



Threat Hunting

Tu mejor arma para evitar tu próximo gran incidente de ransomware (¡y otros!)

Readiness · Detection · Response

Index

What is Threat Hunting?

Intelligence at the Core

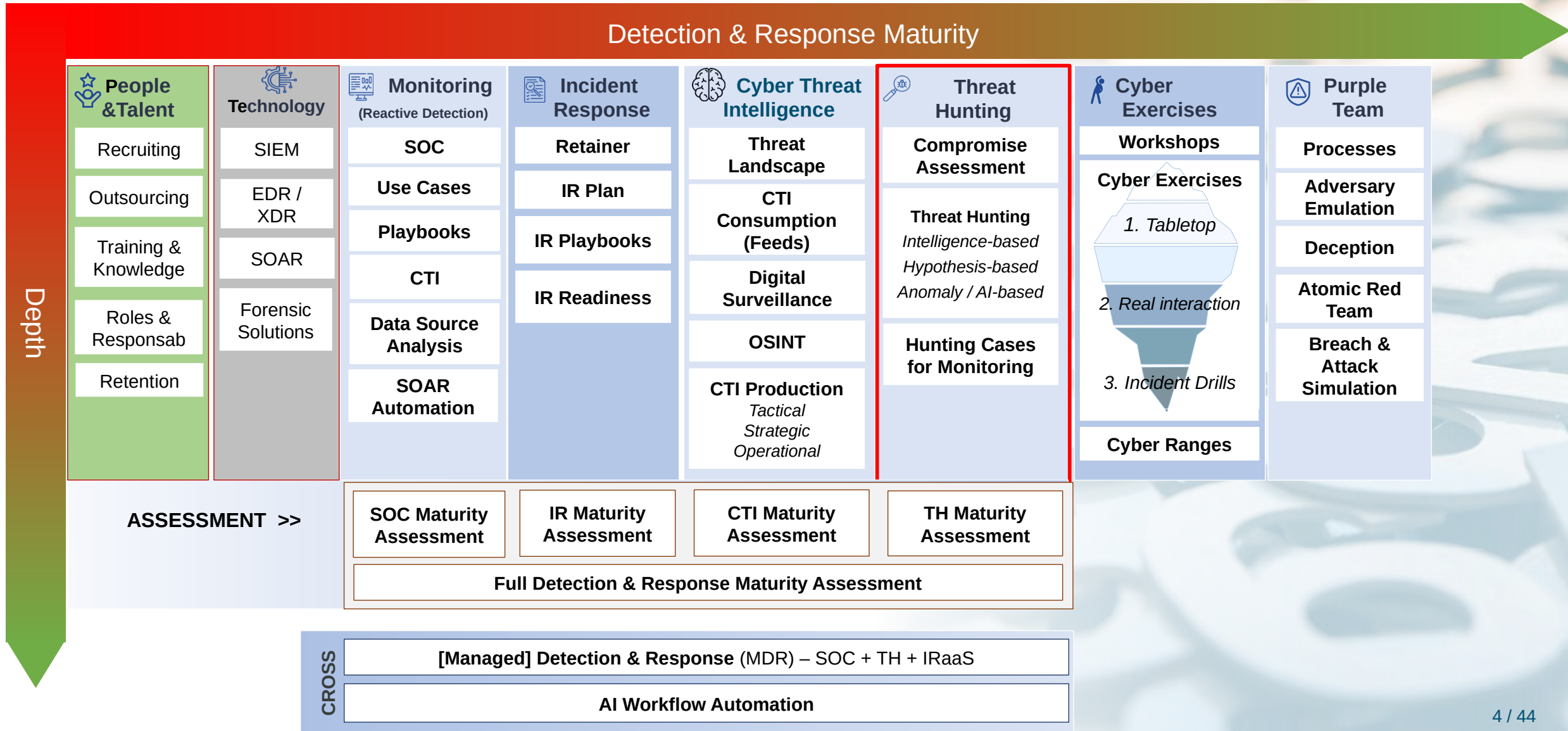
How Does Threat Hunting Work?

Summary. Why Can't You Live Without It?

How Can We Help You?

What is Threat Hunting?

Where Does Threat Hunting Fit?



What is Threat Hunting (TH)?

The goal of threat hunting is not only to find more security incidents but to **improve automated detection capabilities over time**. David Bianco.

To catch intrusions in progress, rather than after attackers have completed their objectives and done worse damage to the organization. SANS Institute.

Threat Hunting = Incident Response – Incident

Threat Hunting is all about Proactive Detection

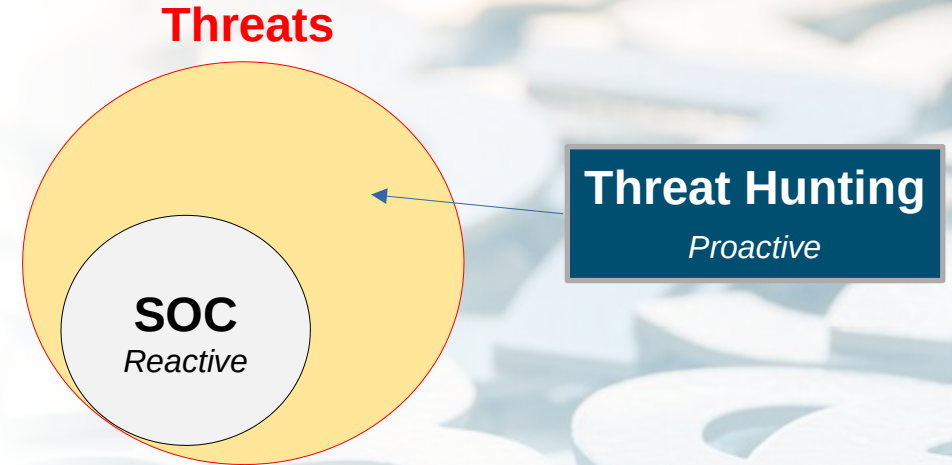
What is Threat Hunting (TH)?

Able to detect unknown threats

Wide variety of TTP and Threats covered

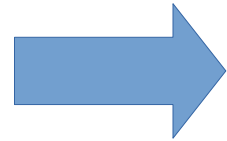
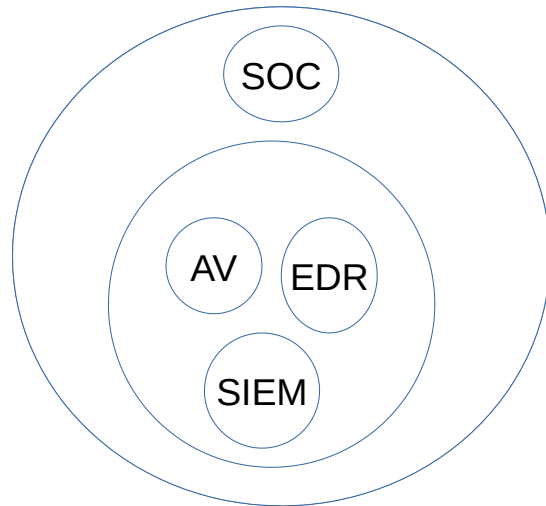
Intelligence-driven

Focus on what cannot be detected by other means



Why is Threat Hunting Necessary?

