#CS4CA
CYBER SECURITY FOR CRITICAL ASSETS
APAC

Implementing threat detection and response from a Zero Trust perspective for Critical Infrastructure

Paul Kwon
CEO / PAGO Networks, Inc.

PAGO NETWORKS | DeepACT Managed Detection and Response

Introduction

Topic

The industry has lots of cybersecurity technologies to protect the critical infrastructure. But can we say all works well or just deployed? During this session, we discuss what the industry found and how the industry applies the actionable detection and response methodologies against the existing threat or the future infiltrated threat from a ZeroTrust perspective. A Zero Trust architecture can be applied to the various areas, but we will take a concept of Zero Trust Approach to Malware-based attacks for critical infrastructure.

– **Paul Kwon**, Founder & CEO, **PAGO Networks**

Focus on

Critical Infrastructure – OT / IT (On-prem / Cloud)

Threat Types

- MALware
- MALicous Activities

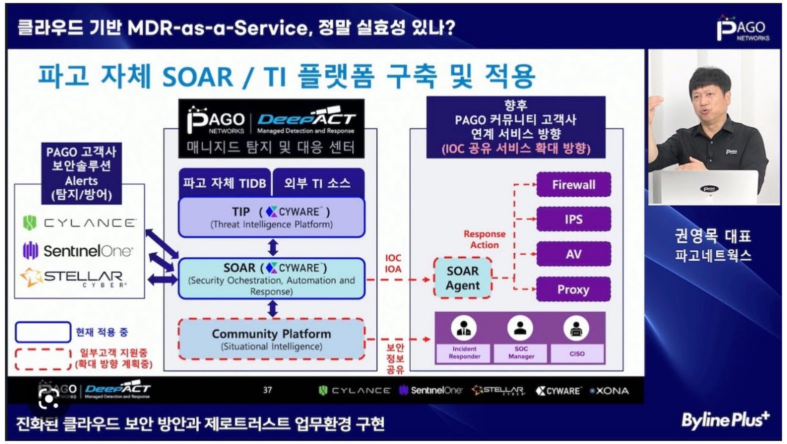
VS.

Technologies

- Detection / Response
- EPP, EDR, NDR, XDR

How to act? , What is the process?

Who I am – Leader, Threat Detection & Response



클라우드 기반 MDR-as-a-Service, 정말 실효성 있나?

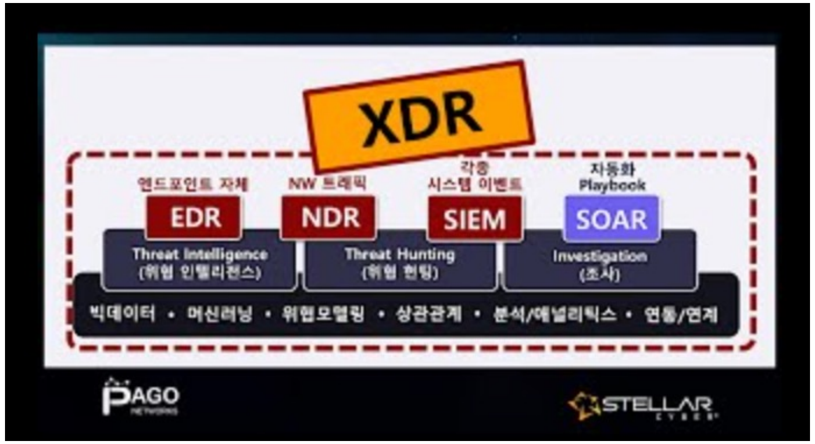
파고 자체 SOAR / TI 플랫폼 구축 및 적용

PAGO NETWORKS | DEEPACT Managed Detection and Response
매니지드 탐지 및 대응 센터
PAGO 고객사 보안솔루션 Alerts (탐지/방어)
CYLANCE
SentinelOne
STELLAR CYBER
파고 자체 TIDB
외부 TI 소스
TIP (CYWARE)
(Threat Intelligence Platform)
SOAR (CYWARE)
(Security Ochestration, Automation and Response)
Community Platform
(Situational Intelligence)
향후
PAGO 커뮤니티 고객사
연계 서비스 방향
(IOC 공유 서비스 확대 방향)
IOC
IOA
SOAR Agent
Response Action
Firewall
IPS
AV
Proxy
보안 정보 공유
Incident Responder
SOC Manager
CISO
현재 적용 중
일부고객 지원중
(확대 방향 계획중)
37
CYLANCE SentinelOne STELLAR CYWARE XONA

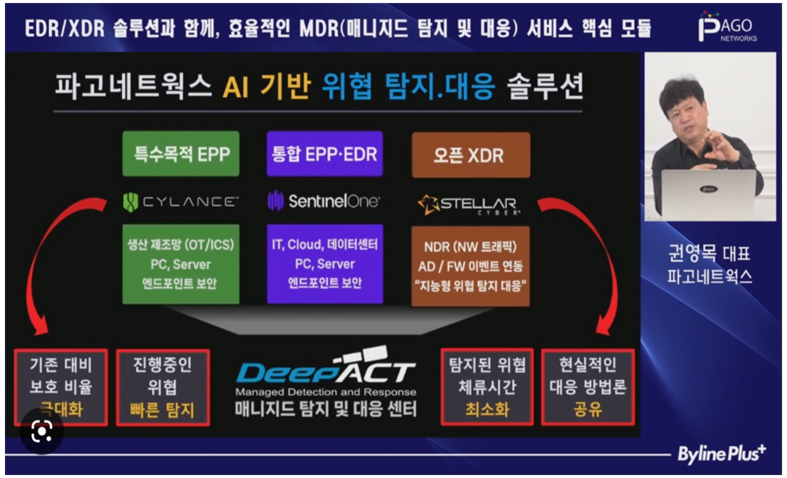
권영목 대표
파고네트웍스

진화된 클라우드 보안 방안과 제로트러스트 업무환경 구현

Byline Plus+



XDR
엔드포인트 자체
NW 트래픽
각종 시스템 이벤트
자동화 Playbook
EDR
NDR
SIEM
SOAR
Threat Intelligence (위협 인텔리전스)
Threat Hunting (위협 헌팅)
Investigation (조사)
빅데이터 • 머신러닝 • 위협모델링 • 상관관계 • 분석/애널리틱스 • 연동/연계
PAGO NETWORKS
STELLAR CYBER



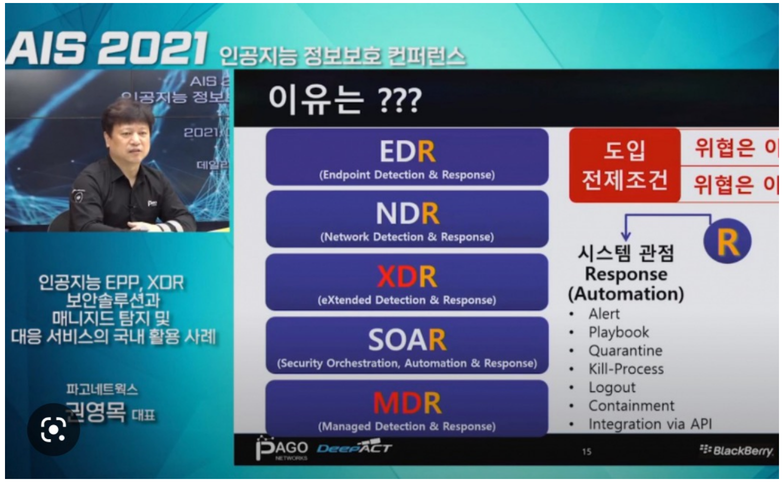
EDR/XDR 솔루션과 함께, 효율적인 MDR(매니지드 탐지 및 대응) 서비스 핵심 모듈

파고네트웍스 AI 기반 위협 탐지.대응 솔루션

특수목적 EPP
통합 EPP·EDR
오픈 XDR
CYLANCE
SentinelOne
STELLAR CYBER
생산 제조망 (OT/ICS) PC, Server 엔드포인트 보안
IT, Cloud, 데이터센터 PC, Server 엔드포인트 보안
NDR (NW 트래픽) AD / FW 이벤트 연동 "지능형 위협 탐지 대응"
기존 대비 보호 비율 극대화
진행중인 위협 빠른 탐지
DEEPACT Managed Detection and Response
매니지드 탐지 및 대응 센터
탐지된 위협 체류시간 최소화
현실적인 대응 방법론 공유

권영목 대표
파고네트웍스

Byline Plus+



AIS 2021 인공지능 정보보호 컨퍼런스

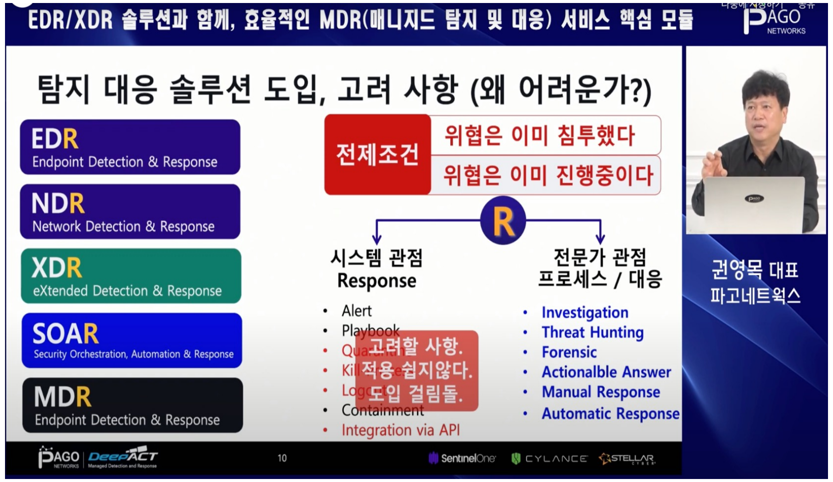
이유는 ???

