



PAGO MDR

위협 인사이트 분석 2023

실제 현업 탐지/방어한 사이버 공격 분석

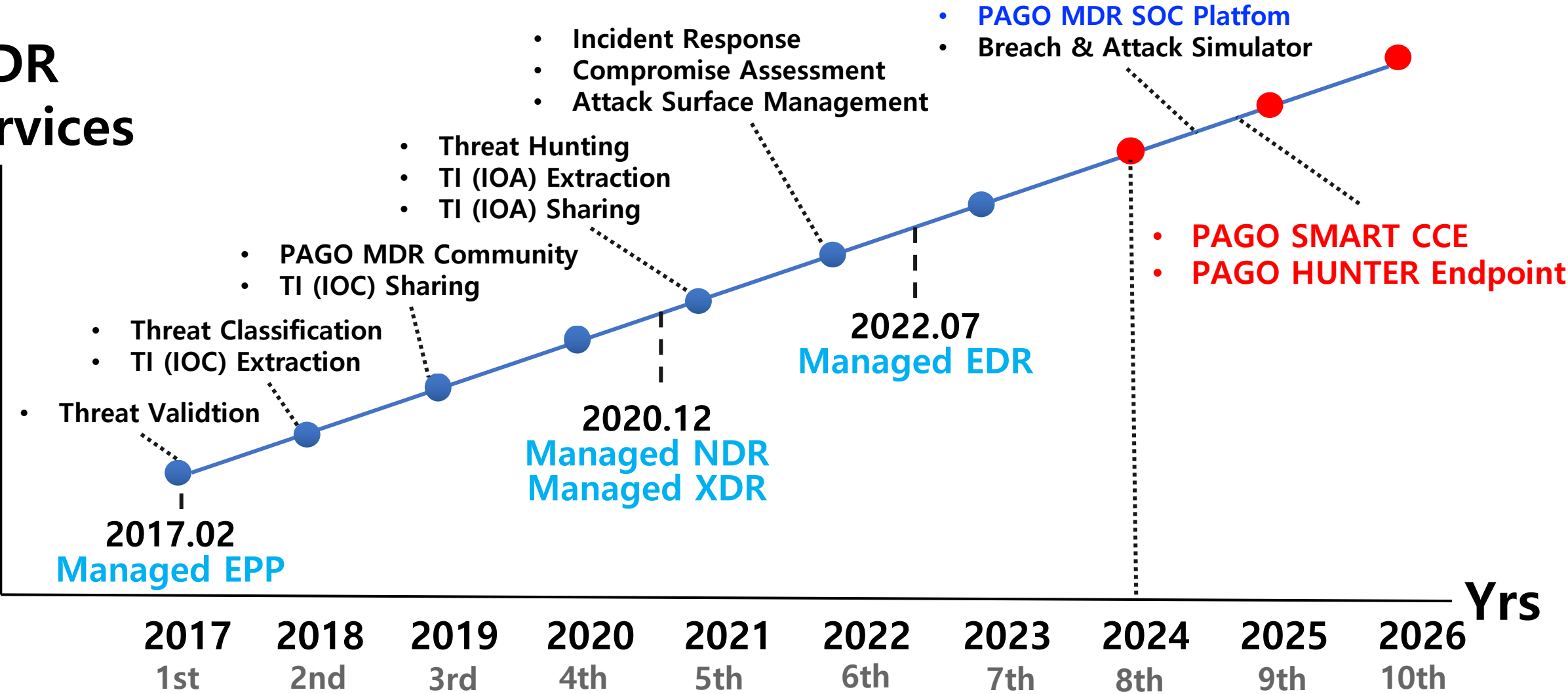




MDR 서비스 이해

PAGO MDR 서비스 이해

MDR Services

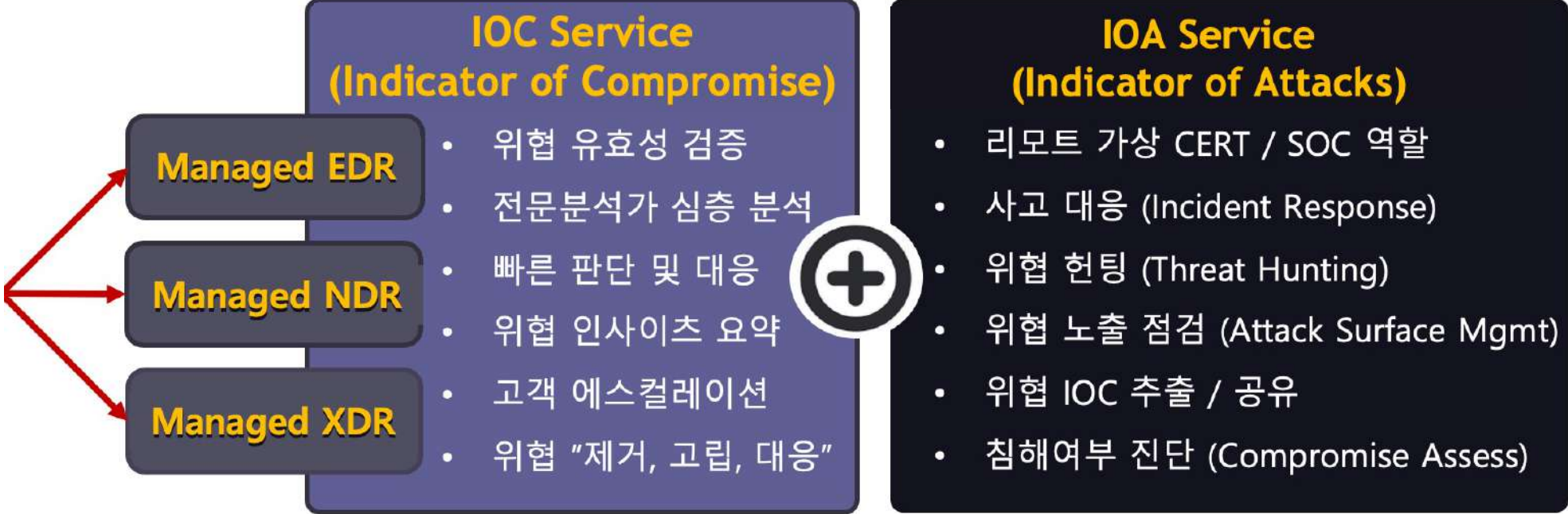


PAGO MDR 서비스 이해

위협 예방 기술
AI Cybersecurity Solutions

능동적인 대응 자동 포함
Human Expert Activities

- OT-Oriented EPP
- Consolidated EPP / EDR
- NDR
- Open XDR



MDR 서비스 자동화

- 위협 인텔리전스 시스템
- 자체 SOAR (플레이북, 워크플로우)
- 위협 자동 분석 시스템
