



Padvish EDR

Amnpardaz Software Company



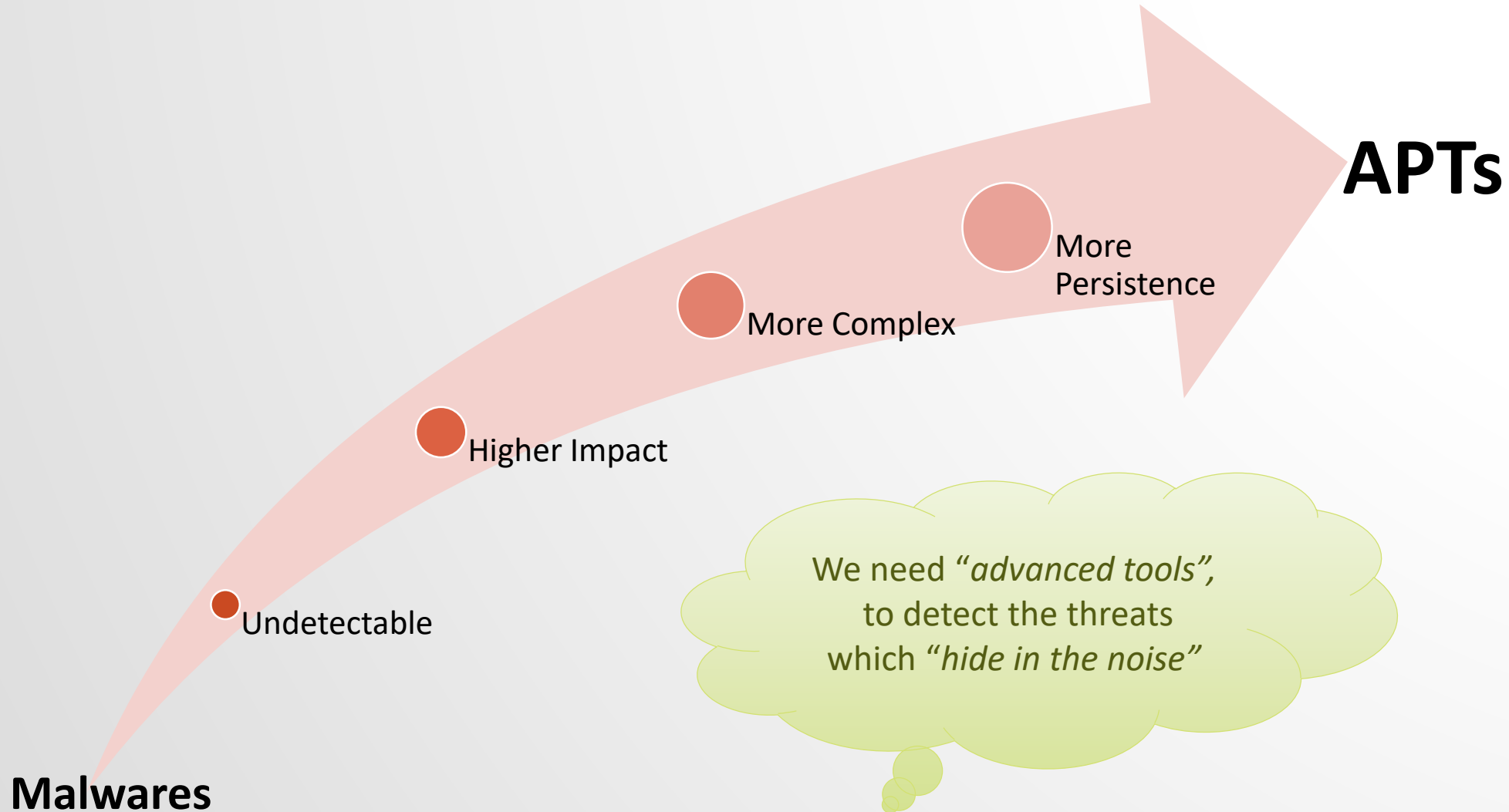
Topics

- ❖ Today's Security Landscape
- ❖ Cyber Attack Explained
- ❖ EDR Explained
- ❖ Padvish EDR
- ❖ Padvish MDR



Today's Security Landscape

Today's Security Landscape



Can't rely on traditional tools...

Attacker have access to security tools

- They can test detection before attack

Security tools are “tools”, not more

- Today's threats are controlled by advanced teams
- A tool cannot defend against a team
- You need an expert team to defend against it

Antivirus catches public malware

- Police catches visible crimes. Spies are caught by agencies.
- Many suspicious alerts are suppressed, as AV cannot ask the user about it

We need tools for experts to find the undetectables...