인공지능 EPP, XDR
보안솔루션과
매니지드 탐지 및
대응 서비스의 국내 활용 사례

파고네트웍스
권영목 대표

EDR
(Endpoint Detection & Response)
NDR
(Network Detection & Response)
XDR
(eXtended Detection & Response)
SOAR
(Security Orchestration, Automation & Response)
MDR
(Managed Detection & Response)
도입 전제조건
위협은 이
위협은 이
R
시스템 관점
Response
(Automation)
15
BlackBerry

- Alert
- Playbook
- Quarantine
- Kill-Process
- Logout
- Containment
- Integration via API



EDR/XDR 솔루션과 함께, 효율적인 MDR(매니지드 탐지 및 대응) 서비스 핵심 모듈

탐지 대응 솔루션 도입, 고려 사항 (왜 어려운가?)

EDR
Endpoint Detection & Response
NDR
Network Detection & Response
XDR
eXtended Detection & Response
SOAR
Security Orchestration, Automation & Response
MDR
Endpoint Detection & Response
전제조건
위협은 이미 침투했다
위협은 이미 진행중이다
R
고려할 사항.
적용 쉽지않다.
도입 걸림돌.
10
SentinelOne CYLANCE STELLAR

시스템 관점
Response

- Alert
- Playbook
- Qua…
- Kil…
- Log…
- Containment
- Integration via API

전문가 관점
프로세스 / 대응

- Investigation
- Threat Hunting
- Forensic
- Actionalble Answer
- Manual Response
- Automatic Response

권영목 대표
파고네트웍스

PAGO NETWORKS | DEEPACT Managed Detection and Response

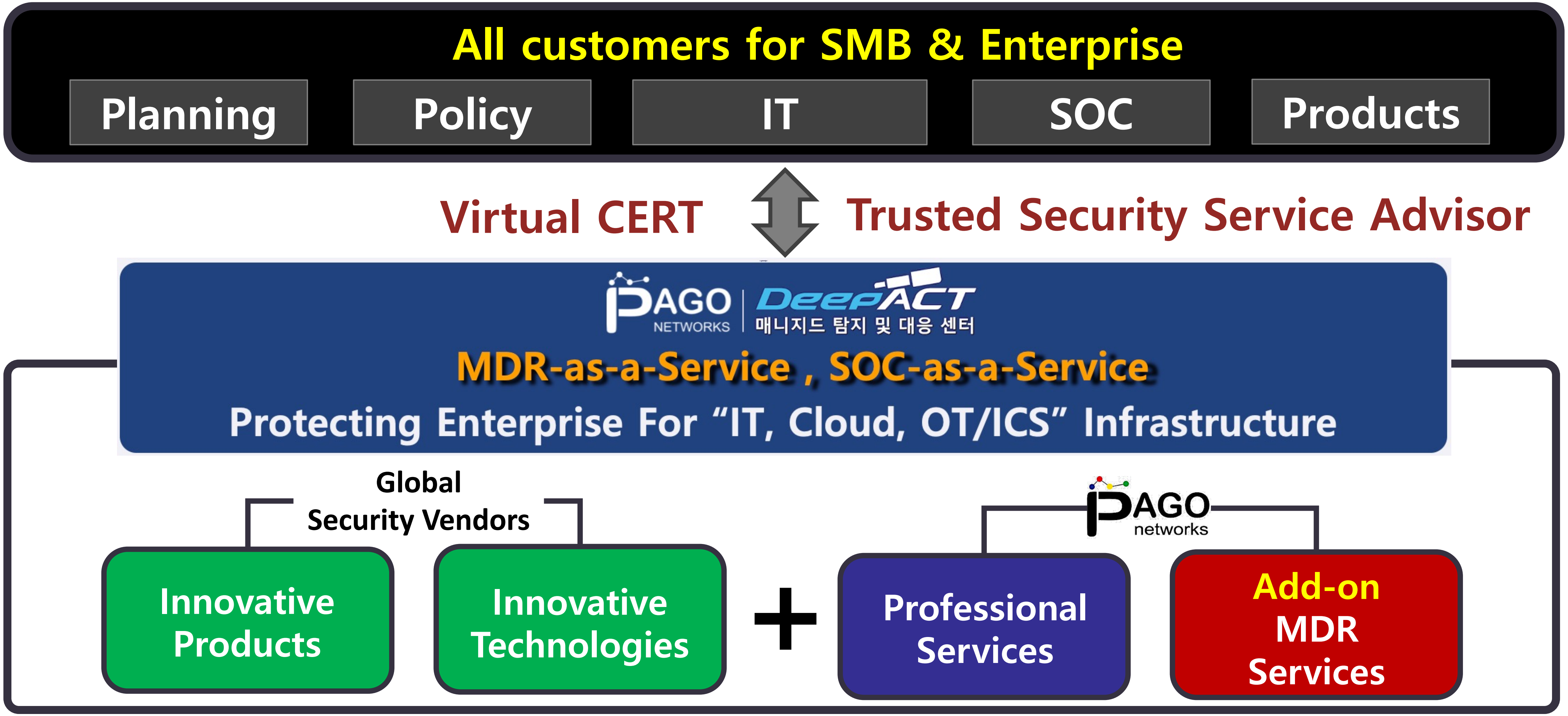
Who PAGO Networks is

PAGO NETWORKS

Not only sells the products,

But also provides the MDR services.