Detection

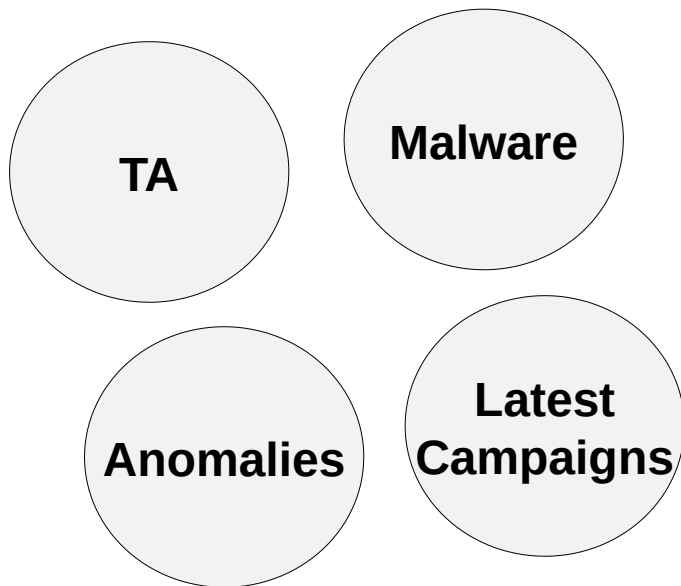


Security Incidents

What is wrong with this strategy?

Reactive Detection

What you think you are detecting



VS

What you are detecting



Reactive Detection

Reactive detection problems:

- Based on alerts.
- High technology dependency.
- High False Positives rate.
- Threat Actors know how to bypass a SOC.

Proactive Detection: Threat Hunting



TH gives you the protection you think you already have (but you don't)

Some Real Statistics

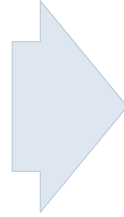
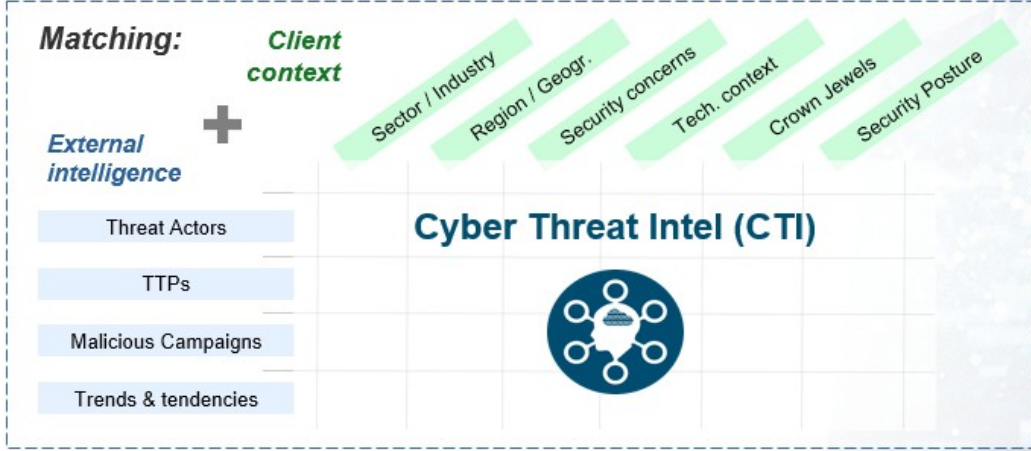
Attacks that cannot be detected by reactive detection are exponentially growing. E.g: interactive intrusions have grown 55% in the last year (CrowdStrike)

Ransomware, the main threat nowadays, is the **Top 2 threat that hunters detect** in a daily basis (SANS)

Resources spent on **remediation are reduced 39%** in organizations doing Threat Hunting (SANS)

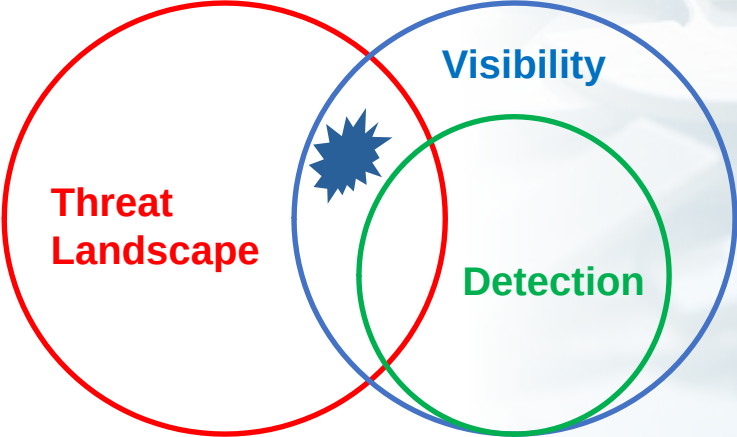
Intelligence at the Core

Close Up: CTI



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
External access via phishing	Process execution	Registry modification	Local administrator	Process execution	Remote desktop	Network discovery	Local administrator	Local administrator	Local administrator	Local administrator	Local administrator

TH



MITRE
ATT&CK™

Now, We Know Who is Going To Attack You

The World has Changed: Threat Intelligence



And We Also Know How They Will Attack You



Tactic	Technique ID	Technique
TA0001 - Initial Access	T1566	Phishing
TA0006 - Credential Access	T1003	Credential Dumping
TA0004 - Privilege Escalation	T1068	Exploitation for Privilege Escalation
TA0007 - Discovery	T1082	System Information Discovery

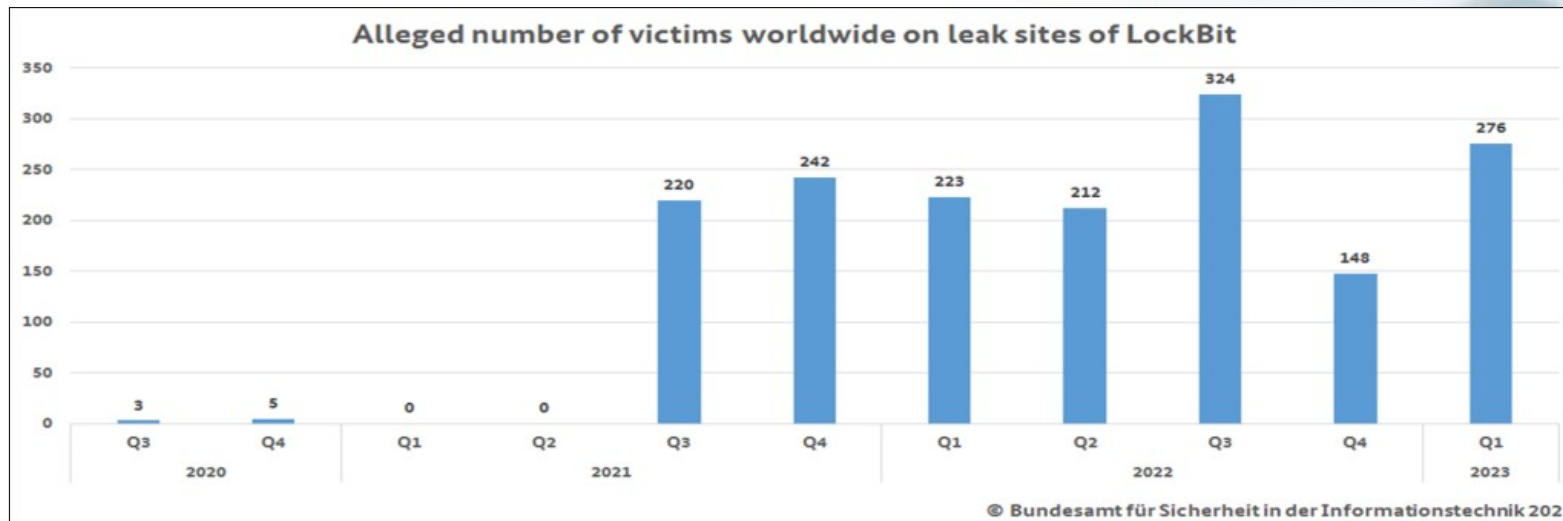
How Does Threat Hunting Work?