Alert Fatigue



Only a small percent of “Alerts” are reported by Antivirus

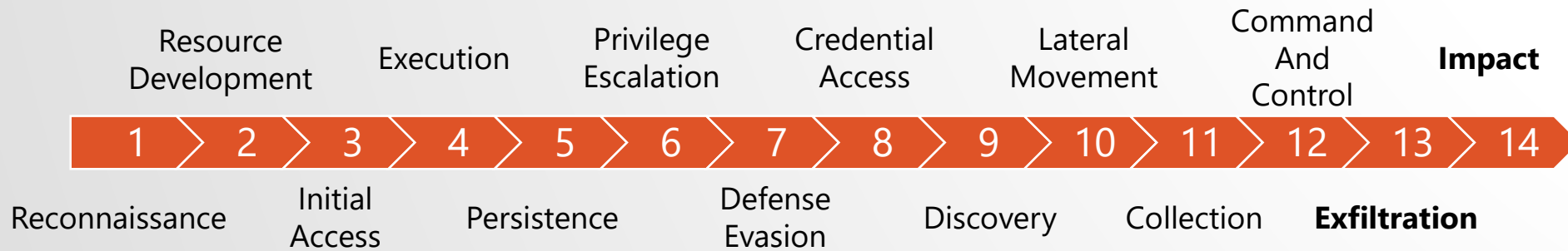
It needs to be 100% sure about it

This is where malwares hide

To find the undetectable,
We need tools to see all the events

Anatomy of cyber-attacks

MITRE ATT&CK Tactics



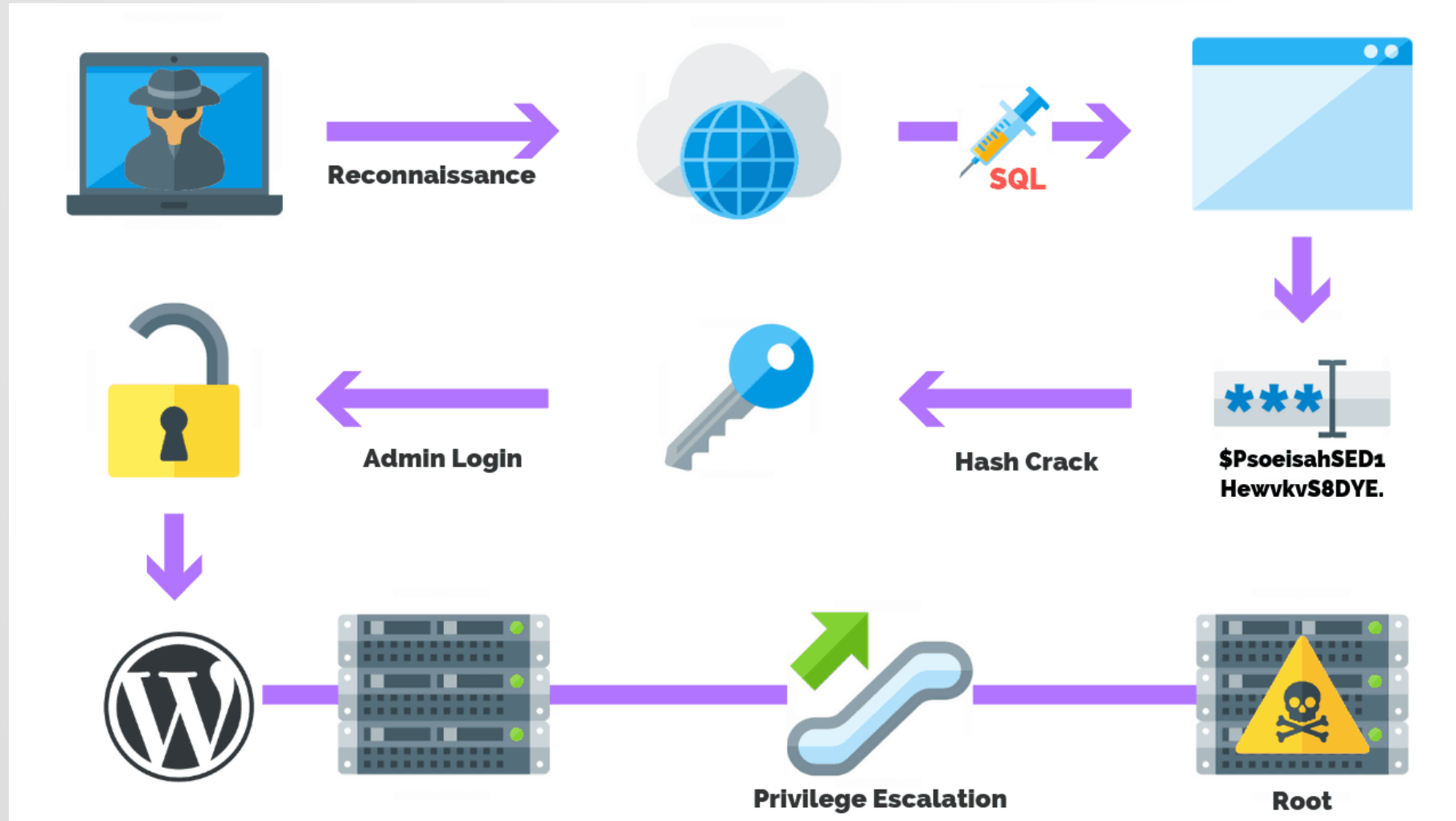
Harder to Detect



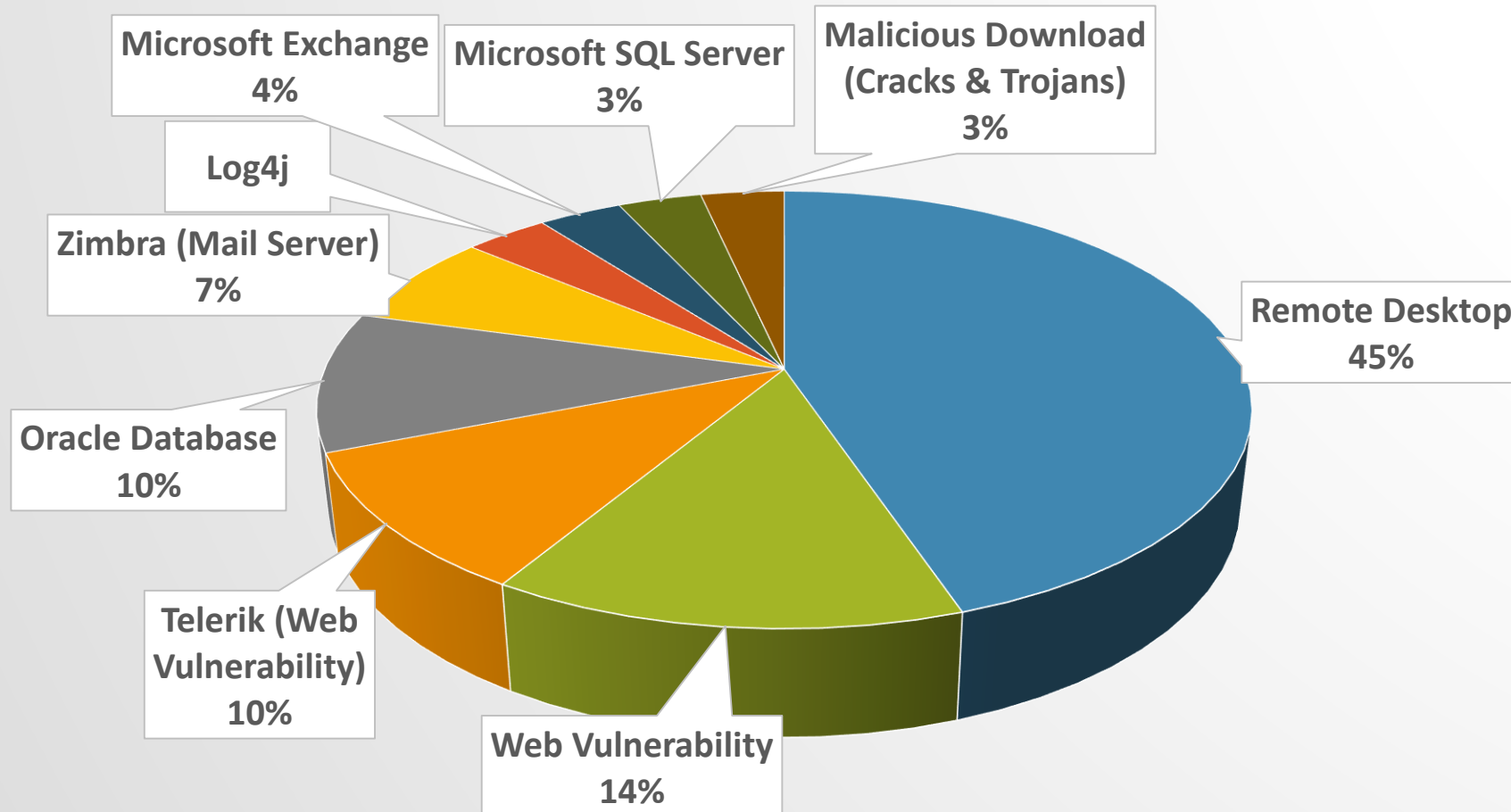
More Destructive



Typical Cyber-Attack Example



Initial Attack Vector (Recent Attacks)



Source: Amnpardaz CSIRT 2023

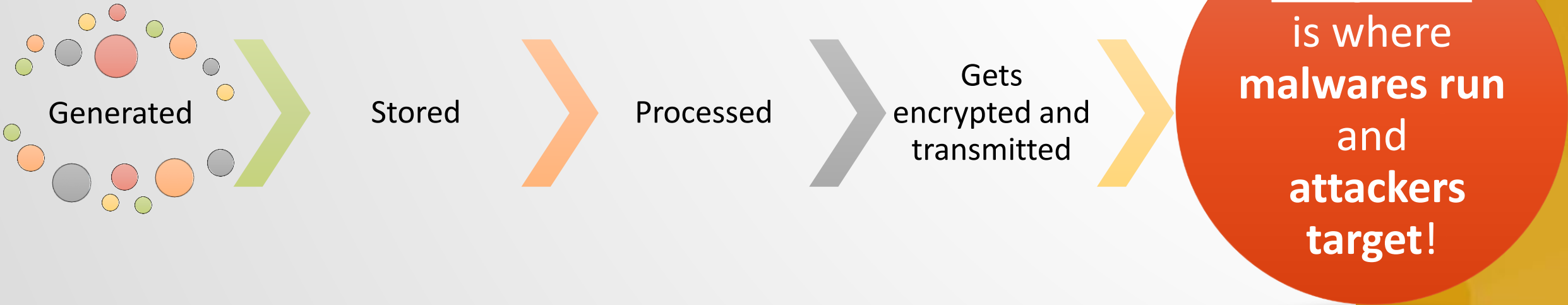


Endpoint Detection and Response

The importance of Endpoint



Endpoint is where your data is ...



Endpoint Detection and Response

Monitor

- See hidden behaviors and suspicious activities
- **Dashboards** and visualization help you to see the big picture
- **Threat hunting** allows experts to find unknown threats

Analyze

- **Alert engine** detects advanced attack indicators (IOA)
- **Forensics and timeline data** allows to find the root cause of the attack
- **Search and find** the hosts and devices affected by the threat