The Role of PAGO Networks MDR Service



All customers for SMB & Enterprise

Planning

Policy

IT

SOC

Products

Virtual CERT

Trusted Security Service Advisor

PAGO NETWORKS | DEEPACT 매니지드 탐지 및 대응 센터

MDR-as-a-Service , SOC-as-a-Service

Protecting Enterprise For “IT, Cloud, OT/ICS” Infrastructure

Global Security Vendors

Innovative Products

Innovative Technologies

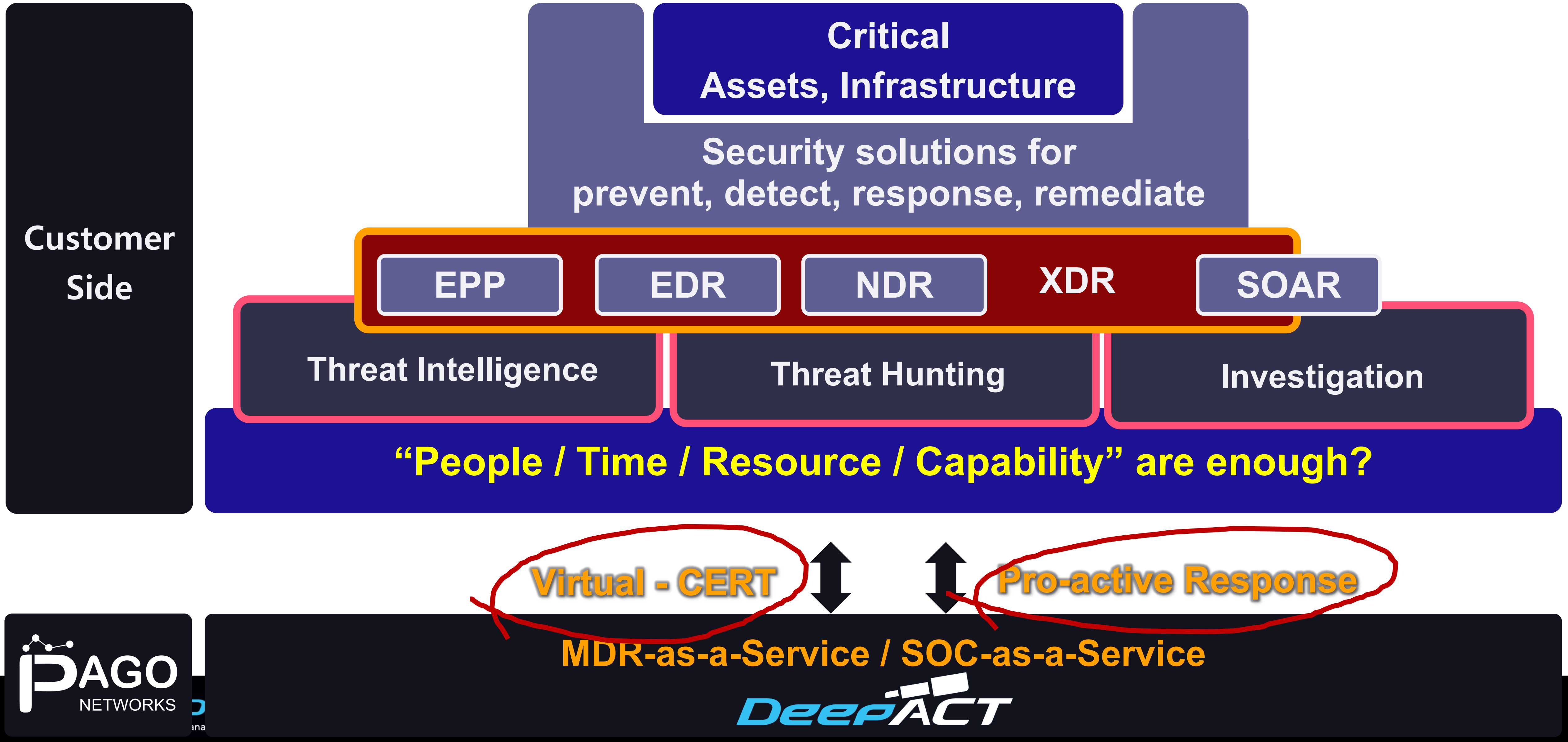
+

PAGO networks

Professional Services

Add-on MDR Services

PAGO is the virtual CERT for all customers



Customer Side

Critical Assets, Infrastructure

Security solutions for prevent, detect, response, remediate

EPP

EDR

NDR

XDR

SOAR

Threat Intelligence

Threat Hunting

Investigation

“People / Time / Resource / Capability” are enough?

Virtual - CERT

Pro-active Response

MDR-as-a-Service / SOC-as-a-Service

PAGO NETWORKS

DeepACT

PAGO NETWORKS | DeepACT Managed Detection and Response

MDR (Managed Detection & Response) Center

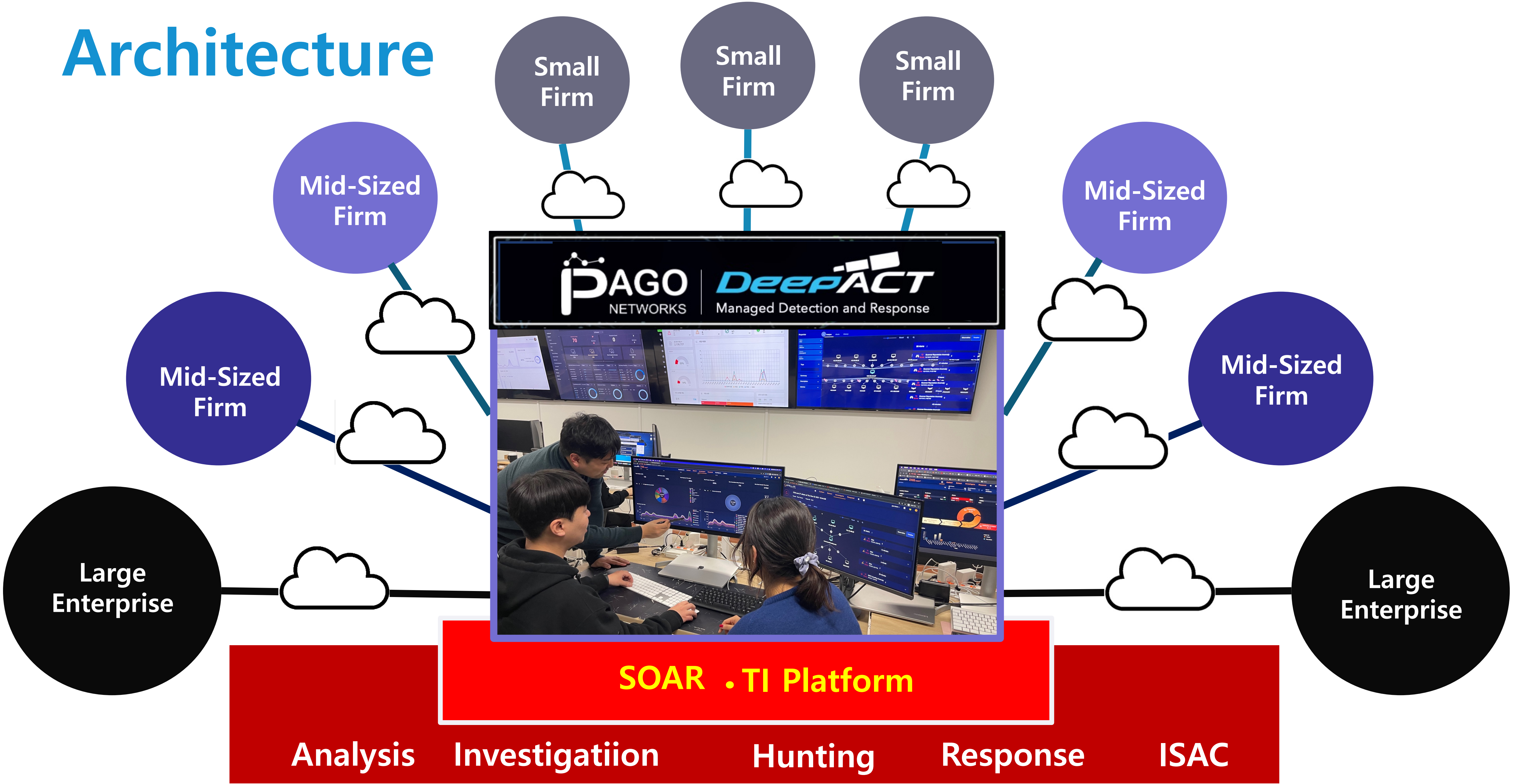
PAGO NETWORKS | DeepACT Managed Detection and Response