Use Case: Lockbit

Top 3 Ransomware.
>250% in 2022

Continuous Evolution
New tools -> new detections

LATAM / EMEA / NA
Main targets

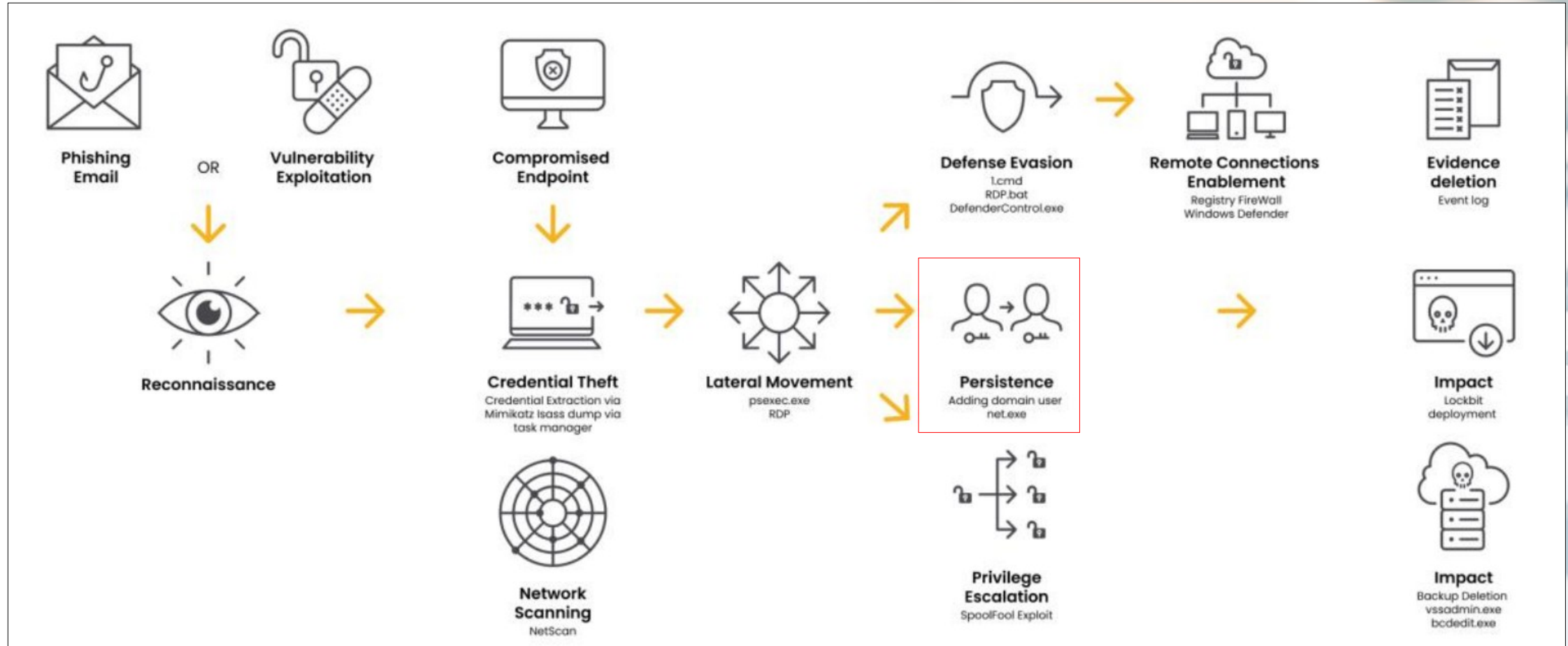


References with the information and graphs of this use case:

Logpoint: <https://www.logpoint.com/en/blog/hunting-lockbit-variations-using-logpoint/>

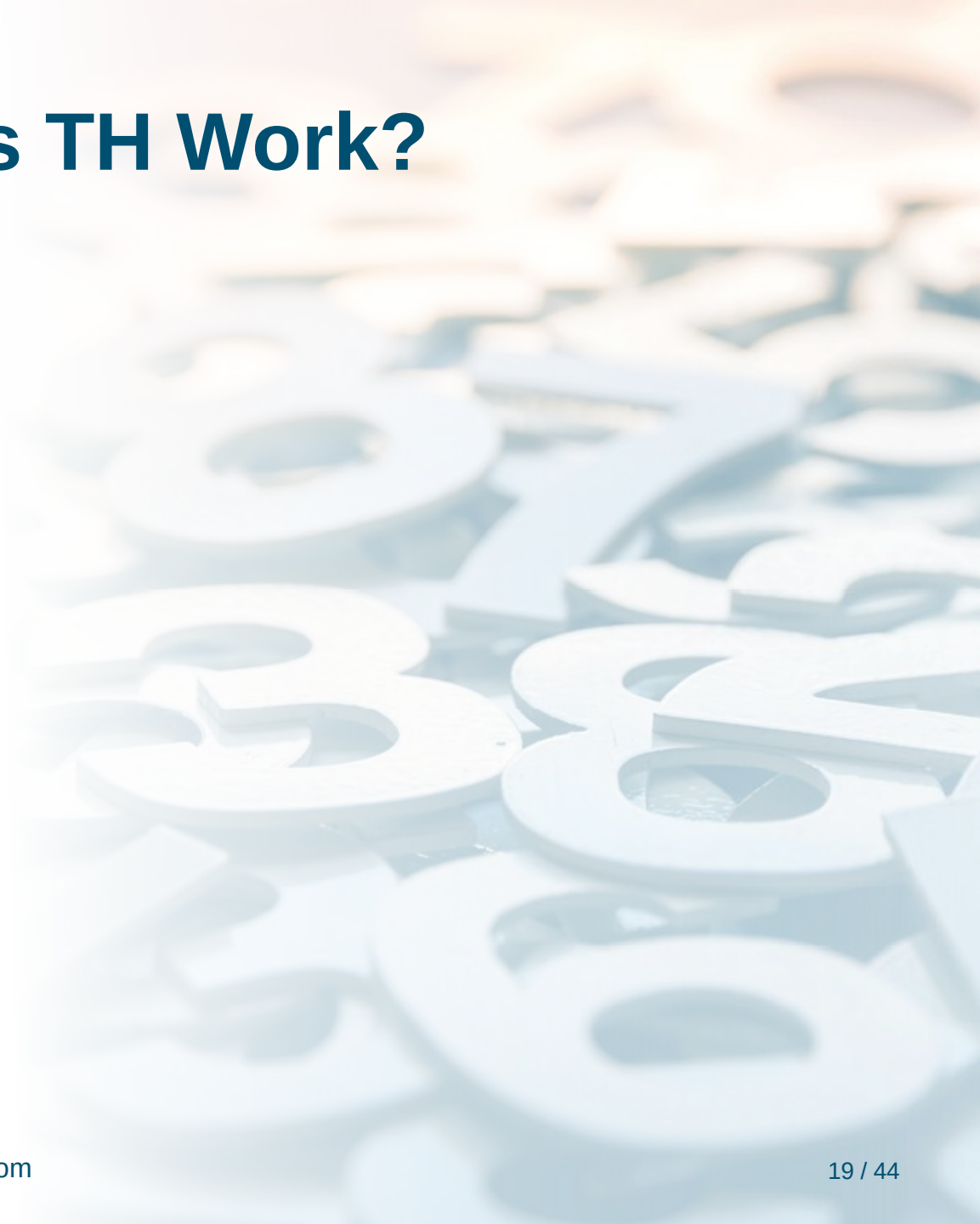
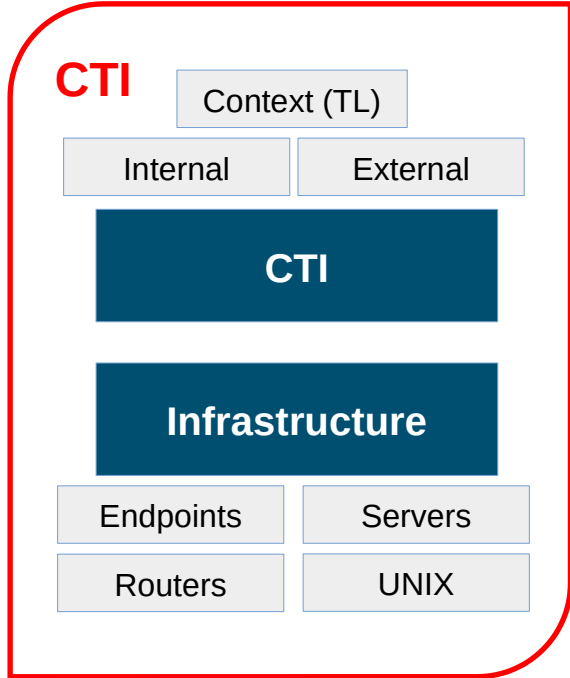
America's Cyber Defense Agency: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a>

