DISCLAIMER

The views and opinions expressed in this presentation are solely those of the presenter and do not necessarily represent the views or positions of Deloitte or any of its affiliates.

DETECT KNOWN UNKNOWNS

Proactive Threat Hunting to climb the highest of the pyramids

Fulvio Colombrino
Niko Mkhatvari

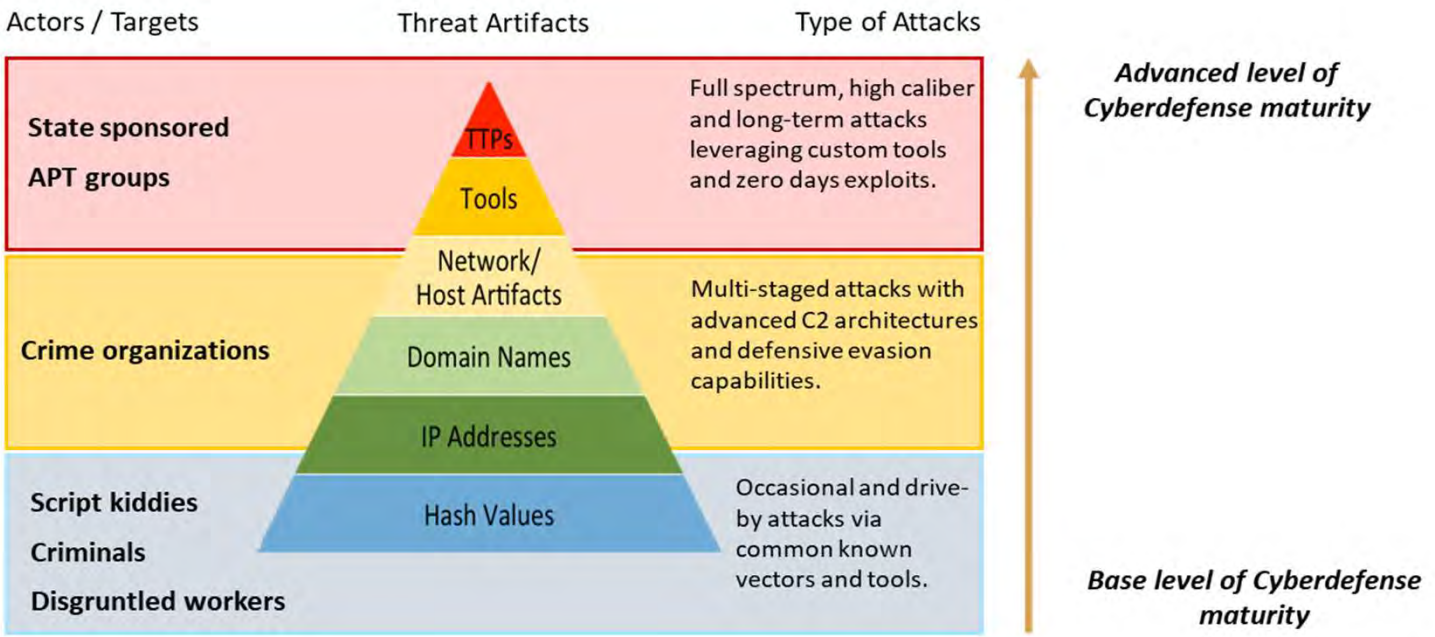
“A goal without a plan is just a wish.”

- Antoine de Saint-Exupery

Hi everyone !

- Fulvio Colombrino
- MsC in Computer Enginnering
- 1+ year as Analyst
- Head of TH project

Pyramid of pain



- Pyramid of pain, by David Bianco

CONF42

Is it necessary ?

CONF42

Is it necessary ?