Threat Analyst

Threat Hunter

Threat Research

Architecture



Small Firm

Small Firm

Small Firm

Mid-Sized Firm

Mid-Sized Firm

Mid-Sized Firm

Mid-Sized Firm

Large Enterprise

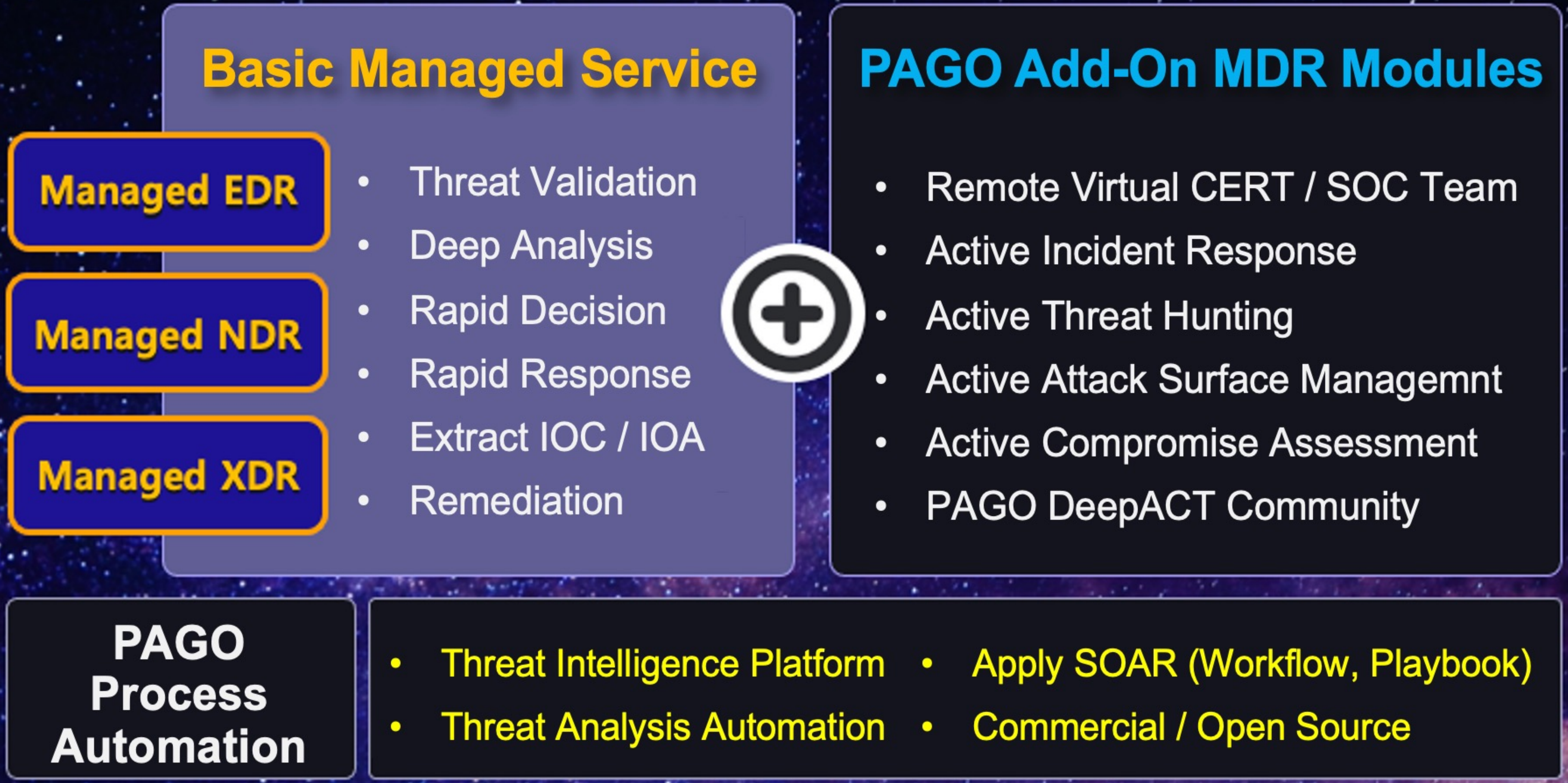
Large Enterprise

PAGO NETWORKS | DeepACT Managed Detection and Response

SOAR • TI Platform

Analysis Investigatiion Hunting Response ISAC

PAGO DeepACT – MDR Contents



Basic Managed Service

- Managed EDR
- Managed NDR
- Managed XDR

- Threat Validation
- Deep Analysis
- Rapid Decision
- Rapid Response
- Extract IOC / IOA
- Remediation

PAGO Add-On MDR Modules

- Remote Virtual CERT / SOC Team
- Active Incident Response
- Active Threat Hunting
- Active Attack Surface Managemnt
- Active Compromise Assessment
- PAGO DeepACT Community

PAGO Process Automation

- Threat Intelligence Platform
- Threat Analysis Automation
- Apply SOAR (Workflow, Playbook)
- Commercial / Open Source

Our customers

ultium cells
rho motion

LG Chem
LG Energy Solution
LG
LG CNS
LX Hausys
Formerly LG Hausys
KOLON
Seohan

SEOUL SEMICONDUCTOR
INTERPARK
DONGSUH
SL Corporation
SHINSUNG E&G
HYUNDAI WELDING
LOCA

ORION
DONGKUK STEEL
Kiswire
Harim
megastudy
주식회사 코렌스 KORENS
HAITAI 해태
KPX Holdings

NEXEN CORP.
KISWEL
KEY FOUNDRY
mcNEX
APS Holdings
YOUNG POONG
울산상공회의소
bhc

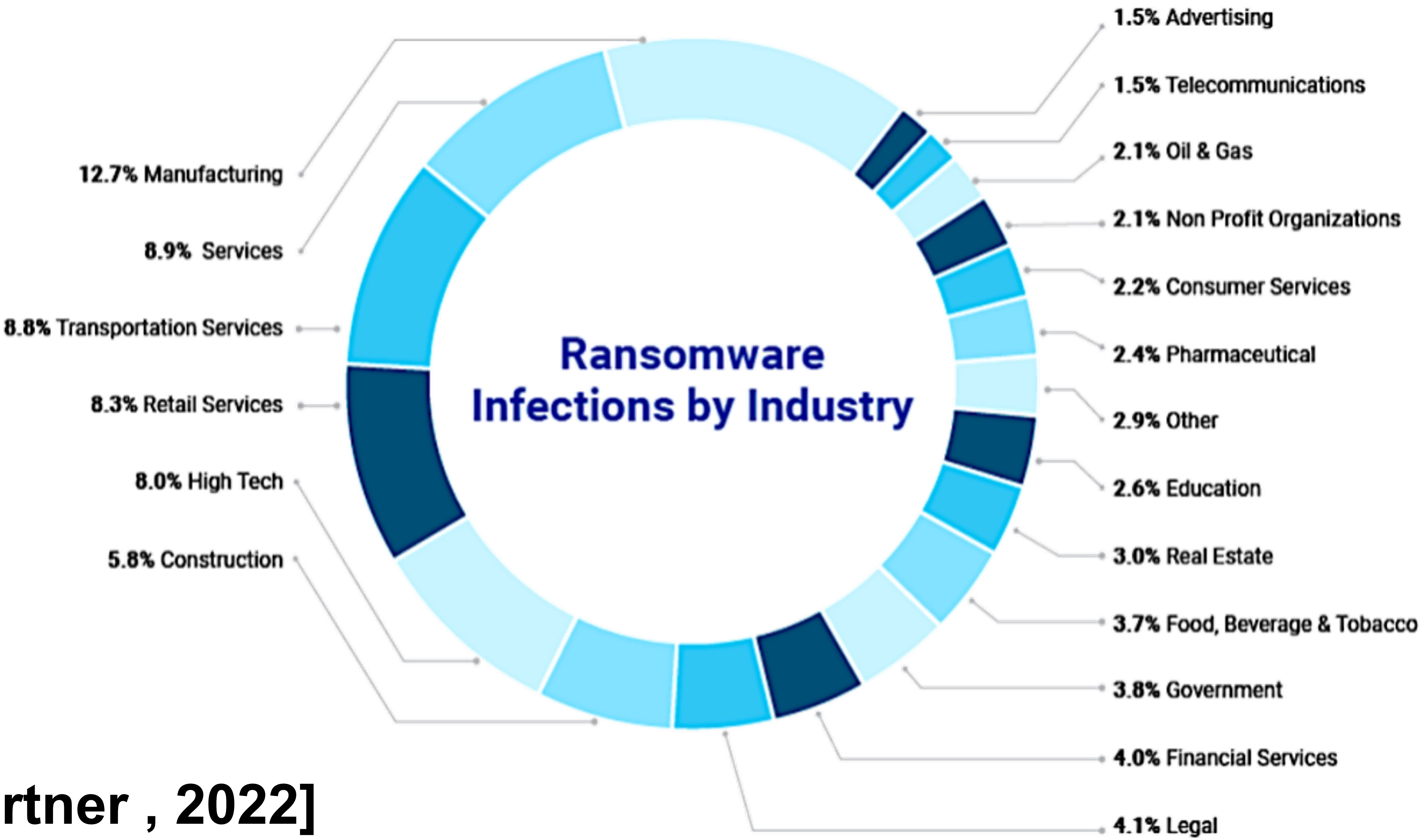
KG Chemical
Smartro
AEKYUNG
Kyung Dong City Gas
SAJO
Zero to Seven
AJUSTEEL
SIB (주)선인

INZI CONTROLS
한국OSG
KICA 한국정보인증
KOREA RATINGS
Duckyang Ind. Co., Ltd.
HANDOK 한독
COSMAX

WOOSIN 우신스틸
SML 삼광의료재단
(주) 엠에스정밀 MS Precision Co.,Ltd.
kukdong KUKDONG SINCE 1967
(주)구일엔지니어링
ILSUNG HISCO
InkTec

DAECHANG FORGING Co.,Ltd.
igaworks
삼원FA
은산해운항공(주) KOREA AEO
TAEYOUNG INDUSTRY
장보고식자재마트
YONWOO
DGB유페이

How to Apply Threat Detection & Response for all Critical Infrastructure



[Gartner , 2022]

Only ”Ransomware” detection enough?

No !!!

If we were targeted by Ransomware,
It’s Not one malware.

But various malware & malicious activities were already penetrated !!

- External Vulnerability Scanning (and Exploit)
- Internal Vulnerability Scanning (and Exploit)
- Backdoor / Trojan / Bruteforce / Exploit Tools
- Exploit Active Directory & Critical Systems
- Steal Admin-Level Account / Password
- Steal User-Level Account / Password
- Steal Browser Cache (URL, Access Information)
- Steal Organization Employee Structure
- Steal Infrastructure Architecture
- Disable the Existing Security Tools (AV, FW, OS Service)
- **Data Breach**
- **Data Encryption (Only here for a specific ransomware)**
- Destroy All Data-Backup (On-Prem / Cloud Backup)
- Malware Duplication
- Technology to increase Dwell-Time

Here is the real example

- **When we detect the below malware simultaneously, What does it mean ?**

✓ Gmer – Rootkit / Kill Process

✓ YDArk – Rootkit / Kill AV & FW

✓ Processhacker – Kill System Process

✓ Mimikatz – Password Dump / Exploit

it's Important to identify

- What types of malware are detected?
- What is their purpose?
- What will be the next step from them

Right, We have been Targeted by Ransomware !!!

Let's see the current EPP / EDR / NDR / XDR

- **Not Easy to know the next step !!!**
  - ✓ Classification - Malware
    - ✓ Trojan, Hacking-Tool, Backdoor, Rootkit, Keylogger, Worm, Brute-Force
  - ✓ Classsification - PUP
    - ✓ Adware, P2P, Free Update, Crack-Tool
  - ✓ Classification - Tools
    - ✓ Remote Access, Remote Control, Remote Shell, Proxy, File Transfer

How can we know the purpose of malware exactly?