- 상용툴 / 오픈소스툴 / 자체 개발

보호 (Protection) 고객 자산 / 인프라스트럭처

위협 예방 기술
AI Cybersecurity Solutions

능동적인 대응 자동 포함
Human Expert Activities

위협 탐지 시
위협 유효성 검증
IOC 추출
위협 인사이트 확보

Unknown 위협
위협 헌팅
위협 조사
IR without Incident

위협 노출 측정
CTEM
Continuous Threat
Exposure Management

보호
극대화

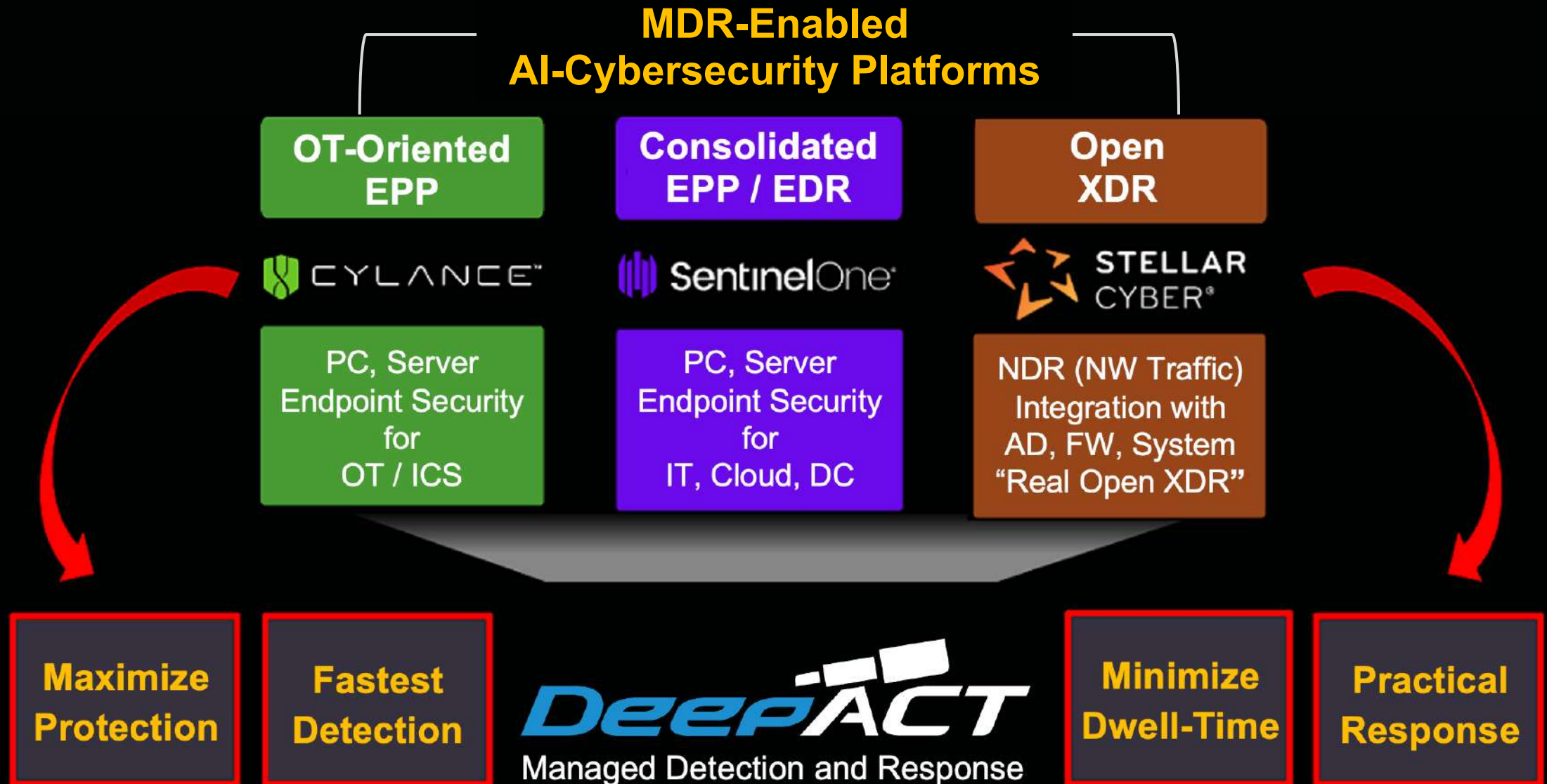
위협
빠른 탐지

위협 체류시간
최소화

현실적인
대응 방안

플랫폼화 → 연동 . 자동화 . 프로세스화 . 커뮤니케이션

AI-Products for Threat Detection & Response



고객이 제공받는 MDR Brain

위협 예방 기술
AI Cybersecurity Solutions

능동적인 대응 자동 포함
Human Expert Activities



IOC

IoC is based on a reactive strategy, since it signals that the attack has already occurred. Reactive strategies are effective in the aftermath of an attack. For example, you'll look for viruses, malware, exploits, signatures, and malicious IPs that the breach has left behind.