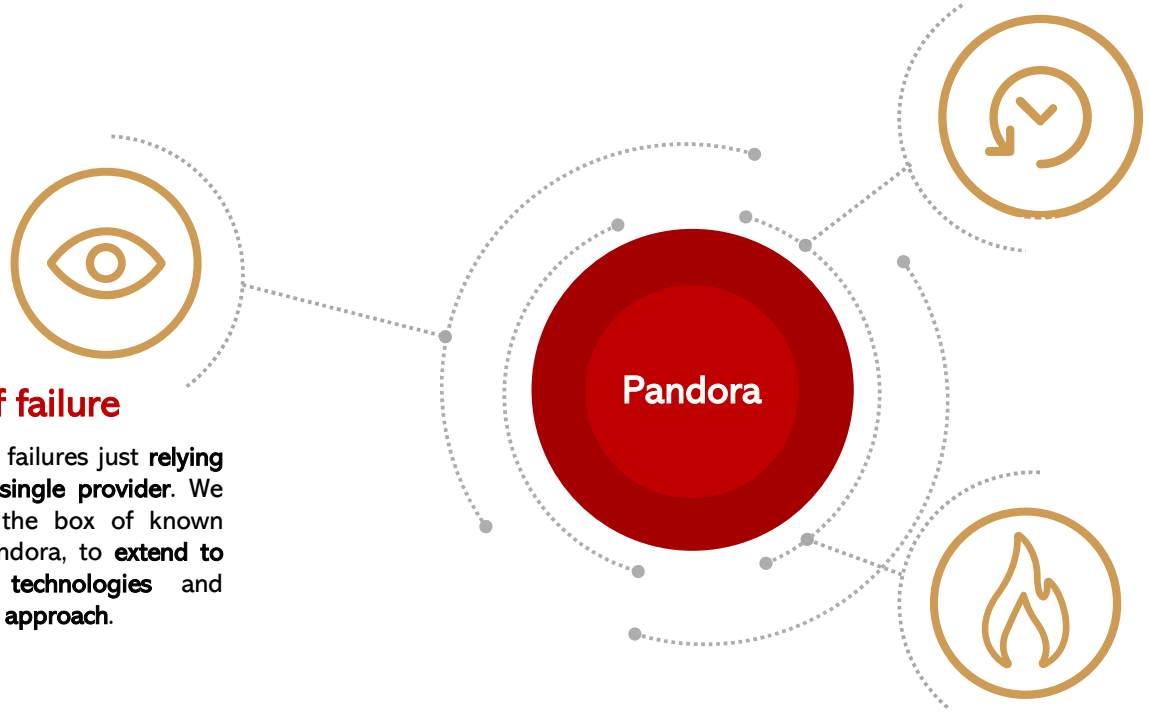
CONF42

Is it necessary ?

CONF42

Is it necessary ?

The three main focus point of the Pandora project



Single point of failure

Avoid single point of failures just **relying on black boxes and single provider**. We are trying to open the box of known unknowns, hence Pandora, to **extend to different detection technologies** and provide more **generic approach**.