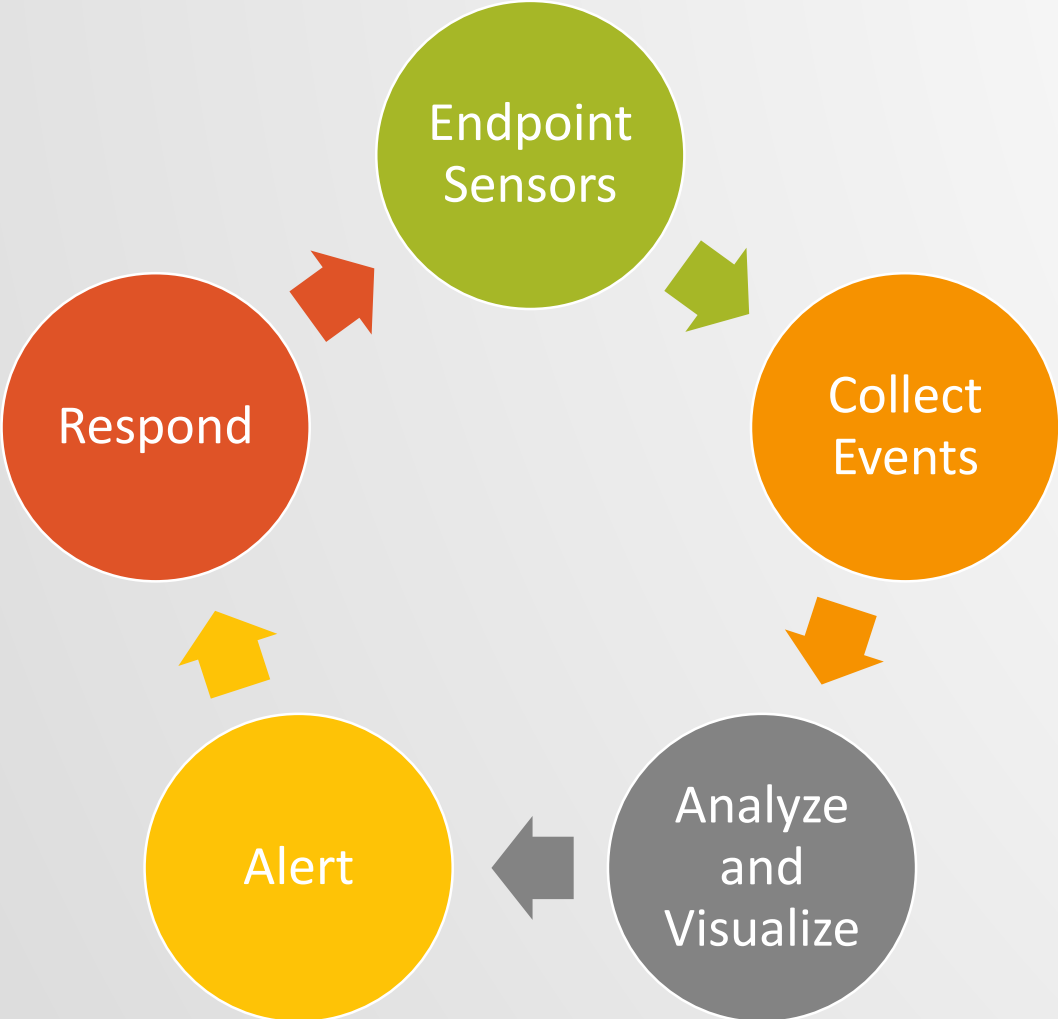
Respond

- After finding and analyzing all aspects of a threat, it's time for response
- Instantly **isolate the hosts** suspected of being infected
- Clean the hosts by **killing** or **quarantining** the artifacts of the attack



Padvish EDR

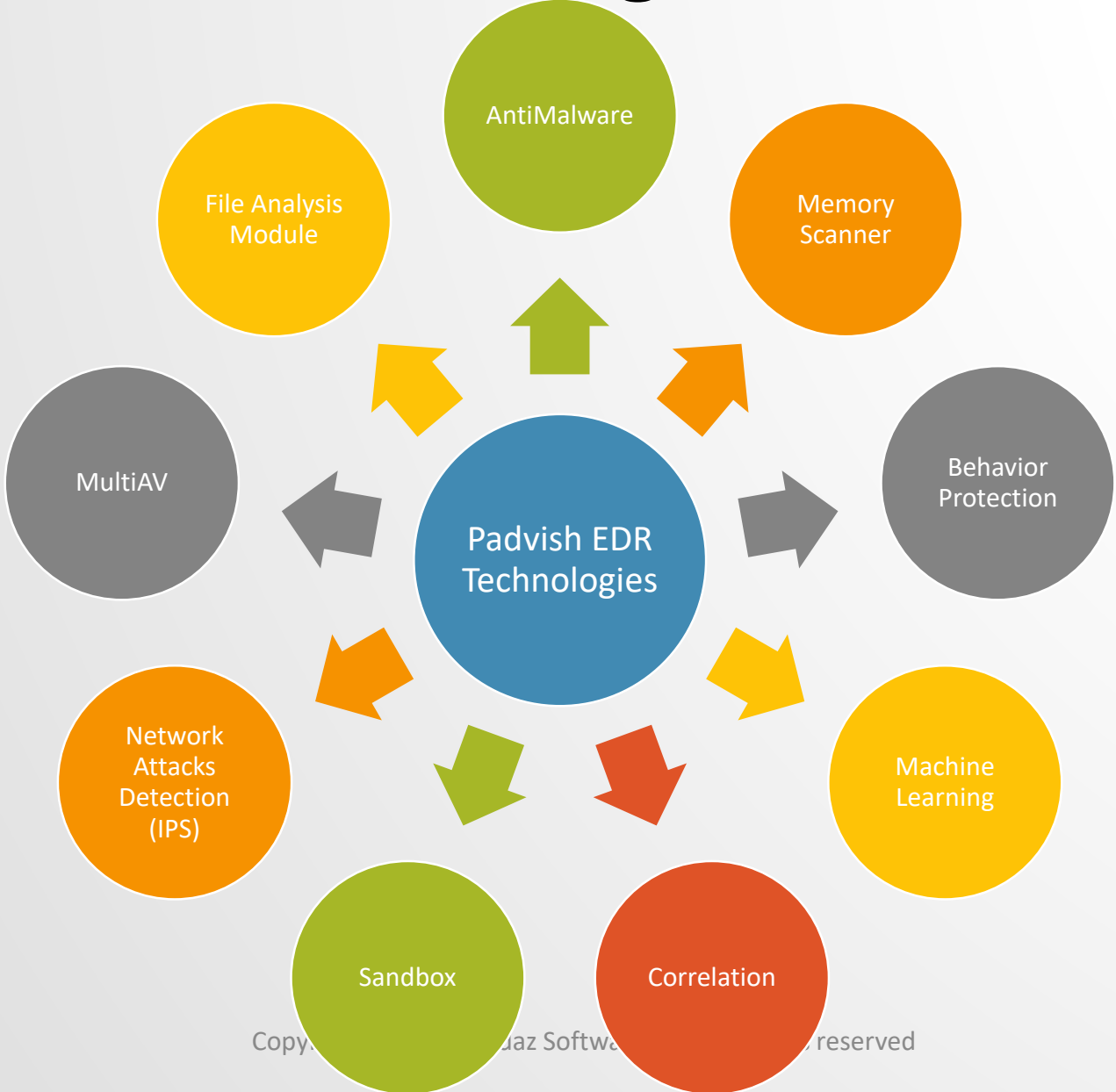
Padvish EDR



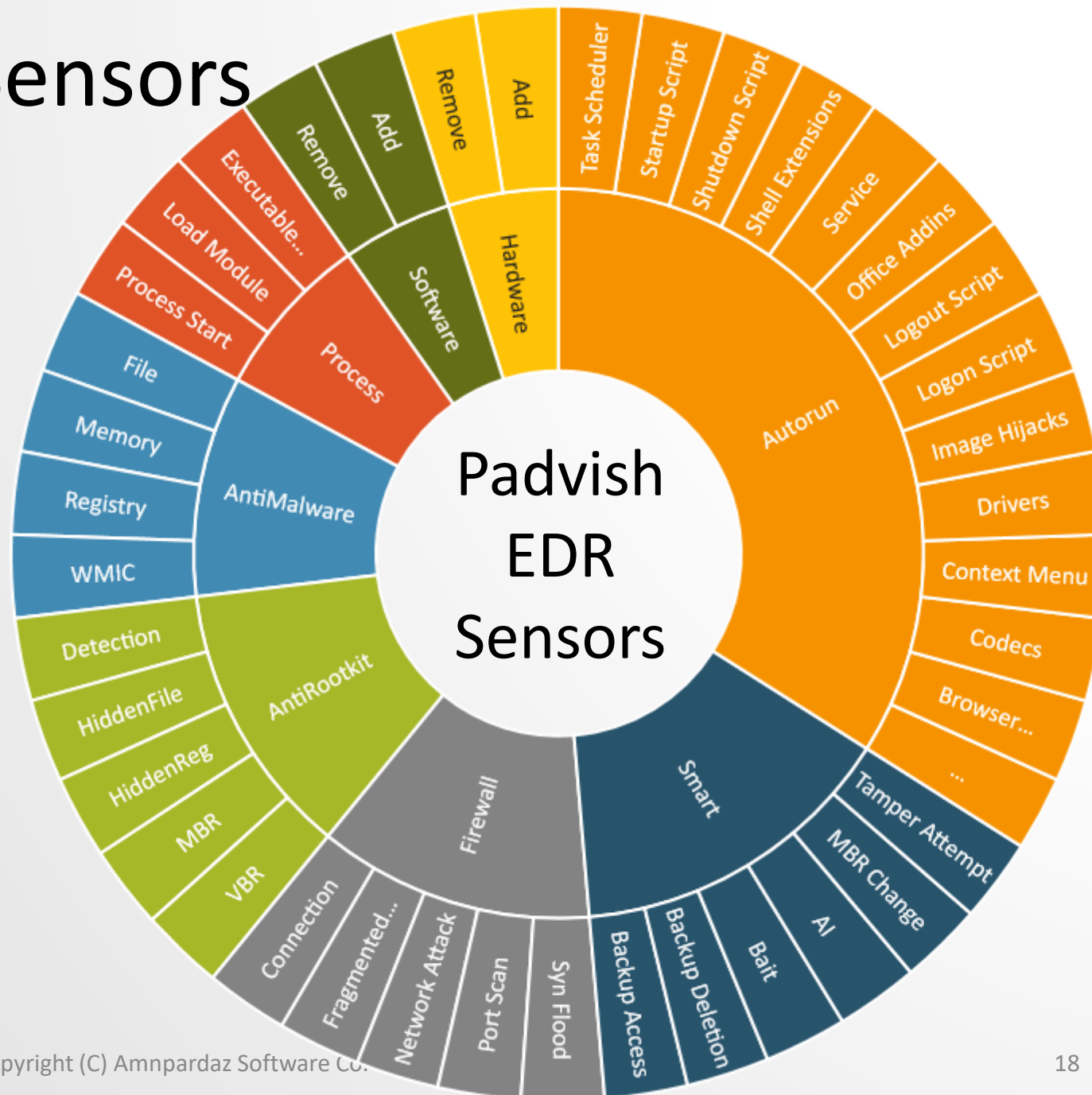
Complete support for every part of the security cycle