- Automated Process
- Automated response
- Platform for scalability

IOA

IoA is a proactive method similar to Threat Hunting, in which defenders search for early warning indications that could suggest an attack, however this is not always the case. True or false positives, code execution, Stealth, Command and Control, or lateral movement within networks are all examples of warning indicators from the perspective of information security.



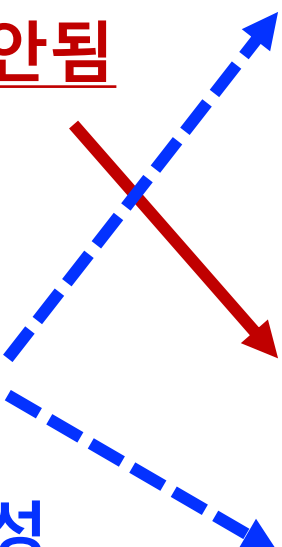
MDR

How It Works

타겟팅 랜섬웨어 피해 – 고려 사항은?

**랜섬웨어에
타겟팅되었다는 의미는,
랜섬웨어 방어에만 집중해서는 안됨**

**이미
수많은 유형의 악성코드와
악성행위가 동반되고,
위협이 숨김과 지속성 유지 속성.**

- 
- 외부 / 내부 취약점 스캐닝 행위 또는 툴 (익스플로잇)
 - 이미 침투한 트로약 / 브루트포스 / 익스플로잇 툴
 - Active Directory & 크리티컬 자산 익스플로잇 시도
 - 관리자(Admin) 권한 계정 및 패스워드 탈취
 - 사용자 레벨 계정 및 패스워드 탈취
 - 웹브라우저 캐쉬 정보 탈취 (URL, Access, User 계정 정보)
 - 조직 임직원 구성 조직도 탈취 (부서, 직급, 직책)
 - 인프라스트럭처 아키텍처 구성도 탈취
 - 작동중인 보안 아키텍처 비활성화 (시스템AV, FW, OS 서비스)
 - **중요 정보 탐색 및 탈취 / 외부 유출**
 - **데이터 암호화 페이로드 (흔히 말하는 랜섬웨어는 이부분만)**
 - 모든 데이터 백업 파괴 (On-Prem / Cloud 백업까지)
 - 멀웨어 복제 / 내부 전파
 - 체류시간 (Dwell-Time) 장기화하기 위한 기술 탑재
 - 내부에 외부 메인 C2와 통신하는, 로컬 서버 C2 운영

위협 유효성 검증의 중요성

- 아래 유형의 악성코드가 동시에 탐지/격리된 경우,
그 의미는 무엇일까요?

- ✓ Gmer – Rootkit / Kill Process
- ✓ YDArk – Rootkit / Kill AV & FW
- ✓ Processhacker – Kill System Process
- ✓ Mimikatz – Password Dump / Exploit

재검증 및 식별 절차 필수

- 유효성 검증 및 분류
- 어떤 종류의 악성코드 / 악성행위?
- 이들의 최종 목적은?
- 이들의 다음 단계는?

맞습니다. 랜섬웨어 에 의해 타겟팅 되었습니다. !!!

성공적인 위협 탐지/예방... 그 이후 !!!