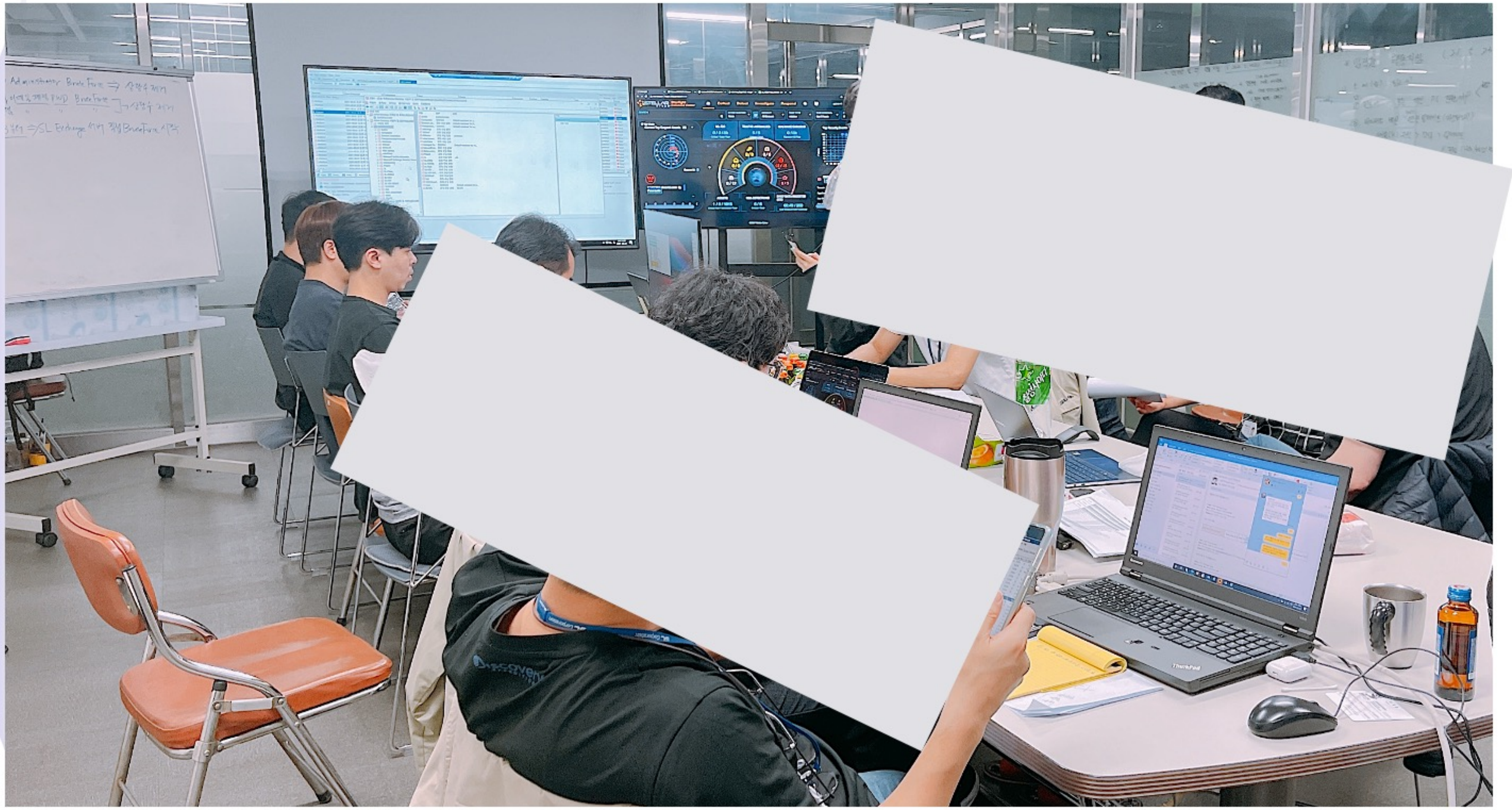
Real Case - Incident Response

May.2021

Massive Ransomware Attack (IT / OT)

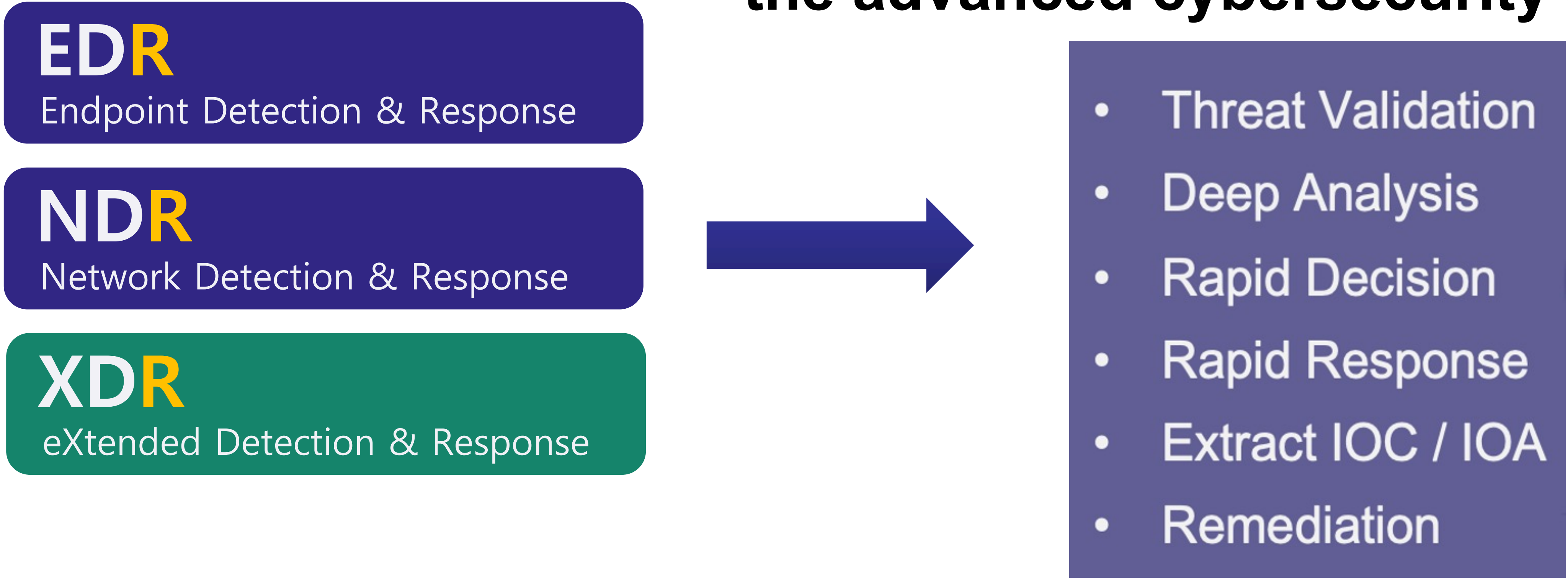
----

many types of malware were penetrated already !!!



What we have learned (1/3)

**Apply the Cleaning Process first,
for all Threat that detected by
the advanced cybersecurity solutions**



EDR
Endpoint Detection & Response

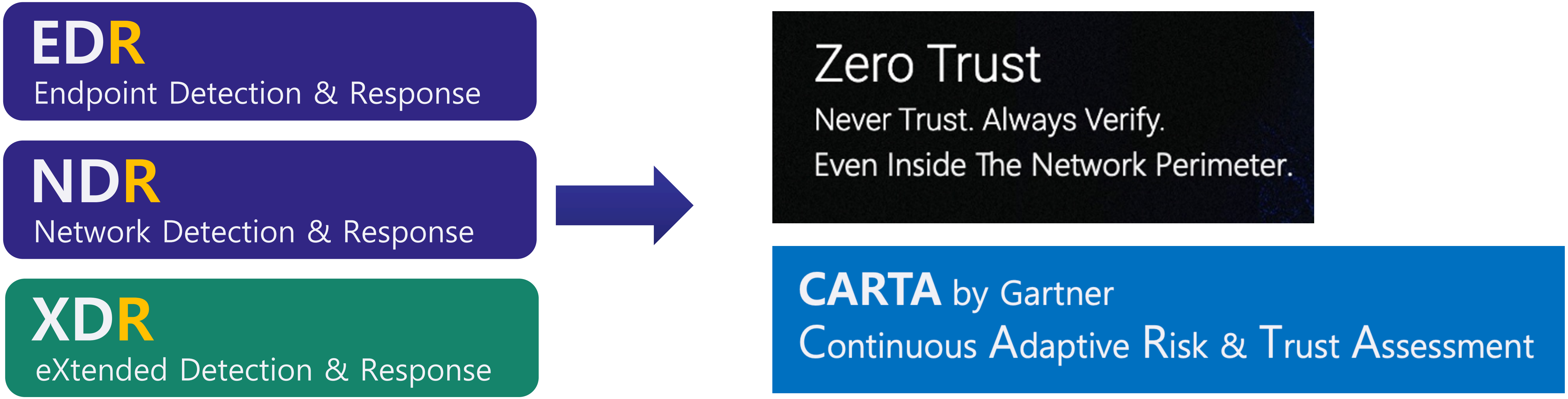
NDR
Network Detection & Response

XDR
eXtended Detection & Response

- Threat Validation
- Deep Analysis
- Rapid Decision
- Rapid Response
- Extract IOC / IOA
- Remediation

What we have learned (2/3)

Apply
the Continuous Assessment



EDR
Endpoint Detection & Response

NDR
Network Detection & Response

XDR
eXtended Detection & Response

Zero Trust
Never Trust. Always Verify.
Even Inside The Network Perimeter.