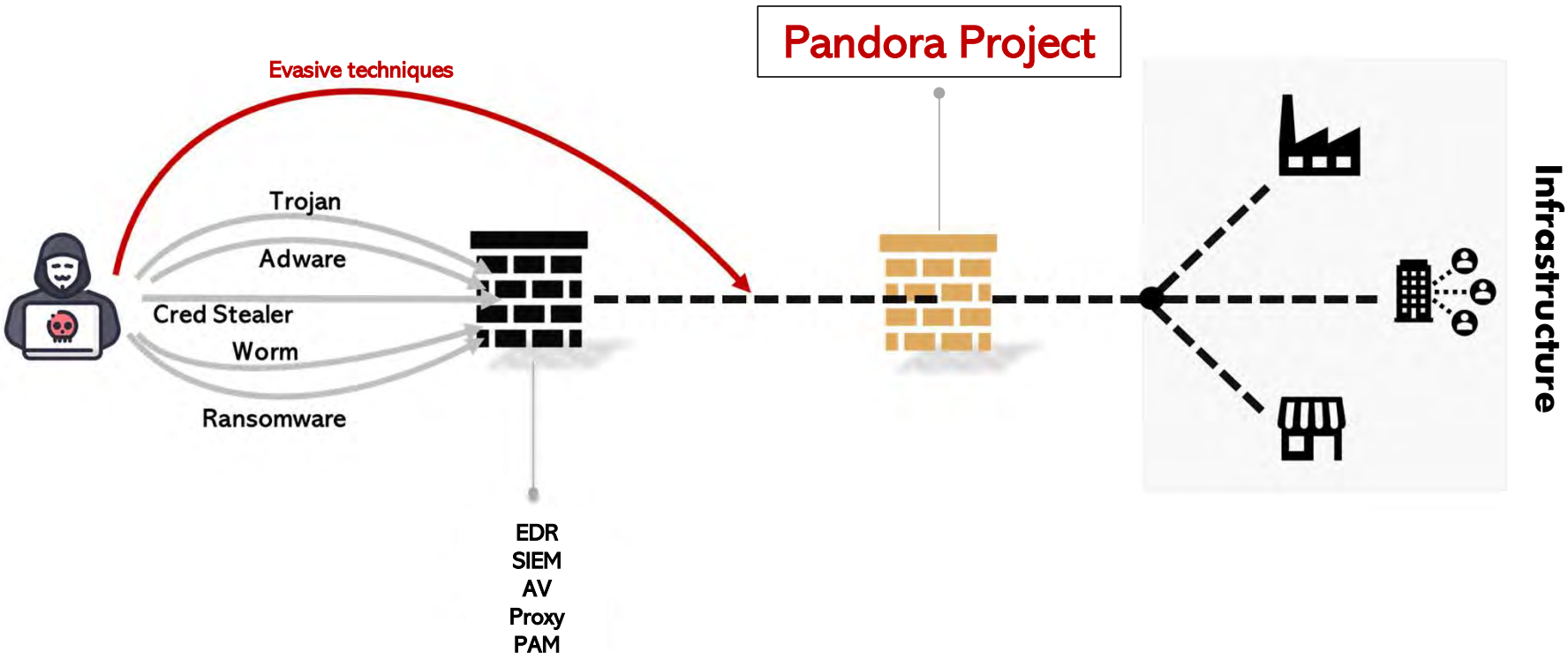
Dwell time reduction

Nowadays one of the toughest achievements is the **reduction** of the dwell time i.e. the **exposure time which spans from Incident to its Detection**. The work aims to **accomplish** this thanks to the analysis of client's **landscape** and latest **threats**.

Assume the breach

A **proactive stance,** employing Threat Hunting techniques, gives the ability to prepare for and respond to security incidents, **minimizing** the impact on business **operations** and sensitive **data**.