성공적인
위협 탐지 / 예방
by EPP, EDR, NDR, XDR

성공적인 탐지/예방일지라도,
위협의 의도, 목적을 아는 것이 더 중요 !!!
(who, when, where, why, what, how)

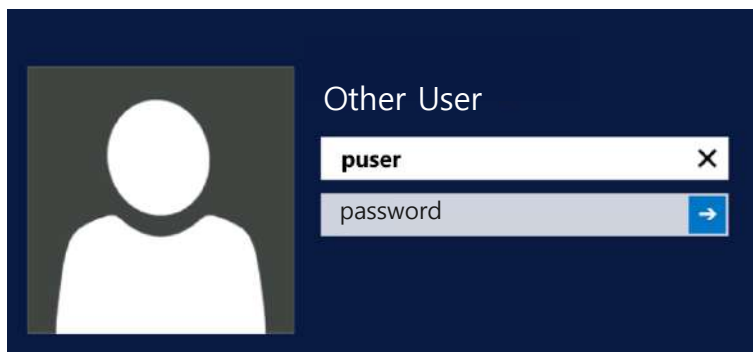
위협 검증 (by PAGO MDR Service)

해킹툴 - "포트스캐닝툴"

도대체 이 위협은 어떻게 다운로드 되었을까요?

추가적인 조사 / 분석 / 헌팅 프로세스 (by PAGO MDR Service)
분산 브루트포스 이후, "puser" 계정 로그인 상황 확인

해당 시스템 대상, ASM 서비스 제공
취약한 RDP 서비스 확인



Source Process	Logins User Name	Source Process	OS	OS Source	Source Process	Logins Base	Source Mach	Login Is Succ	Type
lsass.exe	USER	MICROSOFT WINDO...	N/A	False	wininit.exe	N/A			NETWORK
lsass.exe	ADMINISTRATOR	MICROSOFT WINDO...	N/A	False	wininit.exe	N/A			NETWORK
lsass.exe	PC	MICROSOFT WINDO...	N/A	False	wininit.exe	N/A			NETWORK
lsass.exe	USER	MICROSOFT WINDO...	N/A	False	wininit.exe	N/A			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

위협 탐지 대응 활동의 도착점은 ???

Time	Process	Event Type	Threat Activities	
2023-03-19 09:26:31	wininit.exe	Login	Threat Source - 120.84.10.70	취약한 RDP 이용 성공적인 Bruteforce RDP 무단 로그인 성공
2023-03-19 10:42:02	explorer.exe	File Creation	FlashFXP.exe (Download)	Free FTP 툴 다운로드
2023-03-19 10:42:02	explorer.exe	File Creation	ScanPort.zip (Download)	포트스캔툴 다운로드 (EDR에 의해 탐지/예방)
2023-03-19 10:42:21	FlashFXP.exe	DNS Resolved	104.21.5.173, 172.67.133.170	외부 악성서버 연결