CARTA by Gartner
Continuous Adaptive Risk & Trust Assessment

What we have learned (3/3)

EDR
Endpoint Detection & Response

NDR
Network Detection & Response

XDR
eXtended Detection & Response

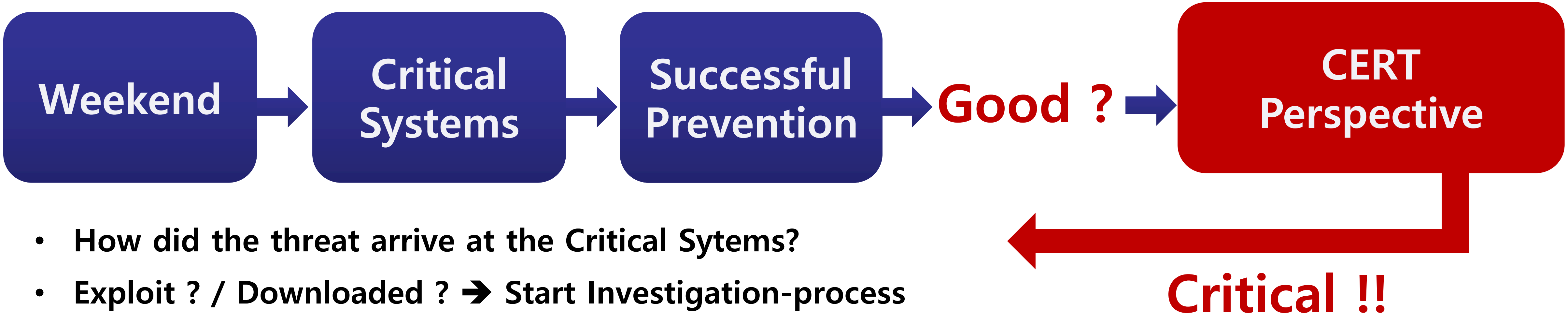
Response from a Tool Perspective

- Alert
- Playbook
- Quarantine
- Kill-Process
- Logout
- Containment
- Integration via API

Response from an Expert Perspective

- Investigation
- Threat Hunting
- Forensic
- Actionalble Answer
- Manual Response
- Automatic Response

Continuous Proactive Response Process



- **How did the threat arrive at the Critical Sytems?**
- **Exploit ? / Downloaded ? ➔ Start Investigation-process**
  - ✓ Users Login / Remote Access ?
  - ✓ AD join ?
  - ✓ Investigate NW traffic
  - ✓ What are the recent malwar that detect or prevented on this server?
  - ✓ Investigate FW logs or other security logs together with a customer
  - ✓ **EASM (Attack Surface Management)**

Real Example (A-1)

Successful Threat Detection / Prevention by EPP, EDR

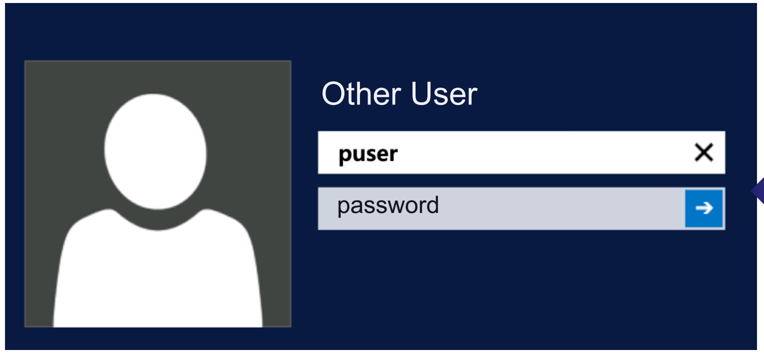
Threat Validation

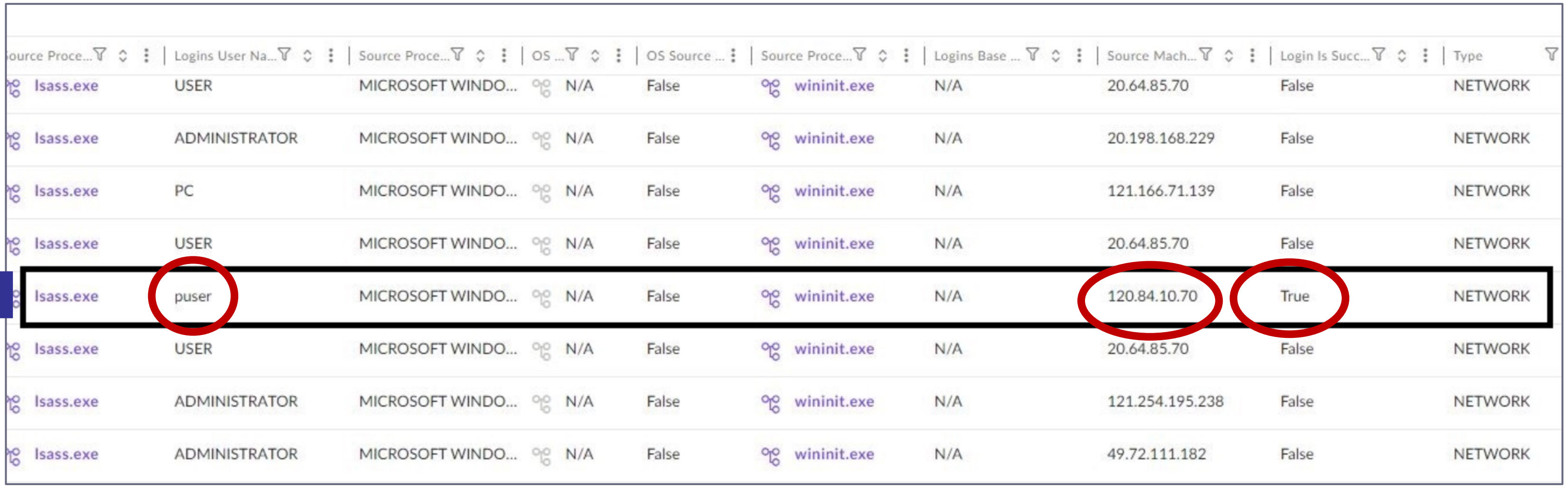
Hacking Tool – “Port Scanning Tool”

How did it downloaded ?