A tailored defensive solution

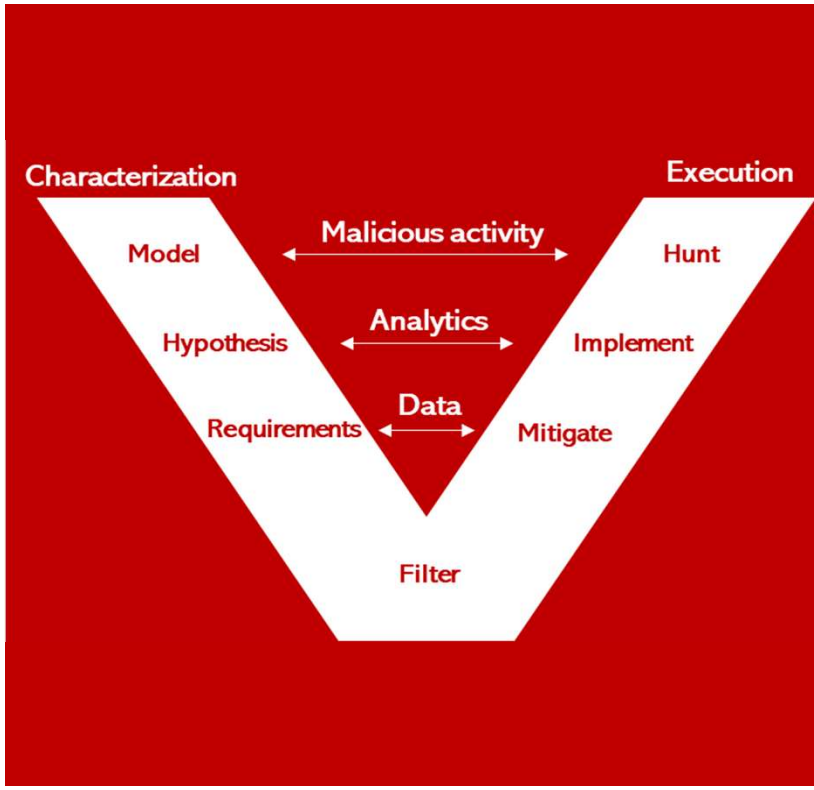


TTP based Threat Hunting

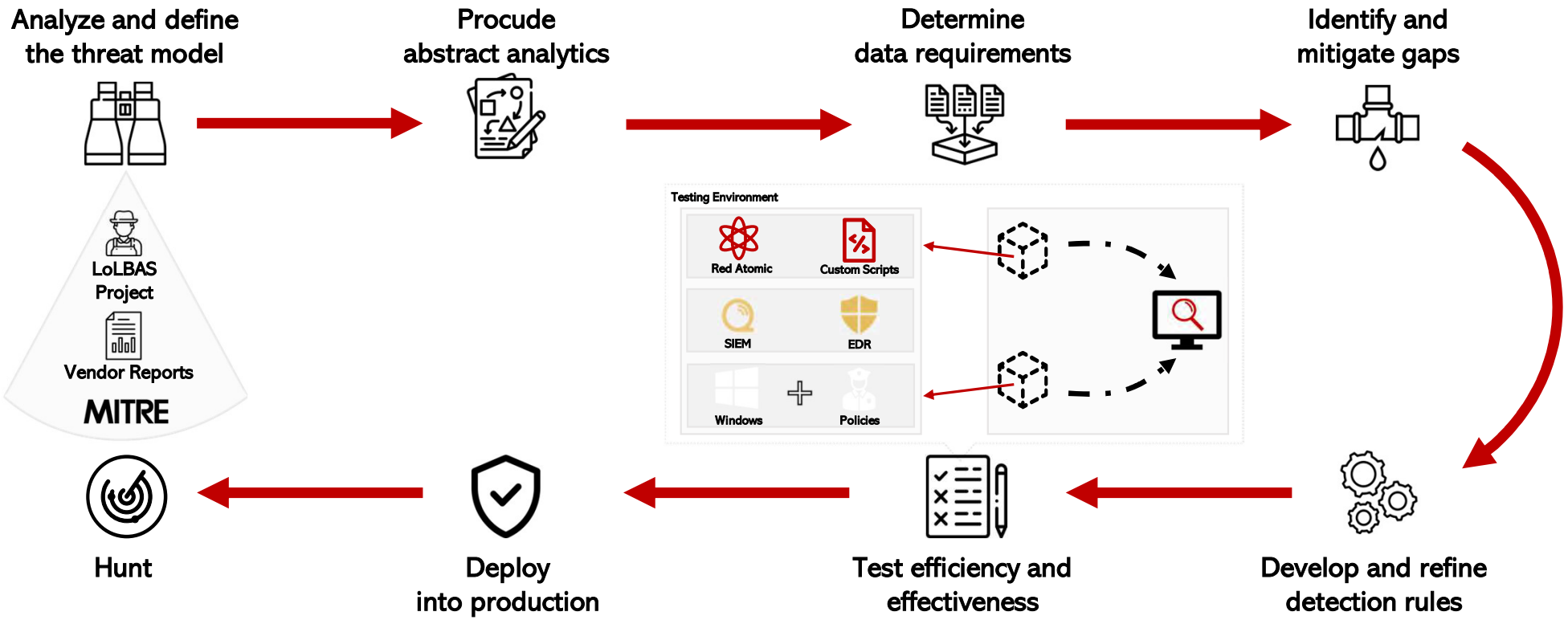
Shifting from the signature based and anomaly based hunting approach to a **behavioral** one.

It allows for a more efficient and effective way to identify and mitigate potential threats through the analysis of the:

- **Tactics:** the overall goals behind the attack
- **Techniques:** the method used
- **Procedures:** step-by-step description of the attack