Use Case: Lockbit



Extracted from Logpoint report about LockBit

How Does TH Work?



Internal Intelligence



External Intelligence



Infrastructure

Previous incidents, internal database...

Research about Lockbit: latest campaigns, latest IOA, reports...

e.g: <https://www.logpoint.com/en/blog/hunting-lockbit-variations-using-logpoint/>

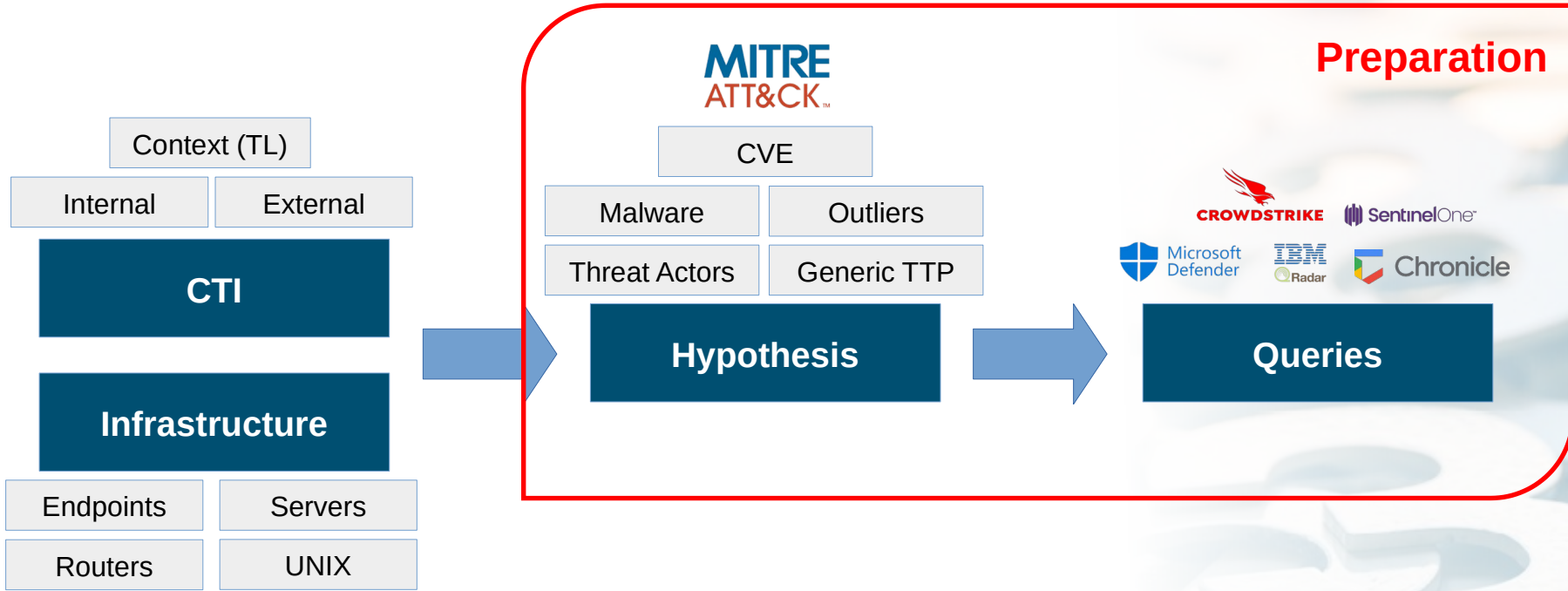
How can YOU detect this threat?

Hardware, tools...

- **Execution** - use of mshta.exe to execute LockBit masquerading as an HTML Application and through scheduled tasks.
- **Privilege Escalation** - User account control bypass via COM like cmlua.dll or cmstplua.dll. Using defender binary mpcmdrun.exe to side load malicious DLL.
- **Persistence** - modifying registry Run\RunOnce keys.
- **Defense Evasion** - Stops defender logging, disables real-time and tamper protection, uninstalls antivirus and malware protection like defender, third party vendor if present. The malware also cleans the event log and further prevents the writing of any new log.
- **Credential harvesting** - Enabling Wdigest authentication mechanism to easily retrieve clear text passwords.
- **Lateral Movement** - Enables RDP in the compromised system, psexec to remotely deploy malware
- **Exfiltration** - Utilizes Stealbit malware to exfiltrate.
- **Impact** - Deletes Shadow copy, modifies boot configuration data to disable auto recovery, and various services and tasks are killed before encryption.

**This information will be used
by TH Team**

How Does TH Work?



Queries Creation

Information from CTI is translated to hypothesis and queries.