Padvish EDR - Technologies



Padvish EDR - Sensors

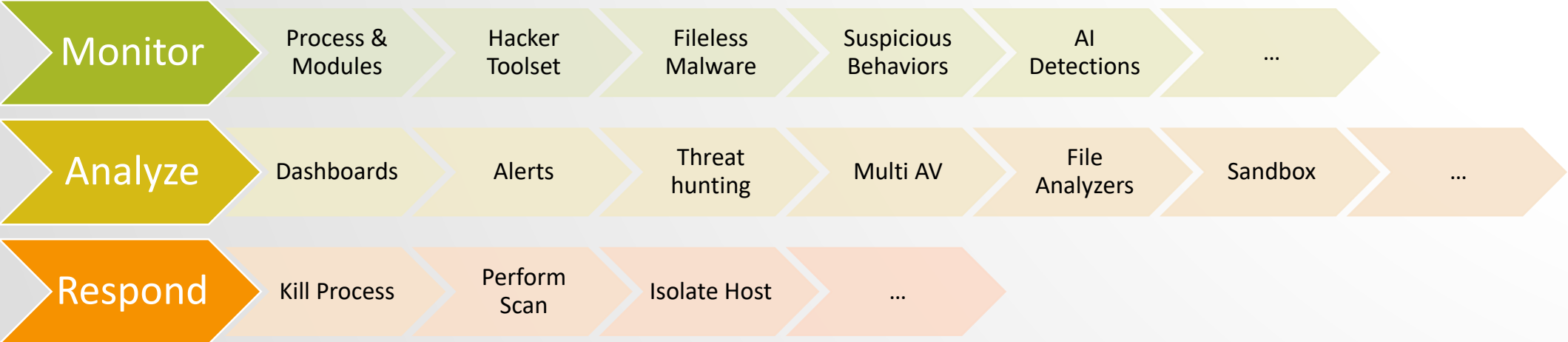


National Regulations Compliance

- ❖ Padvish EDR Expert enables government organizations to comply with multiple national regulations.
- ❖ Padvish EDR Provides Compliance for:
 - Virology Laboratory
 - Multi AV
- ❖ Padvish EDR is an Important Component for:
 - CSIRT
 - SOC



Padvish EDR



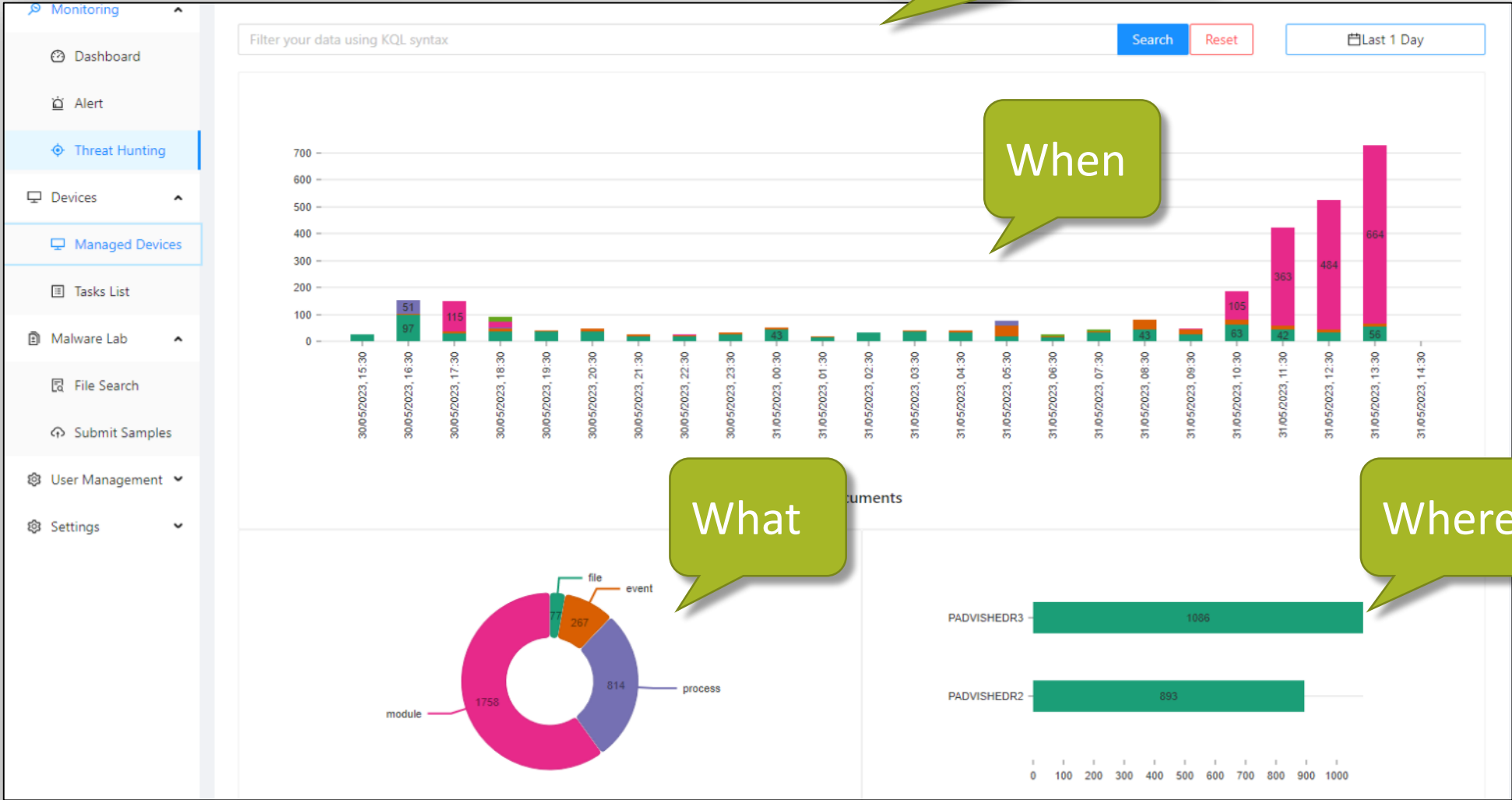
Threat Hunting

Search & Hunt

When

What

Where



EDR Alerts

The screenshot shows a web-based interface for monitoring and managing alerts. On the left is a navigation sidebar with options: Monitoring, Dashboard, Alert (selected), Threat Hunting, Devices, Malware Lab, User Management, and Settings. The main area features a filter section with fields for Name, Severity, Mitre Technique, Device Ip, DateTime (set to Last 1 Year), and Mitre Tactic. Below the filters is a table of alerts. Two callout boxes are overlaid on the interface: a green one pointing to the 'Automatic Alerts' text in the filter area, and another green one pointing to the information icon in the table's 'Information' column.

Name	Severity	Device	Date	Information
Hacktool Detected	Warning	PADVISHEDR2	5/31/2023, 1:55:56 PM	i 🗨
Suspicious RDP Connection	Warning	PADVISHEDR2	5/31/2023, 1:55:54 PM	i 🗨
Remote Software Installed	Warning	PADVISHEDR1	5/31/2023, 1:55:50 PM	i 🗨
Hacktool Detected	Warning	PADVISHEDR1	5/31/2023, 1:45:51 PM	i 🗨
Active Directory Script Installed	Warning	PADVISHEDR3	5/31/2023, 1:44:26 PM	i 🗨
Incorrect Password Input	Warning	PADVISHEDR2	5/31/2023, 1:44:16 PM	i 🗨
Malware Found	Warning	PADVISHEDR3	5/31/2023, 1:44:14 PM	i 🗨



Managed Devices

Choose a Response

The screenshot displays a web interface for managing devices. On the left is a navigation sidebar with options: Monitoring, Dashboard, Alert, Threat Hunting, Devices (expanded), Managed Devices (selected), Tasks List, Malware Lab, User Management, and Settings. The main area features a toolbar with buttons for 'Shut Down', 'Isolate', 'Kill Process', and 'IOC Scan'. Below the toolbar is a table of managed devices. The first row is highlighted in light blue and has a green callout bubble pointing to it with the text 'See Details'. The table columns are: Computer Name, Client Identifier, Product Type, Product Version, Guard Status, Os Name, Ip Addresses, Group Name, and Last Seen.