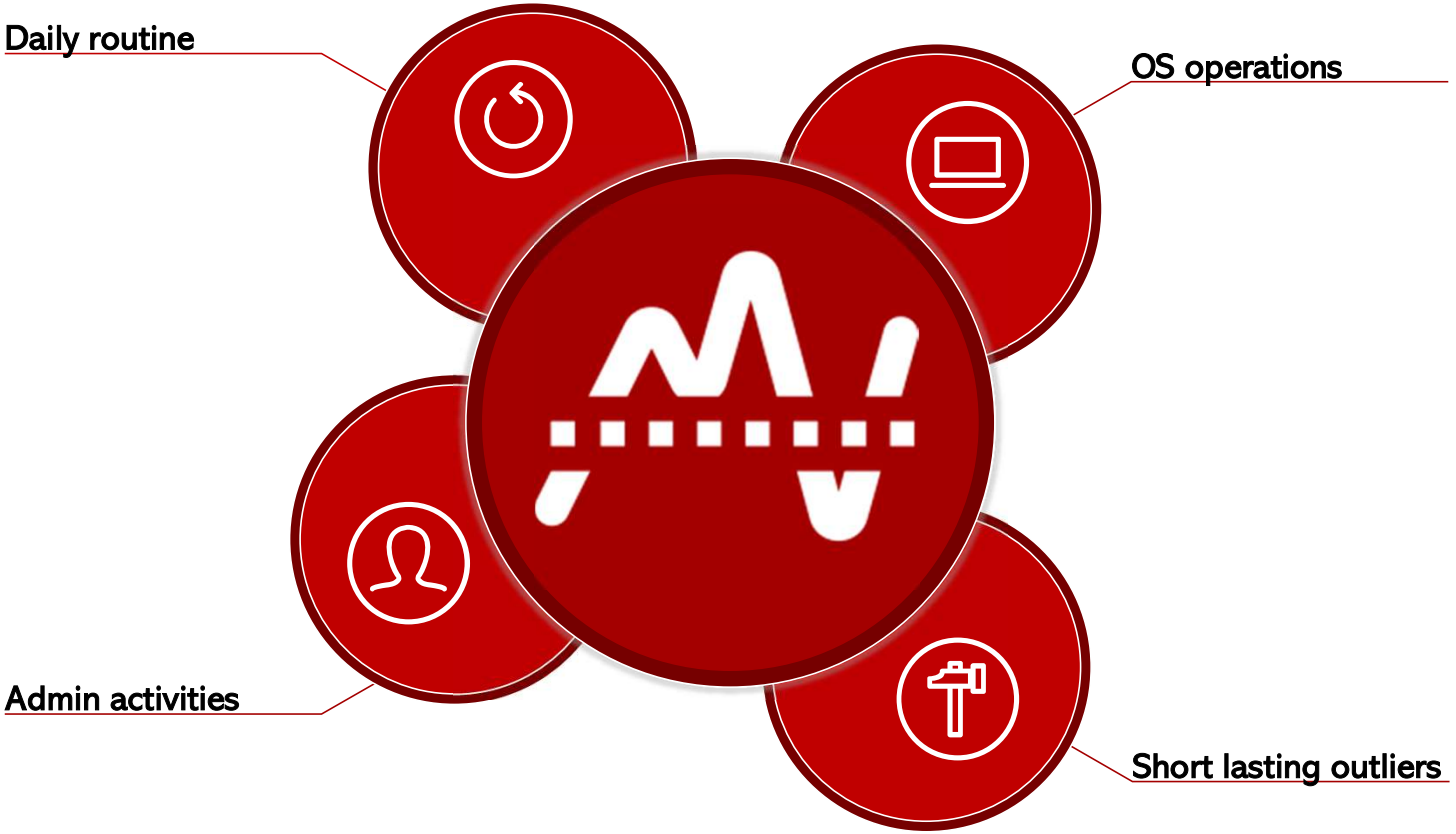


Methodology Workflow



CONF42

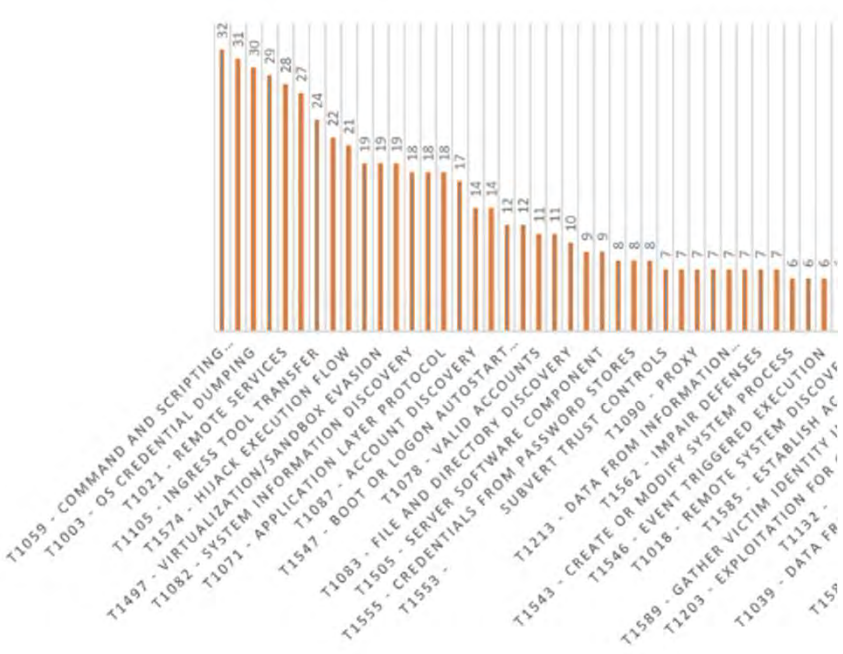
Baseline and it's impact



Threat model

Industry cyber threats

Threat Landscape



Testing environment

To validate the developed rules, **ad hoc testing environments** have been implemented:

- EDR detonation virtual machine
- SIEM detonation virtual machine
- Log collector virtual machine

The purpose is to **test** the default detection capabilities of the perimeter **before** and **after** the **implementation** of the new analytics

Deliverables

- Play Books
- Network changes
- New Testing Environments
- Threat Discoveries
- Security events logs
- New log sources

Use case

Windows Background Intelligent Transfer Service (BITS) is a built-in framework used to transfer files to and from web and SMB servers.
Adversaries abuse BITS to download, execute, and even clean up after running malicious code.

- **Abstract Analytics:**
  - Ingress Tool Transfer (T1105)

    process_name == "BITSAdmin"
    AND
    command_line has_any (["/addfile","/SetNotifyCmdLine","/Resume", "/complete", "transfer", "download"])
  - Defense Evasion / Persistence - System Binary Proxy Execution (T1218)

    process_name == "BITSAdmin"
    AND
    command_line has_any (["/SetNotifyCmdLine"])

- **Data Dictionary:**
  - Windows Process Auditing – EventID 4688
  - Sysmon – EventID 1

Testing phase

```
PS C:\Users\User> Invoke-AtomicTest T1105 -TestNumbers 9
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1105-9 Windows - BITSAdmin BITS Download
BITSADMIN version 3.0
BITS administration utility.
(C) Copyright 2000-2006 Microsoft Corp.
BITSAdmin is deprecated and is not guaranteed to be available in future versions of Windows.
Administrative tools for the BITS service are now provided by BITS PowerShell cmdlets.
Transfer complete.
Done executing test: T1105-9 Windows - BITSAdmin BITS Download
PS C:\Users\User>
```