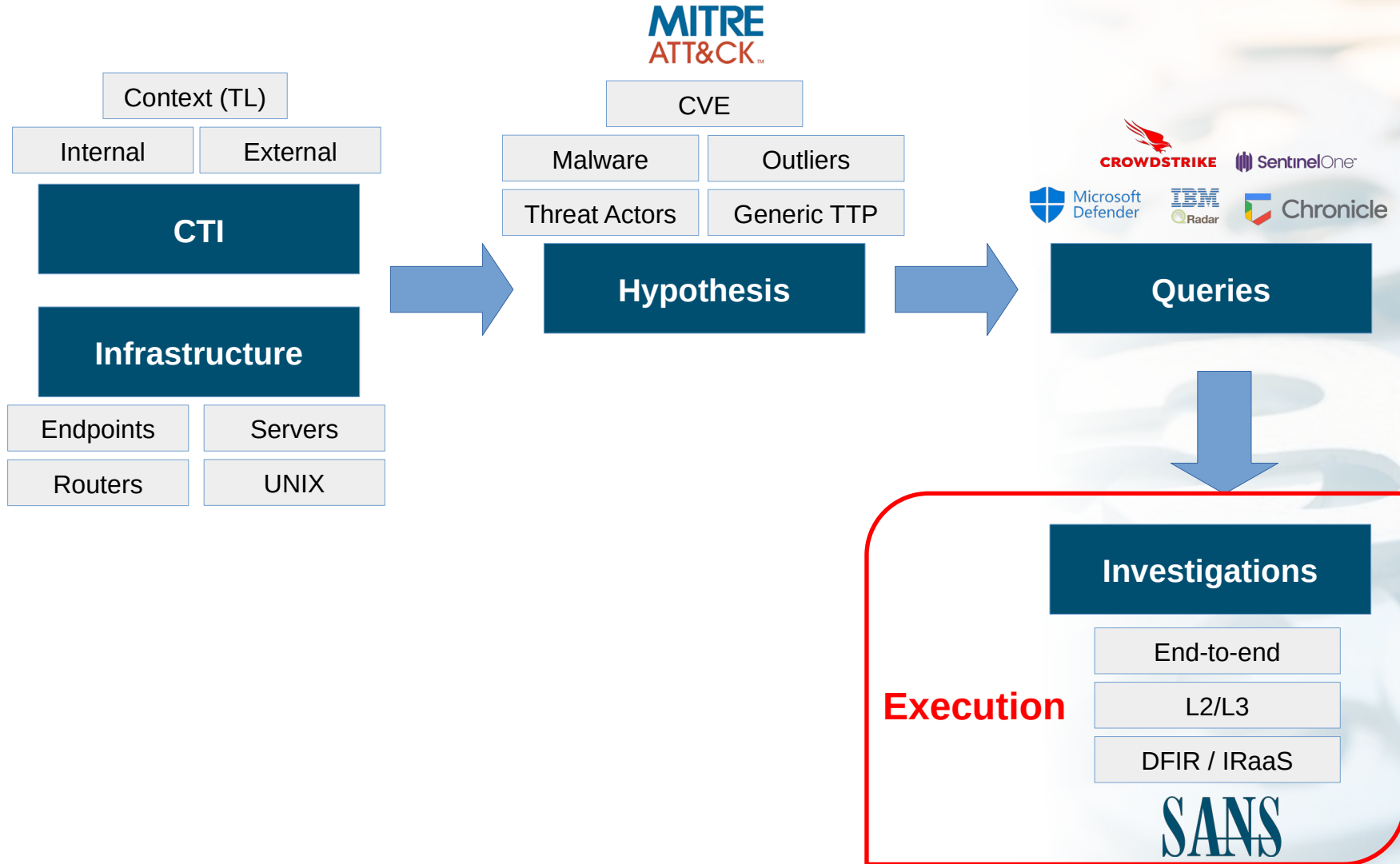
Hypothesis: Lockbit affiliate modifies Run\RunOnce keys to get persistence

Microsoft Defender 365

```
// Persistence via RunOnce, RunServices y RunServicesOnce
DeviceRegistryEvents
|where ActionType == "RegistryKeyCreated"
or RegistryKey contains "RunOnce"
or RegistryKey contains "RunServices"
or RegistryKey contains "RunServicesOnce"
```

Note: this is not a real query to detect lockbit

How Does TH Work?

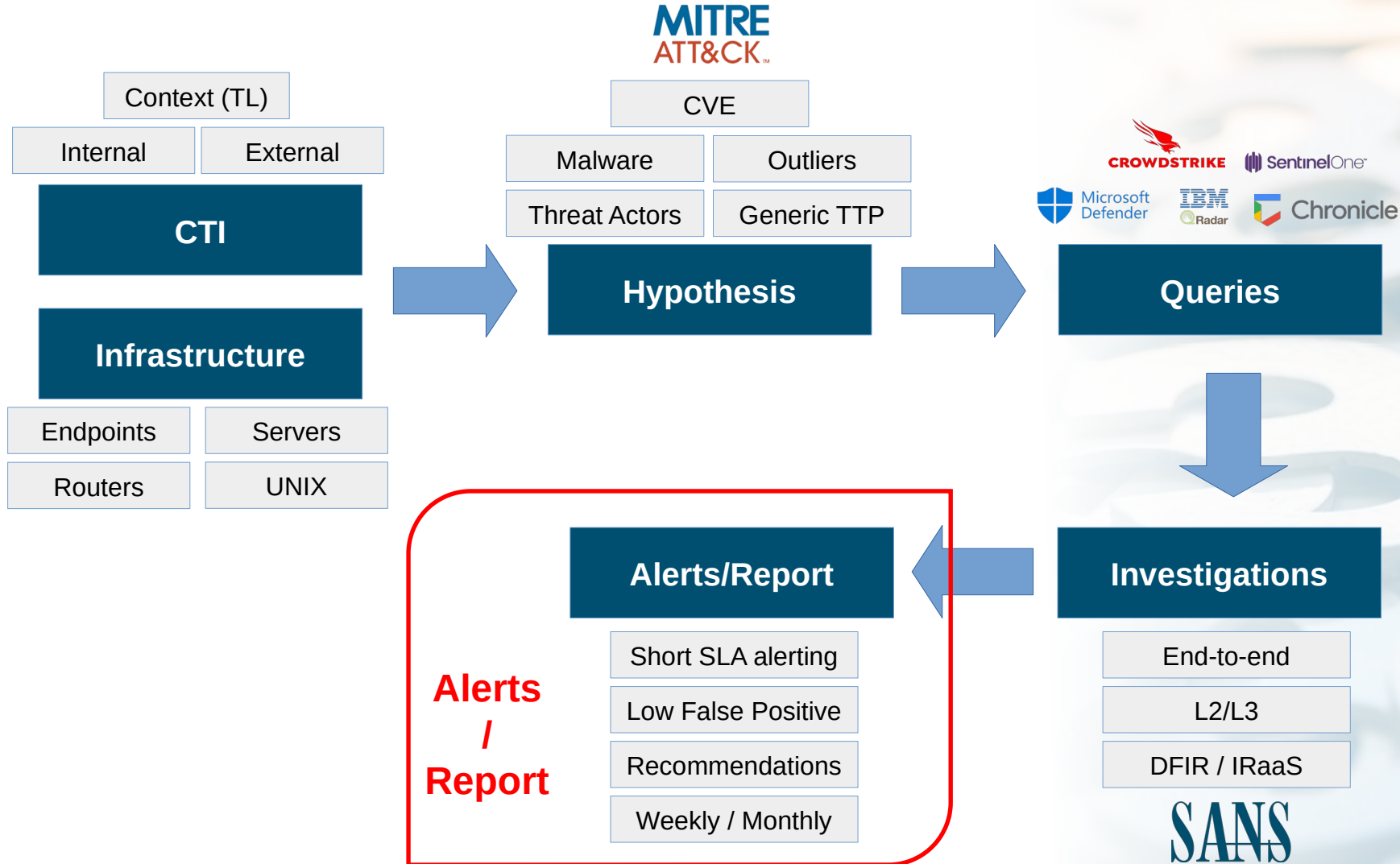


End-to-end investigations

```
label=Registry label=Set label=Value
target_object IN
[*\software\Microsoft\Windows\CurrentVersion\Run*]*\software\Microsoft\Windows\CurrentVersion\RunOnce*,
*\software\Microsoft\Windows\CurrentVersion\RunOnceEx*,
*\software\Microsoft\Windows\CurrentVersion\RunServices*,
*\software\Microsoft\Windows\CurrentVersion\RunOnceEx*,
*\software\Microsoft\Windows\CurrentVersion\RunServices*,
*\software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell*,
*\software\Microsoft\Windows NT\CurrentVersion\Windows*,
*\software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders*] -user IN
EXCLUDED_USERS
```

