatic product detection/ remediation
End
KASPERSKY lab

ADVERSARY EMULATION FOR SECURITY OPERATIONS (“RED TEAMING”)

- Goal: Assessment of **Blue team operational efficiency** and **training**
- **Threat Intelligence driven**
  - Leaks, spear-phishing, insiders, etc.
- Report **artifacts** for Blue team evaluation
  - Detailed stage by stage attack description
  - With timestamps, tools
  - IoCs & IoAs
  - TTPs
- Optionally followed with **workshop**
  - With KL Blue team threat hunters (temporary Purple)



RESEARCH AS OPERATIONS



Digital forensics lab

Escalation for manual DFIR

Global Emergency and Response Team

Semi-automatic DF

SOC 2nd tier

Detection logic adaptation, manual threat hunting

Escalation for customer specific

SOC 1st tier

Escalation for threat detection in products

Threat Research

TTP-based detection logic

MDR provider cloud

TTP-based detection logic development

Escalation for threat detection in products

Sensor data

SOC Research

Targeted Attack Research Group

Defect in product: prevention or detection

Products

Assess products & operational efficiency

Security Assessment

THE END: THE IDEA OF ‘CYBER-IMMUNITY’

- If somebody planned to breach your systems, it will definitely happen
- If we eradicated them, they will come again - they never give up
- Do not rely solely on the perimeter and automatic detection/protection
- Chances to detect after the breach are much higher
- Prioritization on the material risk is the basis of success
- Never relax: silence is a scary sound – assume breach, search, hunt

http://reply-to-all.blogspot.com/2017/07/blog-post_28.html

THANK YOU VERY MUCH!

Sergey Soldatov, CISA, CISSP

Head of SOC, R&D Security Services, Kaspersky lab

intelligence@kaspersky.com

www.kaspersky.ru