<input type="checkbox"/>	Computer Name	Client Identifier	Product Type	Product Version	Guard Status	Os Name	Ip Addresses	Group Name	Last Seen
<input checked="" type="checkbox"/>	PADVISHEDR2	81F5AEA1B78EFD469502BC320F3A4448	Corporate	2.0.2983.10545		Windows 10 Version 21H2 for x64-based Systems (Professional)	172.22.21.43	WorkStations	05/31/2023 14:05
<input type="checkbox"/>	PADVISHEDR2	9F37	Corporate	2.14.143.10570		Windows 10 Version 21H2 for x64-based Systems (Professional)	172.22.21.111	WorkStations	05/31/2023 13:56
<input type="checkbox"/>	WIN-BQOE8H7KTSU	2E5570EBCB7AA6E08A62416D91357547	Corporate	2.0.2983.10545		Windows Server 2019 Version 1809 for x64-based Systems	192.168.105.221		05/08/2023 13:00
<input type="checkbox"/>	ADMIN-PC	977D2B3DCACC855E1EE642673C59101F	Corporate	2.0.2983.10545		Windows 7 for x64-based Systems (Ultimate)	192.168.105.204		04/26/2023 12:48

See Details



Malware Lab

The screenshot displays the Malware Lab interface. On the left is a navigation sidebar with options: Dashboard, Alert, Threat Hunting, Devices, Managed Devices, Tasks List, Malware Lab (selected), File Search, Submit Samples, User Management, and Settings. The main area features a top toolbar with 'Delete', 'Download', and 'Send to sandbox' buttons. Below this are filter tabs for 'Malware', 'Benign', and 'Unknown'. The central section contains form fields for 'Diagnosis Reason', 'Detection Name', 'Analysis Report User', and 'Analysis Report Status', along with a 'Save Changes' button. To the right, a file details panel shows: Status: NewFile, File Size: 41.66 KB, File Name: System.Runtime.dll, Created Date: 5/6/2023, 7:21:55 AM, MD5, Sha1, Sha256, Sha384, and Sha512 hashes. At the bottom, a 'Scan Results' table shows clean results from Eset, Avira, Bitdefender, Microsoft, Padvish, and Kaspersky. Three green callout boxes highlight 'Sandbox', 'Analysis Progress', and 'Multi AV'.

Sandbox

Analysis Progress

Multi AV

Scan Results	File Info	Detail	Comment		
		Clean			Clean
		Clean			Clean
		Clean			Clean



Static File Analyzers

Scan Results **File Info** Detail Comment

NauzFileDetector

Engine Name	NauzFileDetector	Engine Version	0.0.1.0	File Status	Success	Scan Date	6 May 2023, 11:51:55
-------------	------------------	----------------	---------	-------------	---------	-----------	----------------------

DetectItEasy

MSMimeDetectorEngine

TrIDEngine

StringsEngine

APUnPackerEngine

Content

```
"NauzFileDetector": { 1 item
  "detects": [ 1 item
    0: { 3 items
      "filetype": "PE32"
      "parentfilepart": "Header"
      "values": [ 4 items
        0: { 5 items
          "info": "I386, 32-bit, DLL"
          "name": "Windows"
          "string": "Operation system: Windows(95)[I386, 32-bit, DLL]"
          "type": "Operation system"
          "version": "95"
        }
      ]
    }
  ]
}
```

PPT_2_401_3703_1_1401_1_2_1.1.pptx - PowerPoint

For any type of file



Practical Real-World Scenarios

Lets discuss some scenarios...

- ❖ Scenario 1: CERT published an IOC for recent attacks
- ❖ Scenario 2: News about an in-the-wild attack
- ❖ Scenario 3: Forensics of a threat detected by the system



Scenario 1: Scan for an IOC

- ❖ There were multiple cyber attacks during last week, targeting different government organizations.
- ❖ CERT is inspecting the attack, and has provided an IOC signature based on the forensics symptoms gathered.
- ❖ The admin is instructed to run the **IOC scan** on all the endpoints to find if the organization network is infected.



Scenario 1: IOC Rule

Rule Name:

Rule:

```
rule WEBSHELL_ASPX_MOVEit_Jun23_1 {
  strings:
    $s1 = "X-siLock-Comment" ascii fullword
    $s2 = "); string x = null;" ascii
    $s3 = "; if (!String.Equals(pass, " ascii
  condition:
    filesize < 150KB and 2 of them
}
```

Description:



Scenario 1: IOC Scan

Perform Task

* Type: Quick Scan

Path: Please Fill Scan Path

* Rules: WEBSHELL_ASPX_MOVEit_Jun23_1

New Rule

Devices

EDR-CLIENT-2 EDR-CLIENT-1 EDR-CLIENT-3

Cancel Create

Version	OS Name
59	Windows 10 Ve
59	Windows 10 Ve
59	Windows 10 Ve
59	Windows 10 Ve
59	Windows 10 Ve
59	Windows 10 Ve
330	Windows Serve



Scenario 1: IOC Task Results

Computer Name	Response	Command Type	Status	User Name	Date	Information
EDR-WIN7-E	IOC Scan	IOC Custom Scan	SUCCEEDED	test	Jul 15, 2023, 9:26:51 AM	
EDR-CLIENT-1		X				
EDR-WIN7-E		Command Type				
		IOC Custom Scan				
		path	C:\Users\Administrator\Downloads\sample\sample\361ce6a1-sample			
		rule[1]	WEBSHELL_ASPX_MOVEit_Jun23_1			
		type	0			



Scenario 2: In-The-Wild Attack

- ❖ News about an in-the-wild recent attack affecting systems globally has been announced.
- ❖ The News article contains symptoms and signs of the attack, such as the file names, registry paths, and sha256 hashes.
- ❖ The admin uses the **Threat Hunting** panel to inspect **historical data** to find which hosts has been affected by this attack.
- ❖ <https://blog.cyble.com/2023/03/23/cinoshi-project-and-the-dark-side-of-free-maas/>



Scenario 2: Threat Hunting

E3AAFD9F478B82CBB53EC020CDC2E00E0C4DE60A7F66A1166E54AB75B6A9E8C3 Search Reset Last 1 Months

Type	Name	Device	Data
event	Detected Malicious File	EDR-WIN-10 (192.168.6.100)	Trojan
event	Detected Malicious File	EDR-WIN-10 (192.168.6.100)	Trojan
file	Executable File Modified	EDR-WIN-10 (192.168.6.100)	C:\U

Total : 3 < 1 > 10 / page ▾

X

key.path	c:\users\administrator\desktop\sample 2\sample 2\ef9446a1
key.sha1	b929ed50142b9b43fb85c5b1ddb87ec00ca09f24
key.sha256	e3aafd9f478b82cbb53ec020cdc2e00e0c4de60a7f66a1166e54ab75b6a9e8c3
type	file
value.MD5	1798E35F14A67741F3425BA67373667D
value.accessType	11
value.action	QueueFileByPath
value.collectDate	1689494973
value.commandLine	C:\Windows\Explorer.EXE
value.forGuard	0
value.parentCommandLine	
value.parentProcessGuid	

Detail

PM	
PM	
PM	

2.2.4.83

Scenario 3: Forensics of a detected threat

- ❖ An **alert** is generated by Padvish EDR about the detection of a Hacktool on one of the corporate devices.
- ❖ The admin wants to know where the infection has come from (**the root cause**), and which systems it has infected so far.
- ❖ Also they want to **find and block** IP addresses of the botnet's C&C



Scenario 3: Finding the Root Cause

The screenshot shows a security dashboard with a sidebar on the left containing navigation items: Padvish, Threat Hunting, Dashboard, Alert (selected), Threat Hun, Devices, Malware La, Manage, and Settings. The main area displays a list of alerts with columns for Severity, Date, Name, and De. A modal window is open, showing details for a specific alert:

dangerLevel	Critical
timeStamp	2023-07-15T17:51:51.52727Z
alert	Mimikatz
clientName	EDR-WIN-10
ip	192.168.6.100
id	7d297581-55c9-4d5a-9e78-4422abd75191
result.key.guid	4d6f2b65-642a-4915-b2aa-437e58499353
result.type	event
result.value.MD5	0818699D065AFCB1F397D578D3708DC2
result.value.accessType	11
result.value.collectDate	1689443489
result.value.commandLine	"C:\Users\Administrator\Downloads\AnyDesk.exe" --l
result.value.displayName	C:\Users\Administrator\Documents\mimidrv.sys
result.value.malwareName	IOC-HackTool.Win32.Mimikatz.any1

Red arrows point to the **result.value.commandLine** and **result.value.displayName** fields. A 'Reset' button is visible on the right side of the modal.