account_type	100	domain=NT AUTHORITY event_id=13 event_type=SetValue process=C:\Program Files (x86)\Micr... event_category=Registry value set (rule: R... host=SIC-VENUS.sigintcorp.tk
channel	100	event_source=Microsoft-Windows-Sysmon rule=T1060,RunKey account_type=User channel=Microsoft-Windows-Sysmon/Op... col_ts=2022/09/11 11:52:06
event_source	100	collected_at=LogPoint detail="C:\Program Files (x86)\Mic... device_category=OS event_ts=2022/09/11 11:52:20 execution_process_id=2444 execution_thread_id=4632
opcode	100	guid={5770385F-C22A-43E0-BF4C-06... image=C:\Program Files (x86)\Mic... keyword=9223372036854775808 log_level=INFO logpoint_name=LogPoint message=Registry value set norm_id=WindowsSysmon opcode=Info opcode_value=0 process_guid={fe4dedcb-c98a-631d-b816-00... process_id=8988 record=3623310 source_module=in_win source_module_type=im_msvistalog target_object=HKLM\SOFTWARE\Microsoft\Win... task_value=13 user_id=S-1-5-18 utc_ts=2022/09/11 06:07:18 version=2
device_category	100	
event_type	100	{ "EventTime": "2022-09-11T17:37:18.756470+05:45", "Hostname": "SIC-VENUS.sigintcorp.tk", "Keywords": "9223372036854775808", "EventType": "SetValue", "SeverityValue": 2, "Severity": "INFO", "EventID": 13, "SourceName": "Microsoft-Windows-Sysmon", "ProviderGuid": "{5770385F-C22A-43E0-BF4C-06F5698FFBD9}", "Version": 2, "TaskValue": 13, "OpcodeValue": 0, "RecordNumber": 3623310, "ExecutionProcessID": 2444, "ExecutionThreadID": 4632, "Channel": "Microsoft-Windows-Sysmon/Operational", "Domain": "NT AUTHORITY", "AccountName": "SYSTEM", "UserID": "S-1-5-18", "AccountType": "User", "Message": "Registry value set:\nRuleName: T1060,RunKey\nEventType: SetValue\nUtcTime: 2022-09-11 11:52:18.751\nProcessGuid: {fe4dedcb-c98a-631d-b816-00000003100}\nProcessId: 8988\nImage: C:\Program Files (x86)\Microsoft\EdgeWebView\Application\105.0.1343.33\Installer\setup.exe\nTargetObject: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\msedge_cleanup_{F3017226-FE2A-4295-8BDF-00C3A9A7E4C5}\nDetails: \"C:\\Program Files (x86)\\Microsoft\\EdgeWebView\\Application\\105.0.1343.33\\Installer\\setup.exe\" --msedgewebview --delete-old-versions --system-level --verbose-logging --on-logon\nUser: NT AUTHORITY\\SYSTEM", "Category": "Registry value set (rule: RegistryEvent)", "Opcode": "Info", "RuleName": "T1060,RunKey", "UtcTime": "2022-09-11 11:52:18.751", "ProcessGuid": "{fe4dedcb-c98a-631d-b816-00000003100}", "ProcessId": "8988", "Image": "C:\\Program Files (x86)\\Microsoft\\EdgeWebView\\Application\\105.0.1343.33\\Installer\\setup.exe", "TargetObject": "HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\RunOnce\\msedge_cleanup_{F3017226-FE2A-4295-8BDF-00C3A9A7E4C5}", "Details": "\"C:\\Program Files (x86)\\Microsoft\\EdgeWebView\\Application\\105.0.1343.33\\Installer\\setup.exe\" --msedgewebview --delete-old-versions --system-level --verbose-logging --on-logon", "User": "NT AUTHORITY\\SYSTEM", "EventReceivedTime": "2022-09-11T17:37:20.623990+05:45", "SourceModuleName": "in_win", "SourceModuleType": "im_msvistalog" }
process_guid	100	
record	100	
host	100	
keyword	100	
image	100	
target_object	100	
log_level	100	
version	100	
norm_id	100	

How Does TH Work?



Threat Hunting: Not Just Proactive Detection

TH is not only about detecting Threat Actors, you get value from it everyday

- **Bad practices:** passwords in clear text, incorrect use of admin users, PuP...
- **SOC Empowerment:** improve your automatic detections.
- **Red Team / Purple Team:** detect the security issues they are exploiting.
- **EIR:** in case of incident, must have support.

Doing Threat Hunting Is Not Just to Hunt

- **Strategy:** how we identify actors, create hypothesis, workflows...
- **CTI:** to be up-to-date with Threat Actors and campaigns.
- **DFIR:** to get deeper knowledge and analysis capabilities.
- **Malware:** to exploit Threat Actors tools and detect them.
- Extensive **Knowledge and experience:** for good detection capabilities.

Summary. Why Can't You Live Without It?

Threat Hunting is a Must-Have



Threat Intelligence and Proactive Detection start to be **part of regulatory compliance** such as ISO or DORA.

SANS

> 80% of organizations using TH have **reduced the resources** used for **incidents remediation**.



It is **the only way to be protected** against many different threats such as ransomware that reactive detection cannot detect.

That's why more than 51% of organizations have formally introduced a Threat Hunting function

2024 SANS Threat Hunting Survey

Empower All Your Areas

Much more than detecting Threat Actors

Protection

Detect weak configs / bad practices

Helps to evaluate tools such as EDR

May discover potential vulnerabilities

Support to improve configs and tools

Detection

Use of Cyber Threat Intelligence

In-depth manual analysis of threats

Improve automated detections

Enhance teams: SOC, Purple/Red Team

Response

Reduce dwell time to zero in Response

Support other teams during EIR

Be a part of Incident Response

Enhance teams: SOC, Purple/Red Team



Very Easy To Make It Happen

We have the knowledge

Queries

Experts

Technology

You have the tools



Just give us access to your platforms and we will start today

Compromise Assessment

One-Shot Threat Hunting for Specific objectives

**Incident Response
related**


M&A

**Maint Threat Actors and
TTP**


**Bad practices /
Misconfigurations
identification**


How Can We Help You?

How Can We Help You?


 **Technology**


- Other
- SIEM
- EDR
- XDR

 **Technology Maturity Assessment**


 **Monitoring**
(Reactive Detection)

- Standard SOC
- Use Cases
- Threat Landscape
- Continuous CTI
- TH Integration

 **SOC Maturity Assessment**

 **Threat Hunting**
(Proactive Detection)

- Intelligence
- Hypothesis
- Bad Practices
- SOC Integration
- Anomalies

 **TH / CTI Maturity Assessment**

Threat Hunting Services

Managed Threat Hunting (MTH)

Proactive and continuous Threat Hunting services for a wide range of threats detection.



Compromise Assessment (CA)



One shot Threat Hunting to cover a specific goal (Incident Response related, Threats Actor, M&A).

Change your cybersecurity strategy

From reactive to proactive, protecting yourself better in case of incident.

We can be the team or complement your team

We can integrate our team and processes with your SOC, CERT, TH Team, etc.

Review your data to detect past or current breaches

We provide you with the security of not having breaches

Complement your CyberSecurity strategy

Complement for Red Team exercises, post Incident Response, etc.