Investigation / Hunting ➔ Found “puser” log-in success

EASM ➔ Vulnerable RDP Access

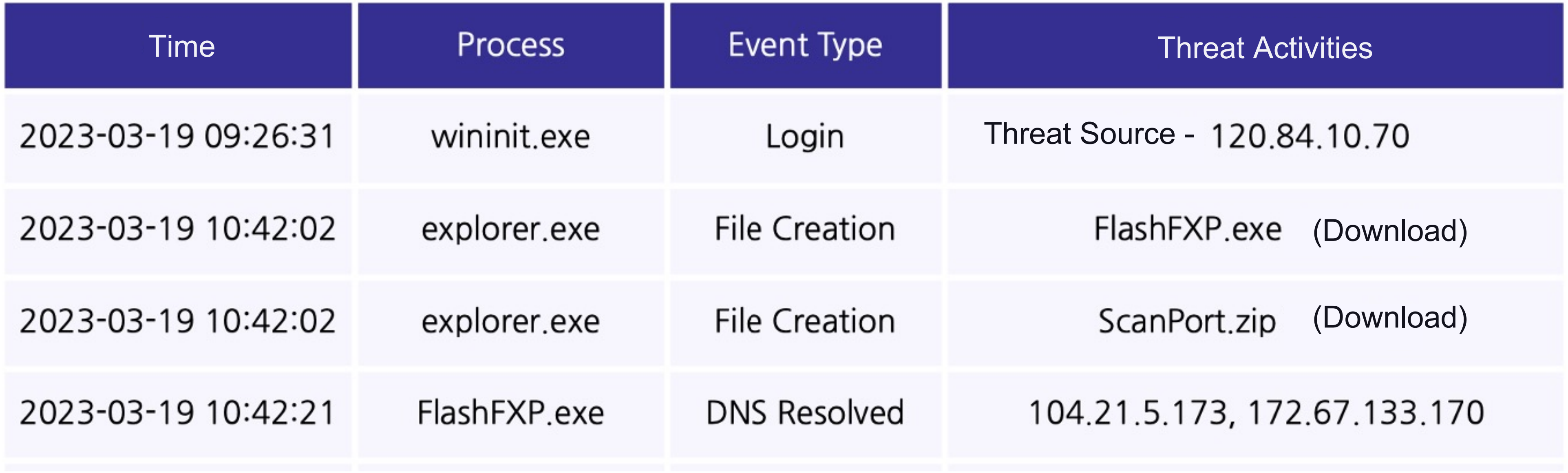




ource Proce...	Logins User Na...	Source Proce...	OS ...	OS Source ...	Source Proce...	Logins Base ...	Source Mach...	Login Is Succ...	Type
lsass.exe	USER	MICROSOFT WINDO...	N/A	False	wininit.exe	N/A	20.64.85.70	False	NETWORK
lsass.exe	ADMINISTRATOR	MICROSOFT WINDO...	N/A	False	wininit.exe	N/A	20.198.168.229	False	NETWORK
lsass.exe	PC	MICROSOFT WINDO...	N/A	False	wininit.exe	N/A	121.166.71.139	False	NETWORK
lsass.exe	USER	MICROSOFT WINDO...	N/A	False	wininit.exe	N/A	20.64.85.70	False	NETWORK
lsass.exe	puser	MICROSOFT WINDO...	N/A	False	wininit.exe	N/A	120.84.10.70	True	NETWORK
lsass.exe	USER	MICROSOFT WINDO...	N/A	False	wininit.exe	N/A	20.64.85.70	False	NETWORK
lsass.exe	ADMINISTRATOR	MICROSOFT WINDO...	N/A	False	wininit.exe	N/A	121.254.195.238	False	NETWORK
lsass.exe	ADMINISTRATOR	MICROSOFT WINDO...	N/A	False	wininit.exe	N/A	49.72.111.182	False	NETWORK

Real Example (A-2)

The Final Findings (EDR / NDR / XDR based Investigation and Threat Hunting)



Time	Process	Event Type	Threat Activities
2023-03-19 09:26:31	wininit.exe	Login	Threat Source - 120.84.10.70
2023-03-19 10:42:02	explorer.exe	File Creation	FlashFXP.exe (Download)
2023-03-19 10:42:02	explorer.exe	File Creation	ScanPort.zip (Download)
2023-03-19 10:42:21	FlashFXP.exe	DNS Resolved	104.21.5.173, 172.67.133.170

Found RDP opened
Successful Bruteforce
Successful RDP Log-in

Free FTP Tool Download

Free PortScan Download

C2 Connection

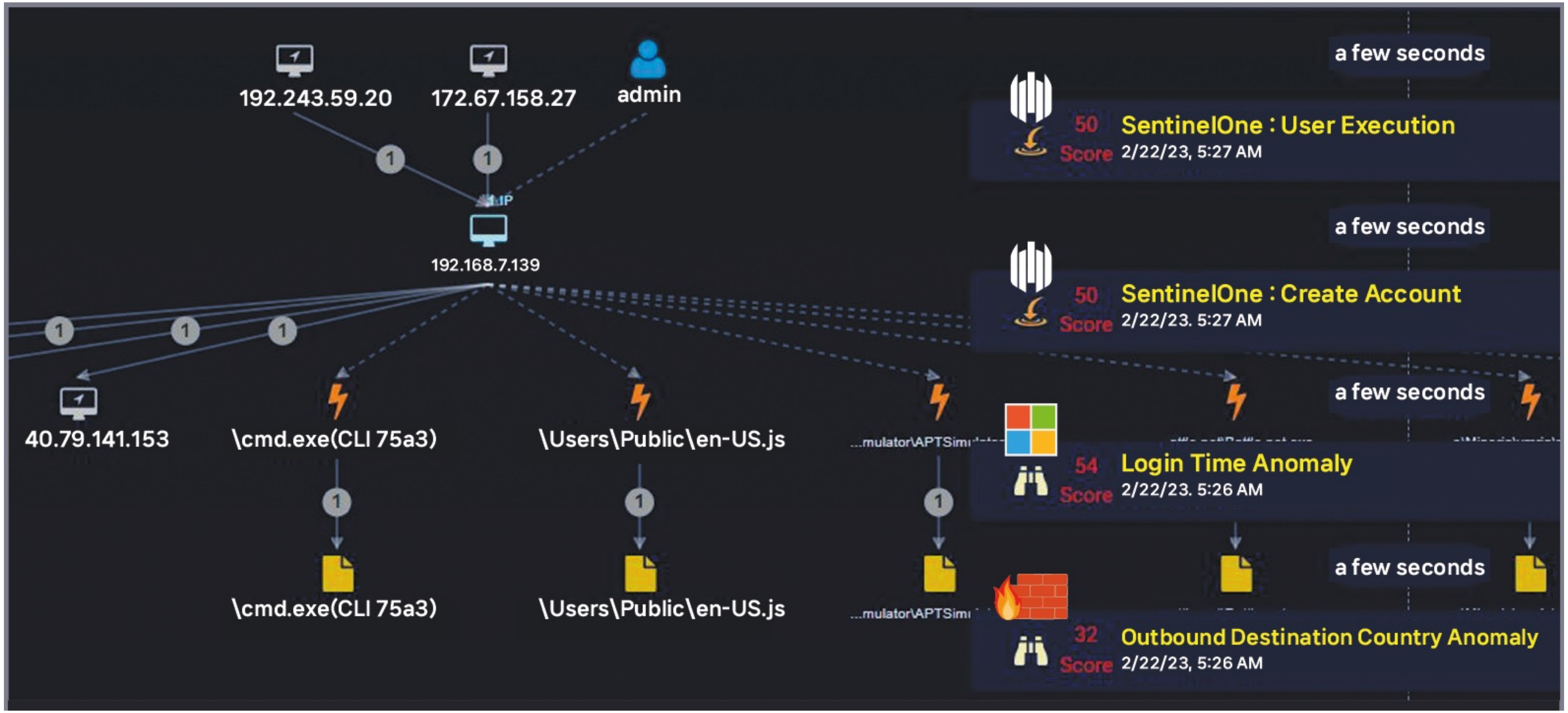
Successful Threat
Detection / Prevention
by EPP, EDR

Additional Response (Action)

For Vulnerable RDP, User, FlashFXP, C2

Real Example (B)

Stellar Cyber XDR – Critical one incident that combined with some weak signals from each SentinelOne, AD and Firewall



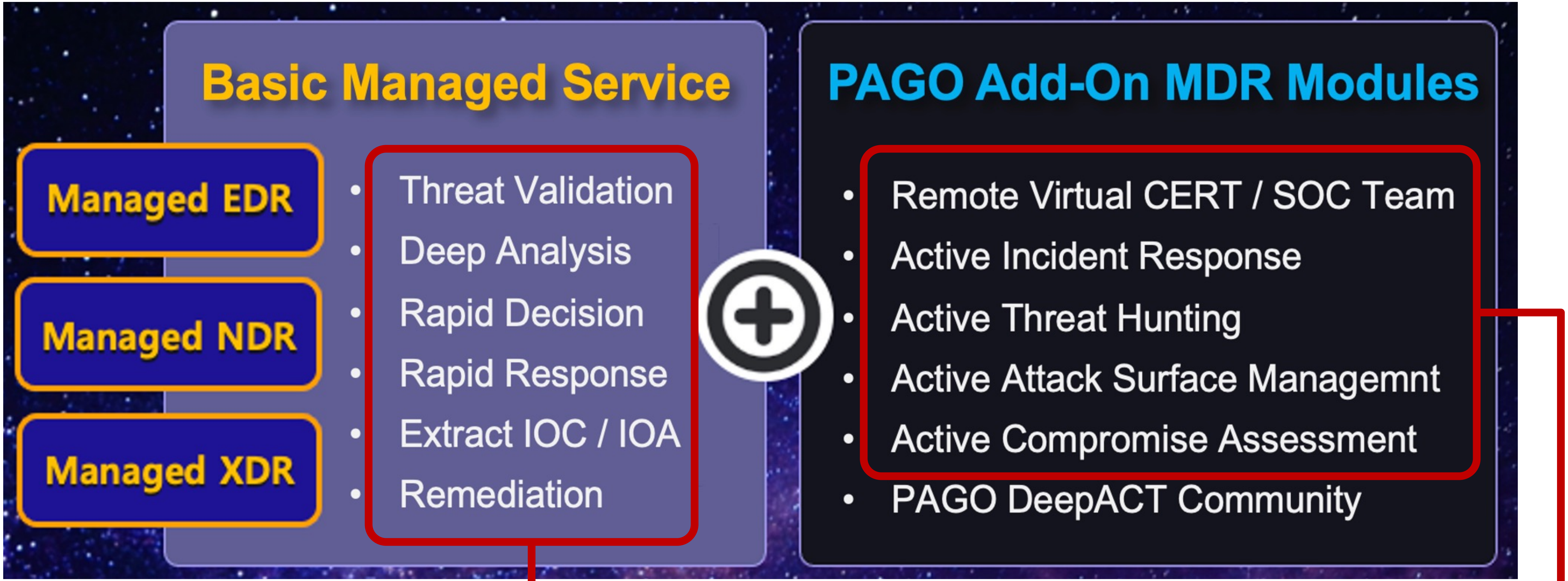
50 Score SentinelOne : User Execution 2/22/23, 5:27 AM