Scenario 3: Threat Hunting

computerName:"EDR-WIN-10" and value.parentProcessPath:"C:\Users\Administrator\Downloads\AnyDesk.exe"


Search

Type	Name	Device	Data	Extra	Date	Detail
file	Executable File Modified	EDR-WIN-10 (192.168.6.100)	C:\Users\Administrator\Documents...	Action Taken: QueueFileByPath C:\Users\Administrator\Documents\nmap-7.93-setup.exe	Jul 15, 2023, 10:29:24 PM	
event	Detected Malicious File	EDR-WIN-10 (192.168.6.100)	HackTool.Win32.mimikatz.bu	Command Line: "C:\Users\Administ...	Jul 15, 2023, 10:21:38 PM	
event	Detected Malicious File	EDR-WIN-10 (192.168.6.100)	HackTool.Win32.Mimikatz.drv	Command Line: "C:\Users\Administ...	Jul 15, 2023, 10:21:38 PM	
event	Detected Malicious File	EDR-WIN-10 (192.168.6.100)	HackTool.Win32.Mimikatz.sys3	Command Line: "C:\Users\Administ...	Jul 15, 2023, 10:21:38 PM	
event	Detected Malicious File	EDR-WIN-10 (192.168.6.100)	HackTool.Win32.Mimikatz.T1a	Command Line: "C:\Users\Administ...	Jul 15, 2023, 10:21:38 PM	
event	Detected Malicious File	EDR-WIN-10 (192.168.6.100)	HackTool.Win32.mimikatz.bu	Command Line: "C:\Users\Administ...	Jul 15, 2023, 10:21:38 PM	
event	Detected Malicious File	EDR-WIN-10 (192.168.6.100)	HackTool.Win32.Mimikatz.drv	Command Line: "C:\Users\Administ...	Jul 15, 2023, 10:21:38 PM	
event	Detected Malicious File	EDR-WIN-10 (192.168.6.100)	HackTool.Win32.Mimikatz.sys3	Command Line: "C:\Users\Administ...	Jul 15, 2023, 10:21:38 PM	



Scenario 3: Threat Hunting

computerName:"EDR-WIN-10" and value.processPath:"nmap" Search

Network Connection	EDR-WIN-10 (192.168.6.100)	216.239.38	value.parentProcessPath	C:\Windows\System32\cmd.exe	+ -
Process Started	EDR-WIN-10 (192.168.6.100)		value.pid	1696	+ -
Process Started	EDR-WIN-10 (192.168.6.100)		value.processUsername	EDR-WIN-10\Administrator	+ -
Process Started	EDR-WIN-10 (192.168.6.100)		value.process	C:\Program Files (x86)\Nmap\nmap.exe	+ -
Process Started	EDR-WIN-10 (192.168.6.100)		value.processGuid	8c0d047d-27e3-4fb5-99e8-880e2b35d0b4	+ -
Executable File Modified	EDR-WIN-10 (192.168.6.100)	c:\program	value.processPath	C:\Program Files (x86)\Nmap\nmap.exe	+ -
Process Started	EDR-WIN-10 (192.168.6.100)		value.protocol	-	+ -
			value.remotelp	216.239.38.120	+ - 
			value.remotePort	443	+ -



Scenario 3

Filter your data using KQL syntax Search Reset Last 1 Months

value.remotelp: "21..." X

Type	Name	Device	Data	Extra	Date	Detail
event	Network Connection	EDR-WIN-10 (192.168.6.100)	216.239.38.120:443	Command Line: "C:\Program Files\...	Jul 15, 2023, 2:47:41 PM	
event	Network Connection	EDR-WIN7-E (192.168.6.100)	216.239.38.120:443	Command Line: "C:\Program Files\...	Jul 15, 2023, 12:34:48 PM	
event	Network Connection	EDR-WIN7-E (192.168.6.100)	216.239.38.120:80	Command Line: "C:\Program Files\...	Jul 15, 2023, 12:31:40 PM	
event	Network Connection	EDR-WIN-10 (192.168.6.100)	216.239.38.120:443	Command Line: "C:\Program Files ...	Jul 13, 2023, 12:08:52 PM	
event	Network Connection	EDR-SER-2019 (192.168.6.100)	216.239.38.120:443	Command Line: "C:\Program Files\...	Jul 12, 2023, 3:07:14 PM	
event	Network Connection	EDR-SER-2019 (192.168.6.100)	216.239.38.120:80	Command Line: "C:\Program Files\...	Jul 12, 2023, 3:03:56 PM	
event	Network Connection	EDR-SER-2019 (192.168.6.100)	216.239.38.120:80	Command Line: "C:\Program Files ...	Jul 12, 2023, 3:03:56 PM	
event	Network Connection	EDR-WIN7-E (192.168.6.100)	216.239.38.120:80	Command Line: "C:\Program Files ...	Jul 12, 2023, 3:02:56 PM	
event	Network Connection	EDR-SER-2019 (192.168.6.100)	216.239.38.120:443	Command Line: "C:\Program Files\...	Jul 12, 2023, 3:02:44 PM	
event	Network Connection	EDR-SER-2019 (192.168.6.100)	216.239.38.120:443	Command Line: "C:\Program Files\...	Jul 4, 2023, 5:52:05 PM	

00 AM: 19

9 10 11 12

EDR

Requirements and Challenges in Organizations

7x24 - Security Expert Team

- Finding, Hiring, Keeping enough Experts for a 7x24 team
- Teaching, Ensure being Up-to-date
- Creating Management and Evaluation Structure

The Technical Gap between Organizations' Goals and Business and the Security Team

- The security team can't report to the upper management
- It won't get enough and consistent attention
- Gets abandoned and unmotivated over time

Limited View of Attacks

- You only monitor your organization network, so your view of attacks is biased
- You won't see latest attacks and techniques, unless you are attacked.
- You're always one-step behind in experience

Alert Fatigue

- Most of the time you are resolving false positives
- Makes the team indifferent to alerts over time

Unbalanced Responsibilities vs Authorities

- Preventing cyber-attacks is a great responsibility, which cannot be placed on the security team with its limited authorities

We need a solution
to these challenges...

Managed Detection and Response

Technology Compare

EDR vs **MDR**



Lower Cost

Easier Maintenance

Responsibility (SLA)

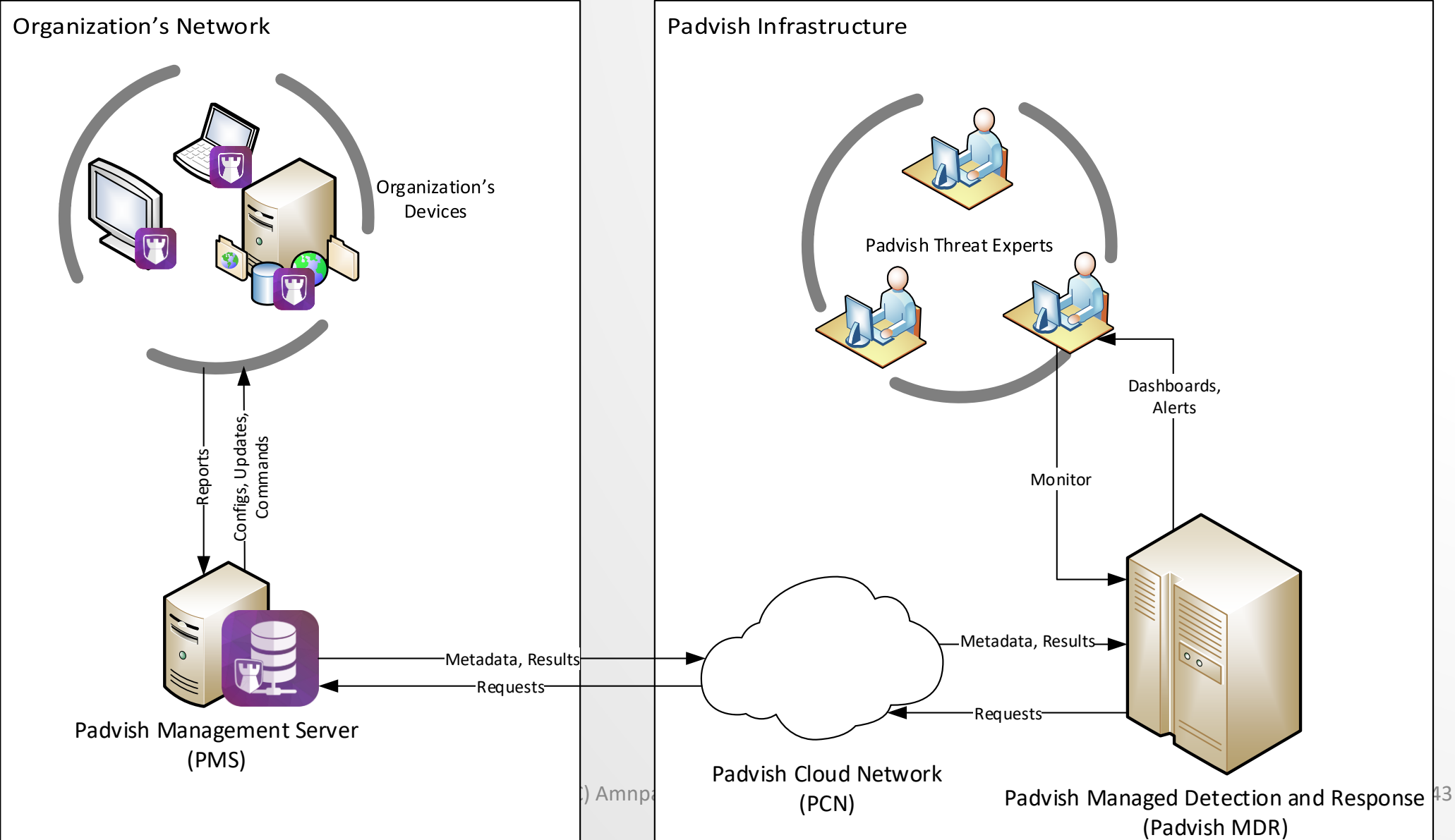


Need more help?