Different options and prices

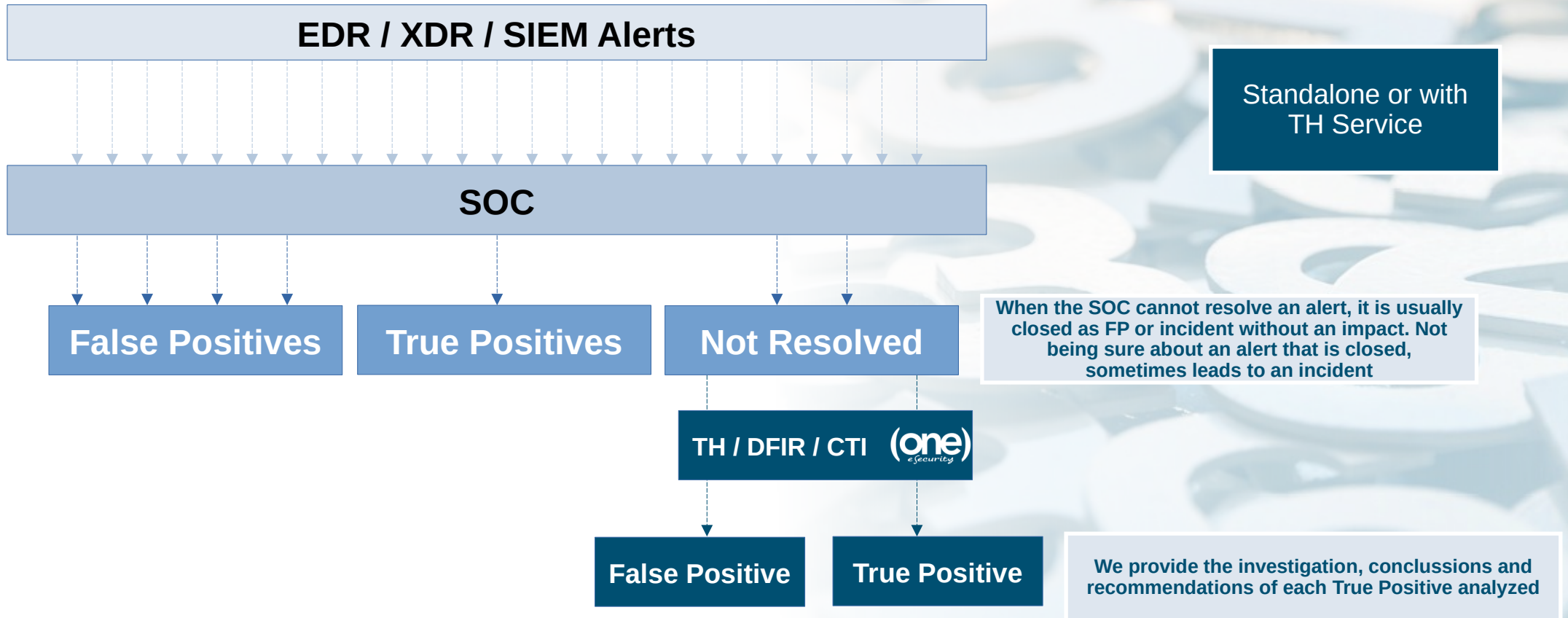
At the vanguard of threats

Maximum flexibility

Quick start

L3 Escalation

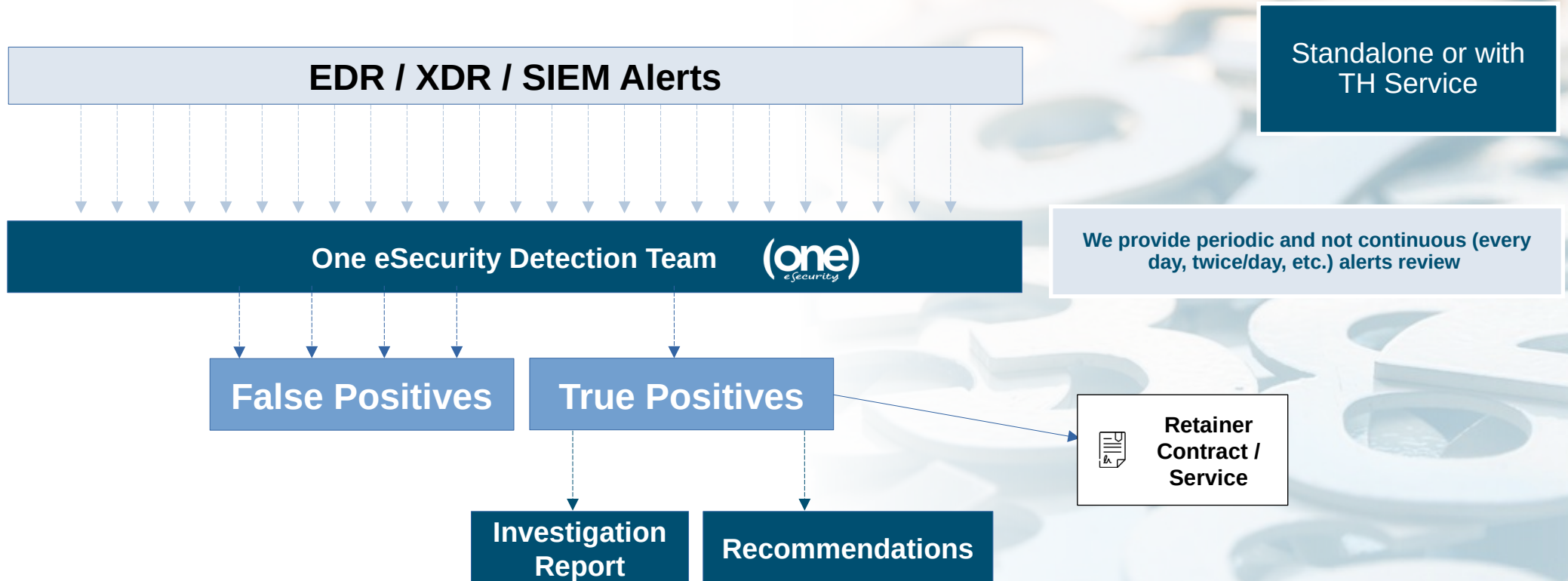
We help you to resolve your most advanced tool alerts, using all our DFIR / TH expertise to investigate then when your SOC or internal team is not capable