출발점

성공적인
위협 탐지 / 예방
by EPP, EDR, NDR, XDR

도착점

실질적인 대응방안이 추가로 도출되어야 함

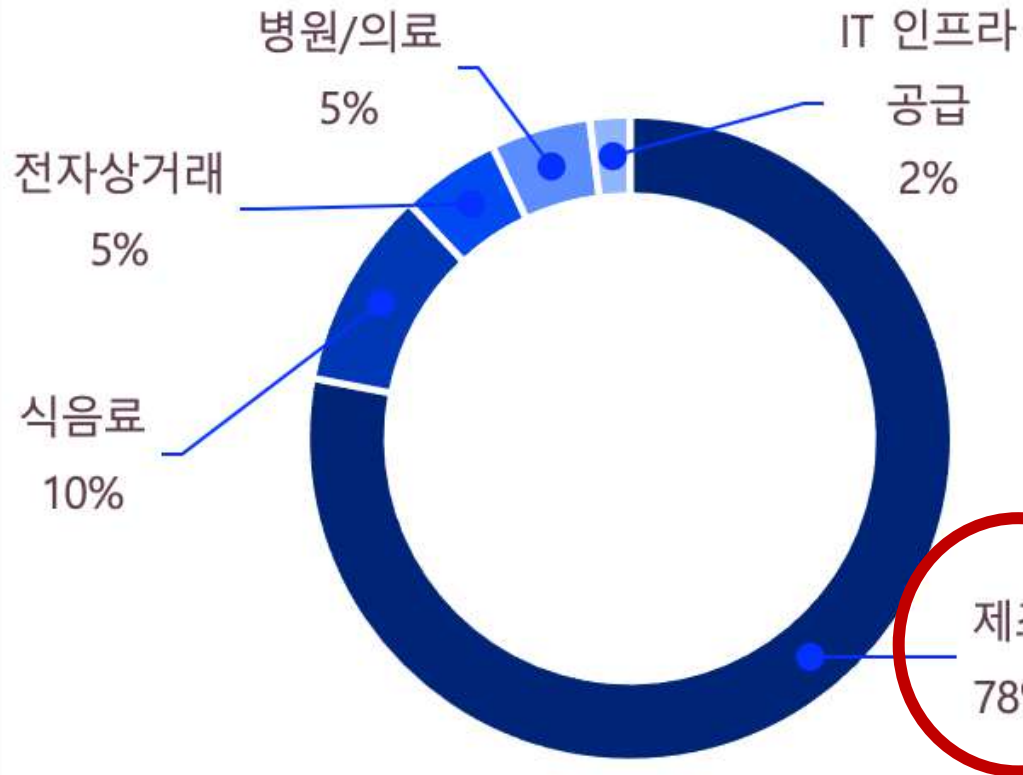
For Vulnerable RDP, User, FlashFXP, C2



MDR 위협 인사이트 분석 2023

대상 산업분야 (MDR 서비스 특성 → 공공, 금융, 국방 제외)

Top 5 Targeted Industries:



상세 분야	
플라스틱	중장비 부품
경강선재	자동차 부품
기능성용기/펌프	철강소재
PCB	공조
용접재료	신소재
반도체	식자재
치과용 의료기기	연료용 가스, 배관
화학	에너지

MDR 서비스 이후, 위협 클리닝 현황

대표적인 4개 고객사 현황 (EDR, NDR, XDR + MDR 사용)