❖ Padvish MDR is the next step



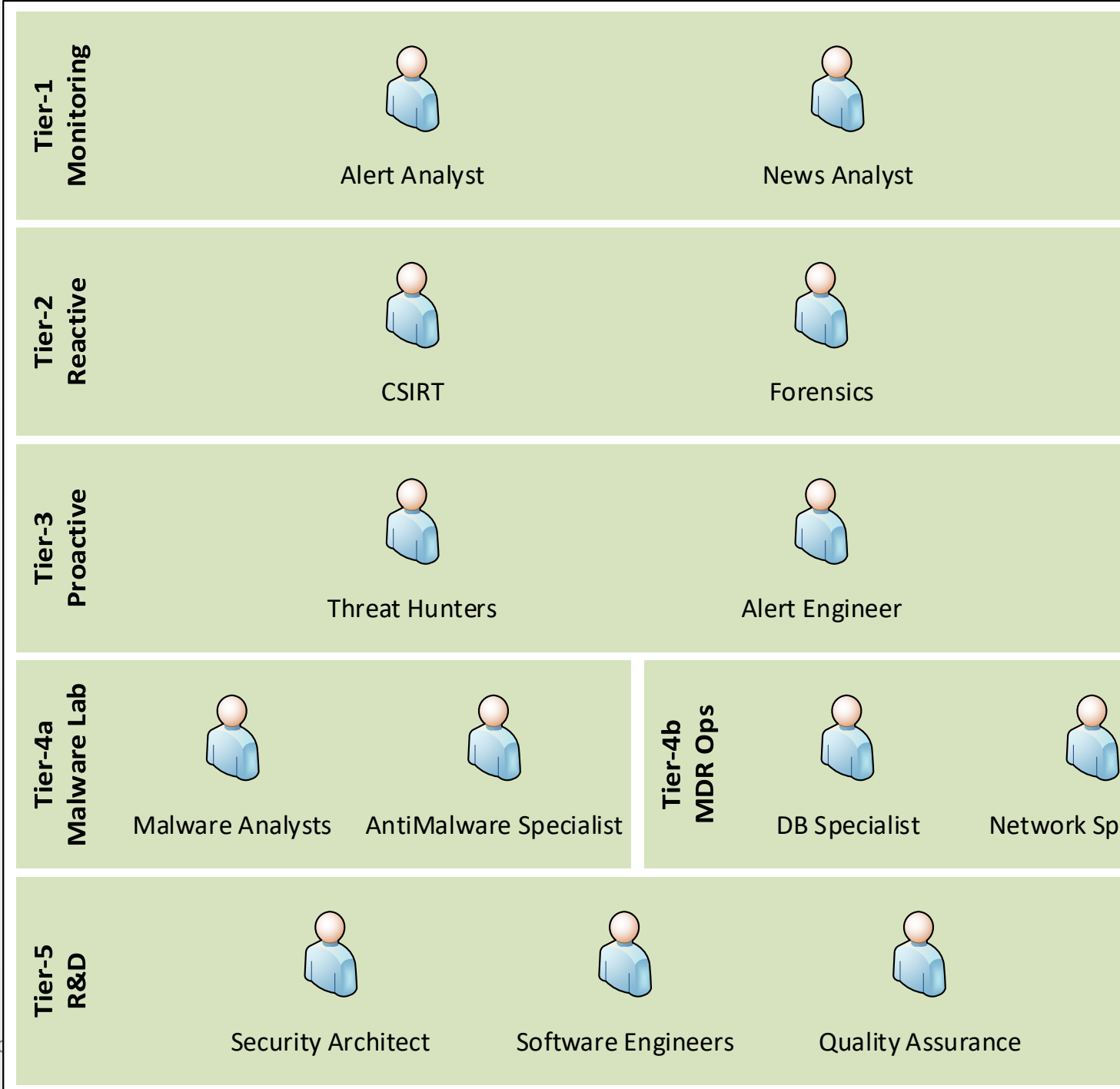
Padvish MDR Infrastructure



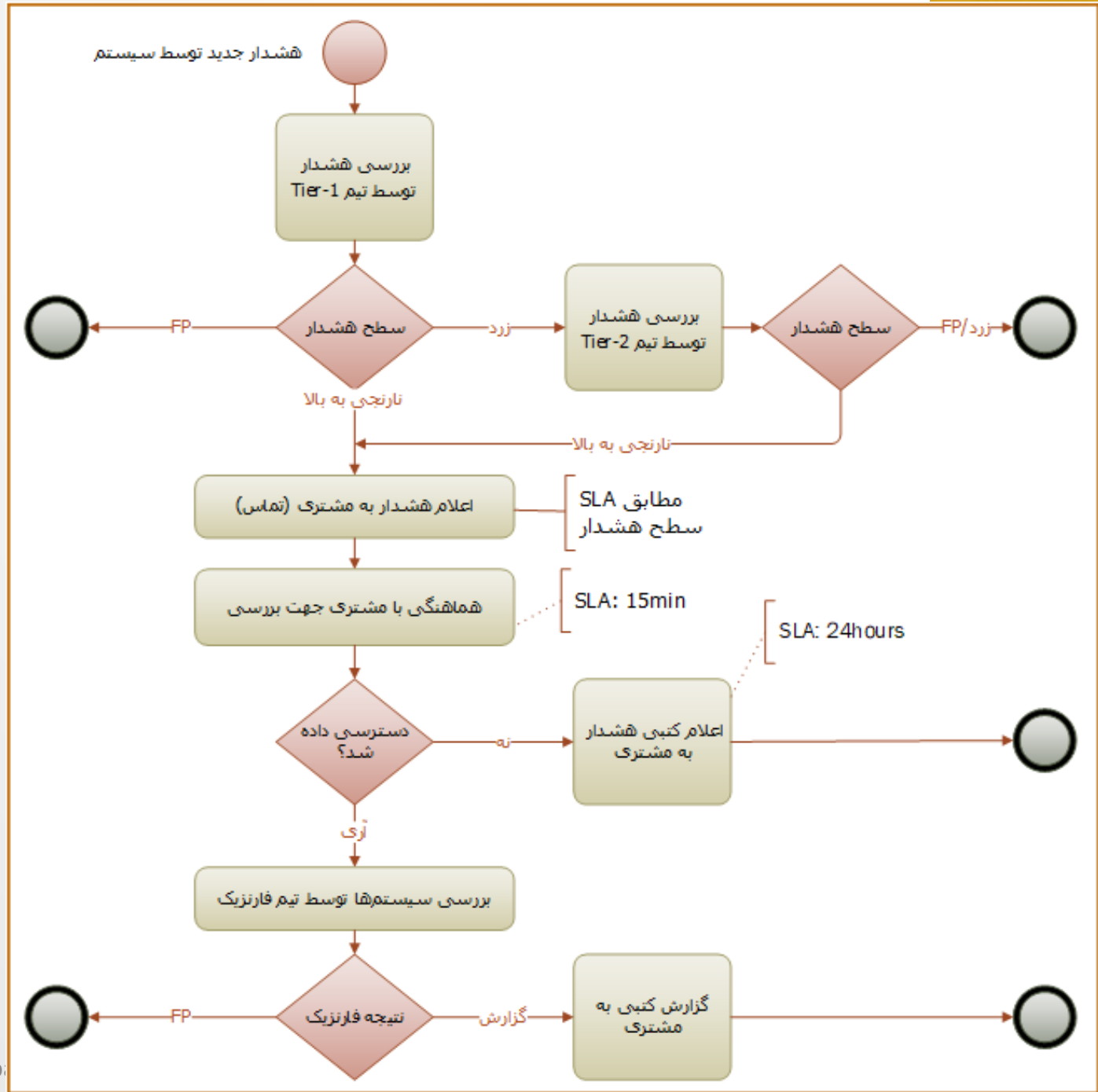
Padvish MDR – Alert SLA

سیاه (بررسی فوری)	قرمز (تماس فوری)	نارنجی (غیر فوری)	زرد (غیر قطعی)	سطح هشدار
خطر فوری هک خطر هک جدی و نزدیک به قطعی است و باید فوراً بررسی شود	نیازمند کسب اطلاع فوری رفتار مشکوک مشاهده شده است که احتمال دارد توسط ادمین انجام شده باشد	بررسی فوریت ندارد آلودگی بدافزاری غیر هک، یا بقایای یک هک قدیمی	احتمال هشدار کاذب هشدار باید توسط تیم انسانی سطح بندی شود	شرح
✓	✓	✓	✗	اعلام هشدار از طریق تماس
۲۴×۷	۲۴×۷	ساعات کاری (۷ صبح تا ۷ شب)	-	زمان تماس
الزامی	در صورت عدم اطلاع ادمین	با نظر ادمین	-	بررسی الزامی
۱ ساعت	۱ روز	۱ هفته	-	مهلت آغاز بررسی
✓	✓	✗	-	اعلام کتبی هشدار