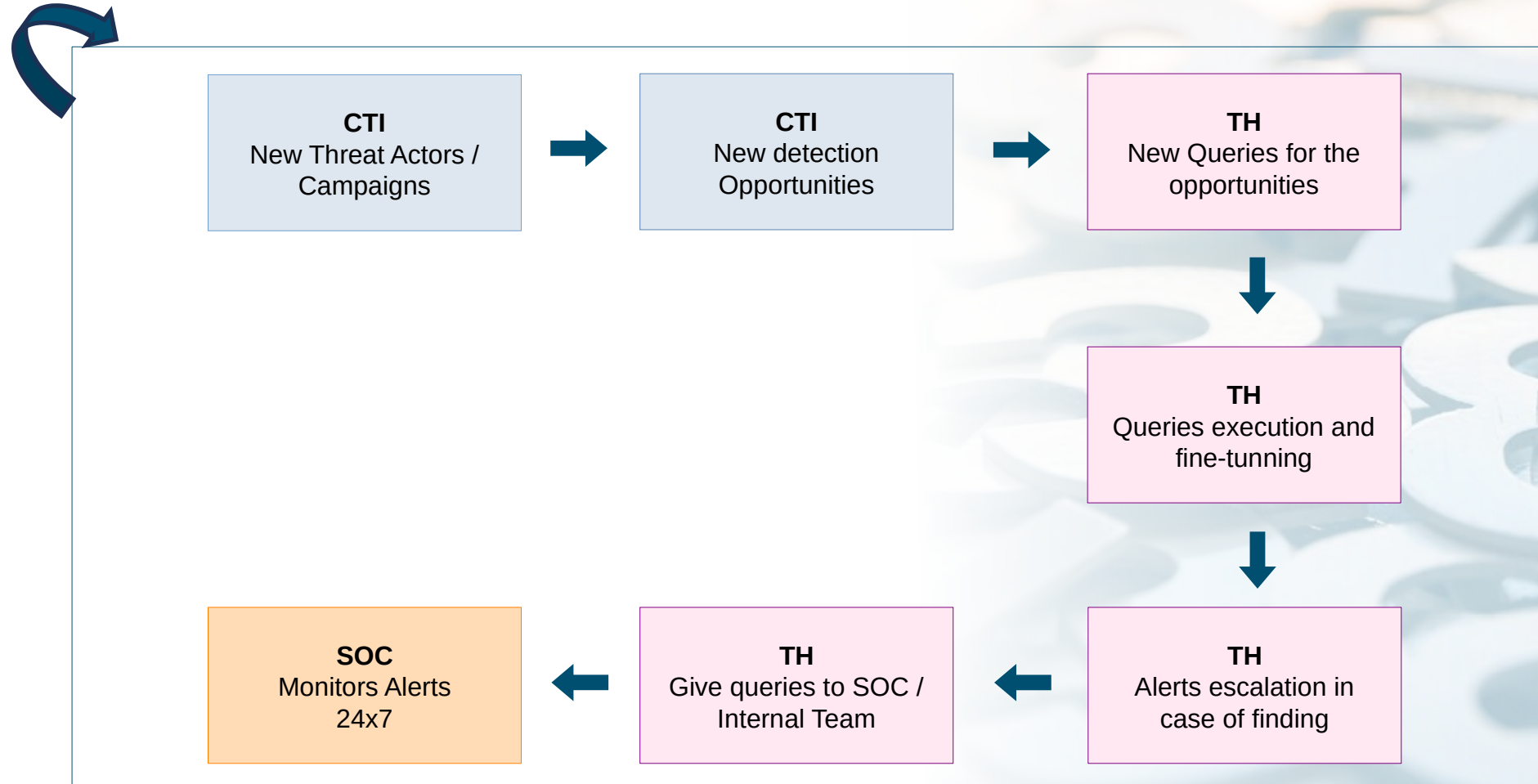
Alerts Review

A SOCless solution to take advantage of your tools



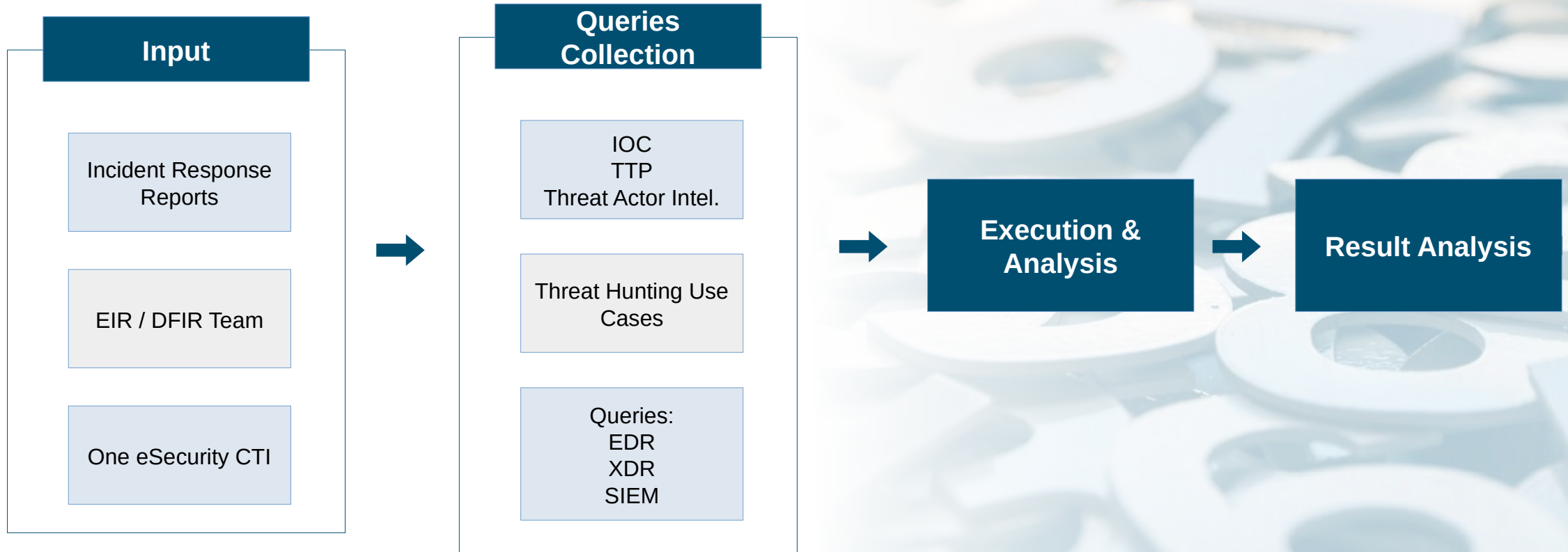
SOC Empowerment

Create new use cases for you SOC, the latest threats and the power of our Threats Hunting services, so your SOC can monitor them 24/7



CA Incident Response Related

Benefit from One eSecurity Threat Hunting expertise in one-shot. Example:



Tailoring The Solution

**Any devices (e.g:
routers)**

**Any other tools
(e.g: firewalls)**

**Other Data
Sources (e.g:
network traffic)**

**Different Types of
CA**

About Our Services

Fortune 500
customers

Hunting about 100k
assets daily

Continuous Threat Hunting is crucial for the early detection of potential security threats & vulnerabilities

51% of organizations have formally defined Threat Hunting methodologies

SANS 2024 Threat Hunting Survey

Feedback from our customers

One eSecurity is detecting Threats that other service providers are not detecting

One eSecurity provides services that other service providers cannot (netflows, Ciscos)

One eSecurity is giving useful extra information about threats under investigation

Client 1

After an incident through their network devices attended by One eSecurity, we started a Threat Hunting service with EDR, SIEM, and some hunting types very uncommon and customer oriented, such as config. files in network devices and netflows, detecting different vector attacks before the intrusion was confirmed and wrong configurations in new network devices before they were exploited.

Client 2

Customer with an EDR and a SIEM that needs help to complement its team and get a more proactive perspective. We helped them by reviewing the tools alerts, investigating the most complex ones, and continuously introducing new queries in their platforms to cover their needs. They reduced the internal team needed and we helped stop some attacks with the queries we were introducing in the EDR.

Client 3

Fortune 500 bank customer with multiple EDRs and tenants in many different countries. With our automation, we have been able to hunt in hundreds of thousands of assets and detect different attacks.



Making the world safer since 2007

San Francisco · Miami · Mexico City · São Paulo · Madrid · London · Singapore · Santiago de Chile · Bogotá

www.one-esecurity.com | ds4n6.io