50 Score SentinelOne : Create Account 2/22/23. 5:27 AM

54 Score Login Time Anomaly 2/22/23. 5:26 AM

32 Score Outbound Destination Country Anomaly 2/22/23, 5:26 AM

What I wanted to say is …



Basic Managed Service

Managed EDR

Managed NDR

Managed XDR

- Threat Validation
- Deep Analysis
- Rapid Decision
- Rapid Response
- Extract IOC / IOA
- Remediation

PAGO Add-On MDR Modules

- Remote Virtual CERT / SOC Team
- Active Incident Response
- Active Threat Hunting
- Active Attack Surface Managemnt
- Active Compromise Assessment
- PAGO DeepACT Community

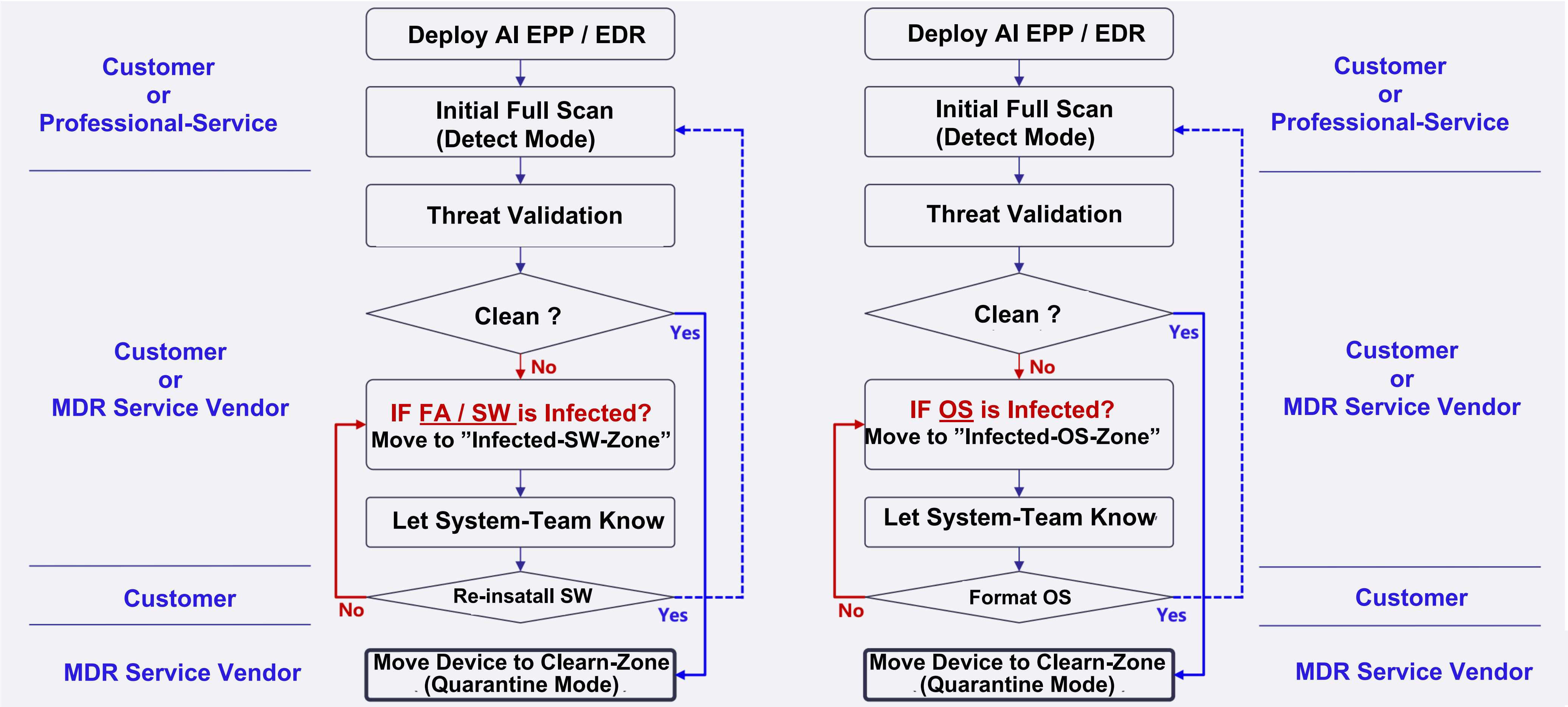
The Industry CAN DO
or SHOULD DO for fighting with All Threat !!!

One more step for OT Critical Infrastructure Endpoint Security

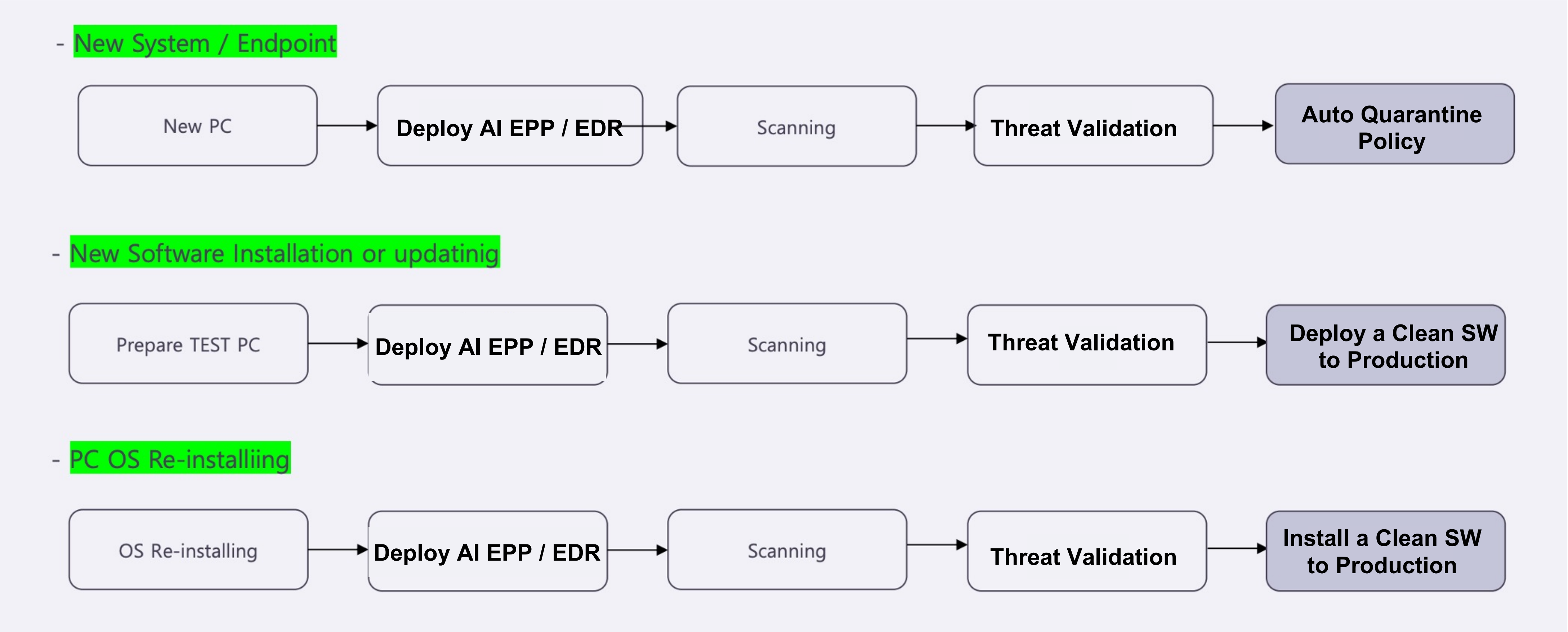
Beautiful Night View

But this is what we need to protect internally

Legacy-AV or App-Whitelist didn't work well? Consider AI EPP or EDR and Process !! (1/2)



Legacy-AV or App-Whitelist didn’t work well? Consider AI EPP or EDR and Process !! (2/2)



- New System / Endpoint

New PC → Deploy AI EPP / EDR → Scanning → Threat Validation → Auto Quarantine Policy

- New Software Installation or updatinig

Prepare TEST PC → Deploy AI EPP / EDR → Scanning → Threat Validation → Deploy a Clean SW to Production

- PC OS Re-installiing

OS Re-installing → Deploy AI EPP / EDR → Scanning → Threat Validation → Install a Clean SW to Production

The Process is Working Well

Already verified
from the global enterprises

If Don’t have the enough resources,

Discuss with
your trusted MDR Service Provider

The Goal for protecting Critical Infrastructure

Detection & Response
for
All Threat
that already penetrated

Detection & Response
for
All Threat
that is infiltrating

Apply
Continuous Zero Trust Approach to the advanced Attacks

Thank you

PAGO NETWORKS | DeepACT Managed Detection and Response

MDR-as-a-Service , SOC-as-a-Service

Protecting Enterprise For "IT, Cloud, OT/ICS" Infrastructure

Sales@pagonetworks.com