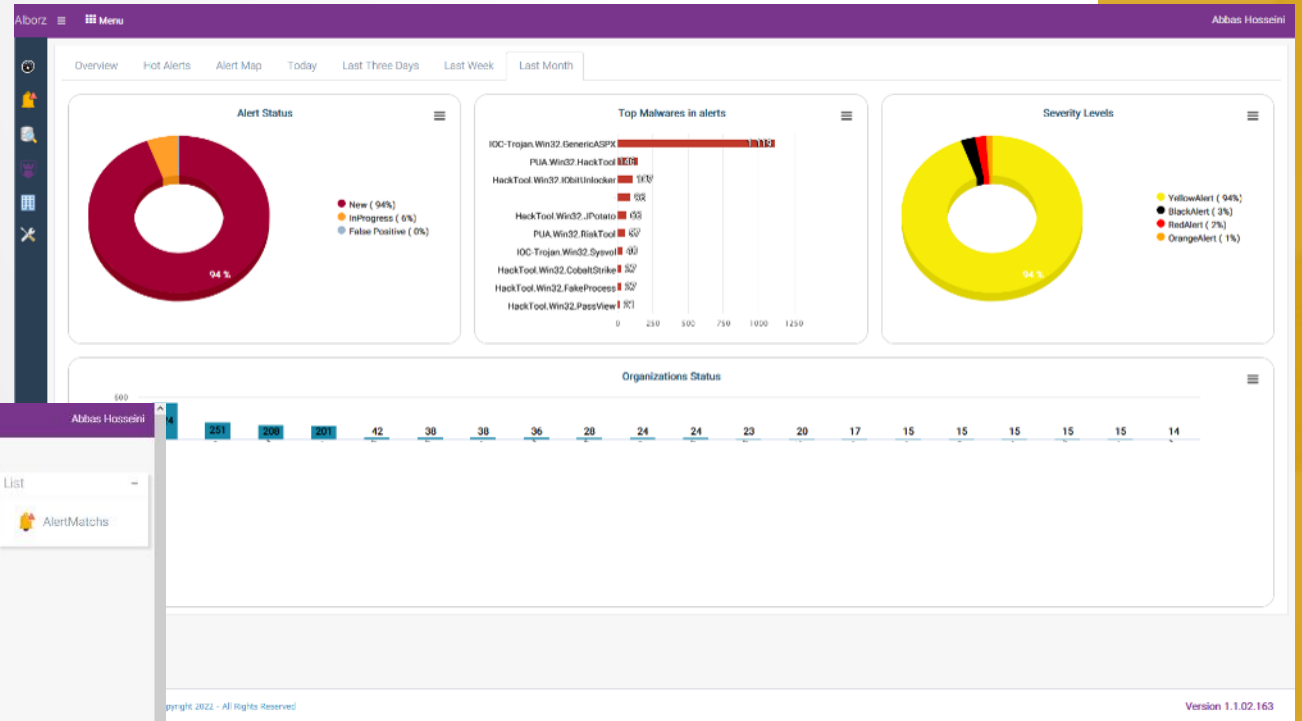
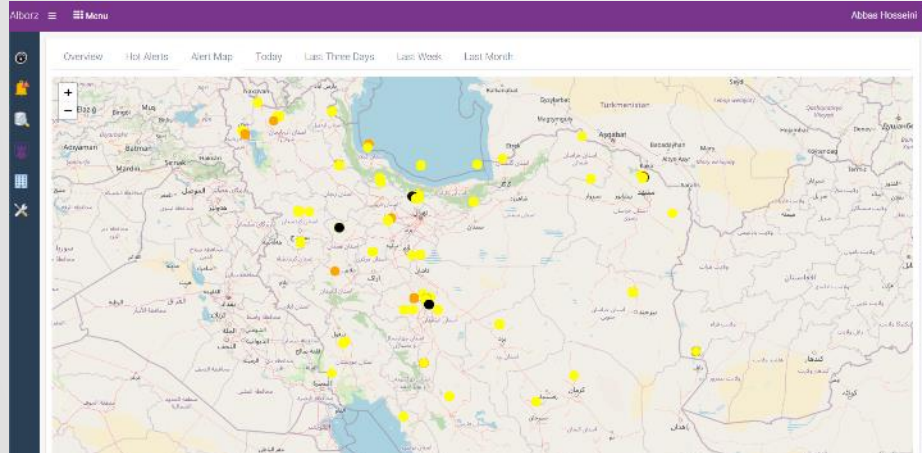
Padvish MDR Tiering



Padvish MDR Alerting Process



Padvish MDR



Alert Management > AlertMatch Management

AlertMatches

Show 10 records

Row Num	Alert Query	Padvish Server	MDRAlert Date	Malware Name	Detection Type	Response Status	Ticket ID
1	New Alert by filter		07/04/2023 14:28:21	PUA.Win32.HackTool.Panicom-264120875	-	New	
2	New Alert by filter		07/04/2023 13:44:55	HackTool.Win32.IKbitLocker	-	New	
3	New Alert by filter		07/03/2023 17:07:46	PUA.Win32.HackTool.Panicom-264120875	-	New	
4	New Alert by filter		07/03/2023 17:01:20	HackTool.Win32.JIPuato-286327112	-	New	
5	webshell alert?		07/03/2023 16:54:01	Backdoor.HTML.WebShell-679077987	-	InProgress	126275
6	New Alert by filter		07/03/2023 16:52:51	HackTool.Win32.PowerTool	-	New	
7	New Alert by filter		07/03/2023 15:52:26	PUA.Win32.HackTool.Panicom-264120875	-	New	
8	New Alert by filter		07/03/2023 15:21:41	HackTool.Win32.PassView	-	New	
9	New Alert by filter		07/03/2023 15:13:14	-	Tamper Attempt By RDP-Session	New	
10	New Alert by filter		07/03/2023 14:38:20	-	Malware Infection By RDP-Session	New	

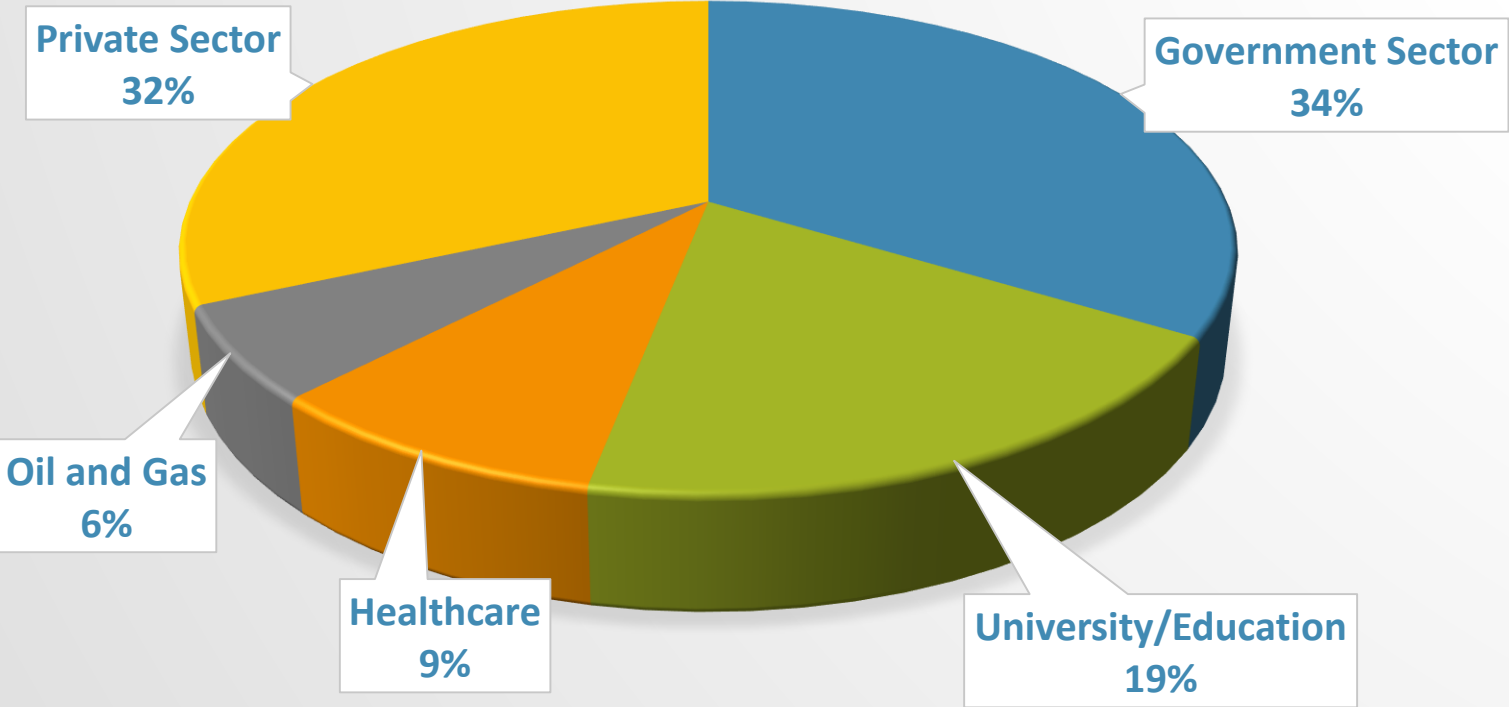
Showing 1 to 10 of 18487 records

First Prev 1 2 3 4 5 - 1549 Next Last



Padvish Antivirus – Real-world Performance

Recent Cyber-Attacks Prevented by Padvish Antivirus
(Last 12 Month)



Thanks