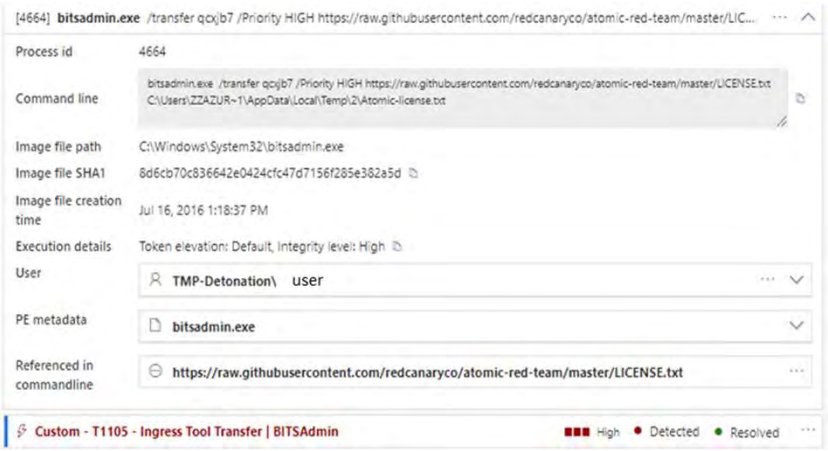
```
PS C:\Users\User> Invoke-AtomicTest T1197
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1197-1 Bitsadmin Download (cmd)
BITSADMIN version 3.0
BITS administration utility.
(C) Copyright 2000-2006 Microsoft Corp.
BITSAdmin is deprecated and is not guaranteed to be available in future versions of Windows.
Administrative tools for the BITS service are now provided by BITS PowerShell cmdlets.
Transfer complete.
Done executing test: T1197-1 Bitsadmin Download (cmd)
Executing test: T1197-2 Bitsadmin Download (PowerShell)
Done executing test: T1197-2 Bitsadmin Download (PowerShell)
Executing test: T1197-3 Persist, Download, & Execute
BITSADMIN version 3.0
BITS administration utility.
(C) Copyright 2000-2006 Microsoft Corp.
BITSAdmin is deprecated and is not guaranteed to be available in future versions of Windows.
Administrative tools for the BITS service are now provided by BITS PowerShell cmdlets.
Created job {717498AE-145A-4A73-9EC8-AA19F0BF57FC}.
BITSADMIN version 3.0
BITS administration utility.
(C) Copyright 2000-2006 Microsoft Corp.
BITSAdmin is deprecated and is not guaranteed to be available in future versions of Windows.
Administrative tools for the BITS service are now provided by BITS PowerShell cmdlets.
Added https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1197/T1197.md -> C:\Users\ZZAZUR~1\AppData\Local\Temp\bitsadmin3_flag.ps1 to job.
BITSADMIN version 3.0
BITS administration utility.
(C) Copyright 2000-2006 Microsoft Corp.
BITSAdmin is deprecated and is not guaranteed to be available in future versions of Windows.
Administrative tools for the BITS service are now provided by BITS PowerShell cmdlets.
notification command line set to 'C:\Windows\system32\notepad.exe' 'NULL'.
BITSADMIN version 3.0
BITS administration utility.
(C) Copyright 2000-2006 Microsoft Corp.
BITSAdmin is deprecated and is not guaranteed to be available in future versions of Windows.
Administrative tools for the BITS service are now provided by BITS PowerShell cmdlets.
 resumed.
BITSADMIN version 3.0
BITS administration utility.
(C) Copyright 2000-2006 Microsoft Corp.
BITSAdmin is deprecated and is not guaranteed to be available in future versions of Windows.
Administrative tools for the BITS service are now provided by BITS PowerShell cmdlets.
Job completed.
Done executing test: T1197-3 Persist, Download, & Execute
Executing test: T1197-4 Bits download using desktopimgdownldr.exe (cmd)
'desktopimgdownldr.exe' is not recognized as an internal or external command,
operable program or batch file.
Done executing test: T1197-4 Bits download using desktopimgdownldr.exe (cmd)
```

Results

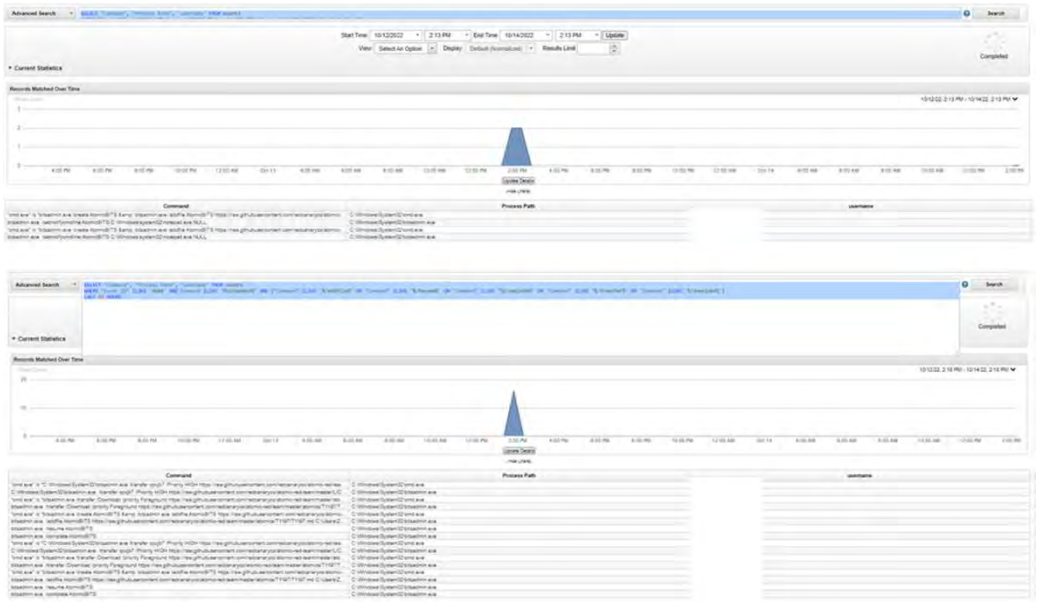
	EDR	SIEM
Device Categories	End points and Couple of servers	Specific Servers, DC.
Required Events	Yes	Yes
Auto Detection	No	No
Custom Detection	Yes	Yes
Simulation	Yes	Yes
Results	Yes	Yes

Results

EDR

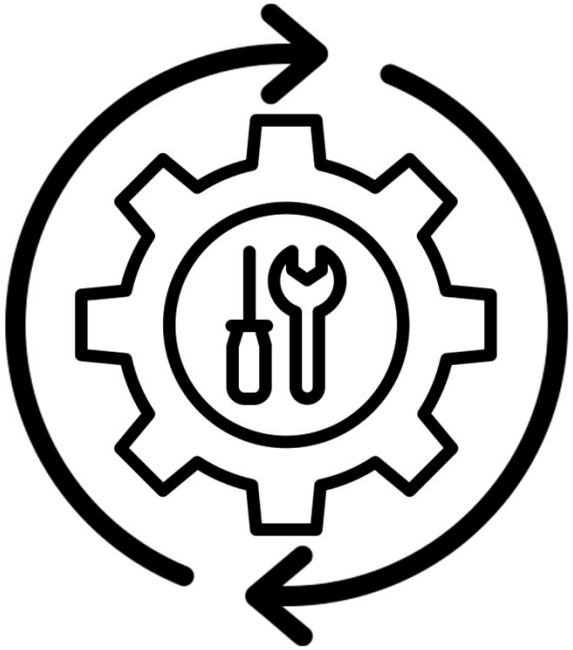


SIEM



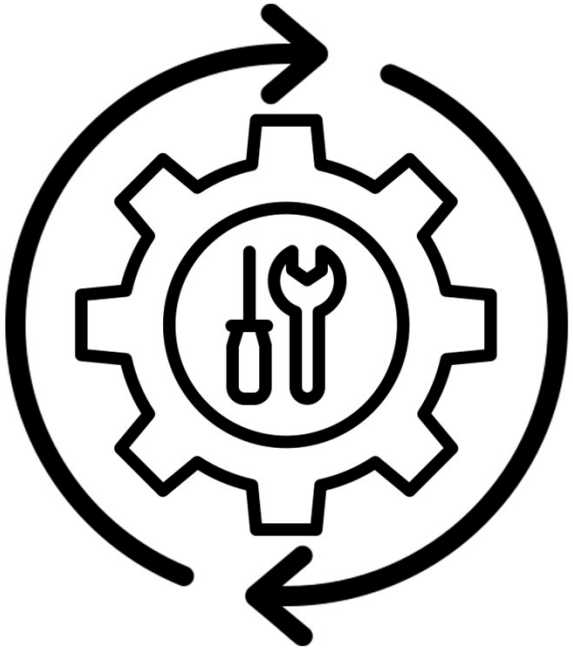
CONF42

What next ?



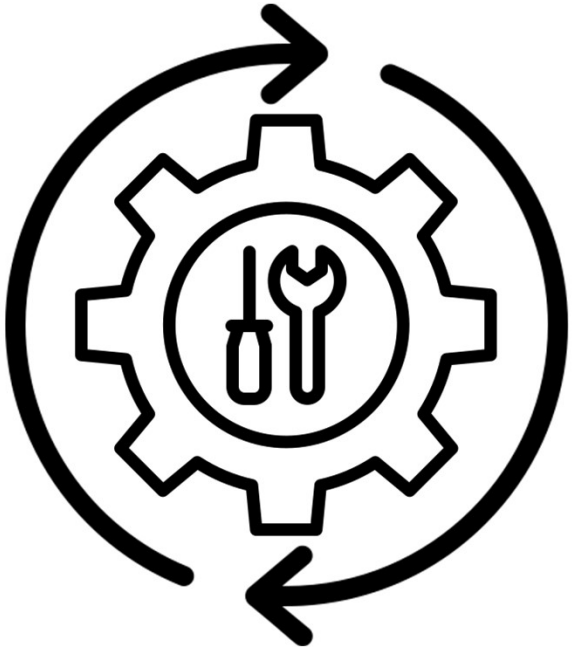
CONF42

What next ?



CONF42

What next ?



Thank you for your attention !

Questions ?

Linkedin: Fulvio Colombrino
Mail: fulvio.colombrino@virgilio.it
Twitter: @ll_Colombo