고객사 위협 클리닝 현황

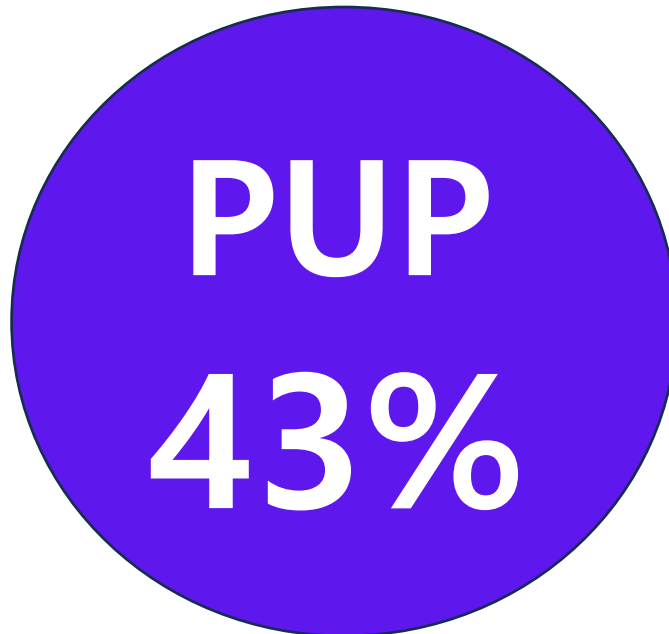


고객사 위협 클리닝 현황



악성코드 관점, Malware / PUP 비율

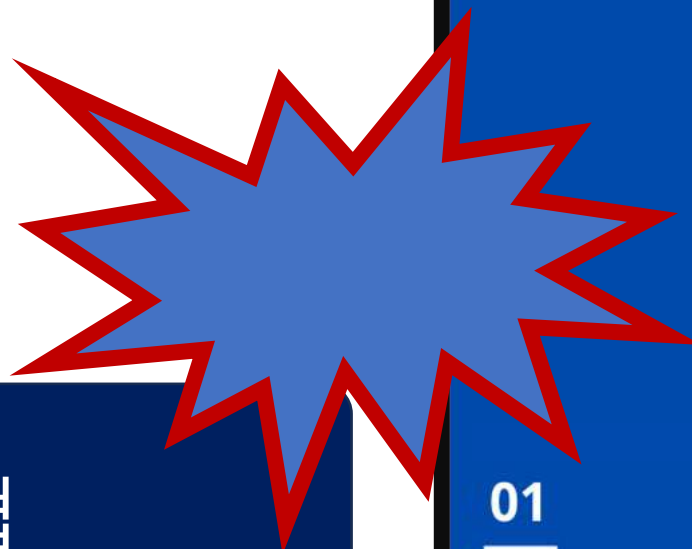
- 애드웨어
- 게임
- P2P
- 크랙툴
- 해킹툴



- 랜섬웨어
- 트로얀
- 백도어
- 다운로더
- 드롭퍼
- 루트킷
- 바이러스
- 크립토마이너
- 익스플로잇
- 웜

악성코드 유형 비율

크리티컬한 위협
초기 단계에서 HackTool
사용이 42% 탐지됨



01
해킹툴
42%

05
바이러스
1%

06
스피어 피싱
1%

03
크립토마이너
19%

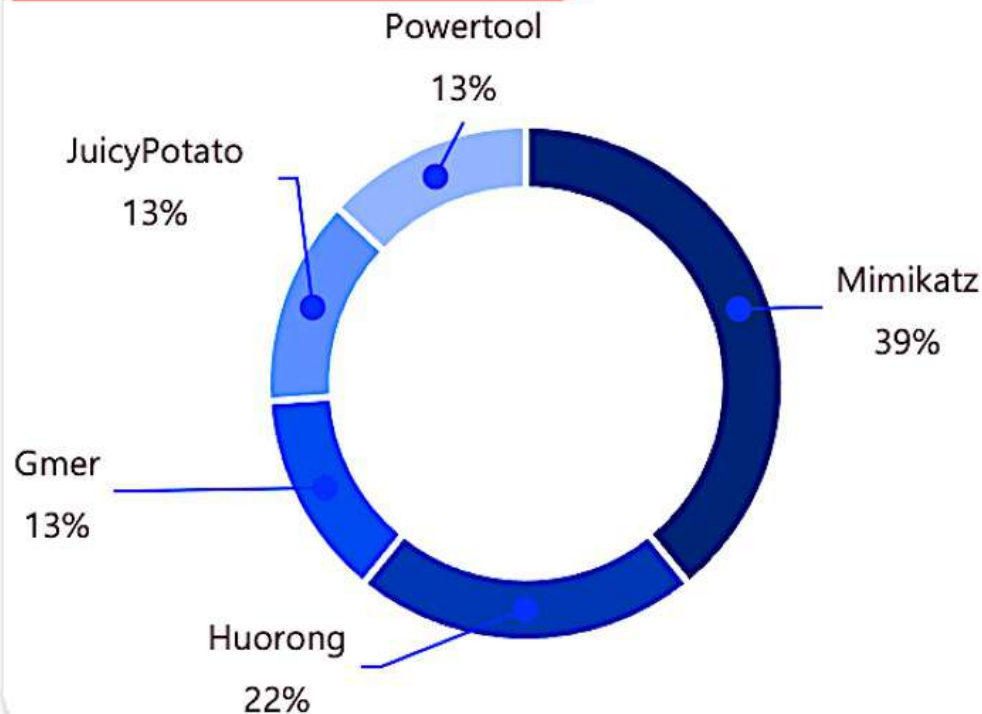
04
랜섬웨어
11%

02
트로얀
26%

해킹툴 유형 - 분석 결과

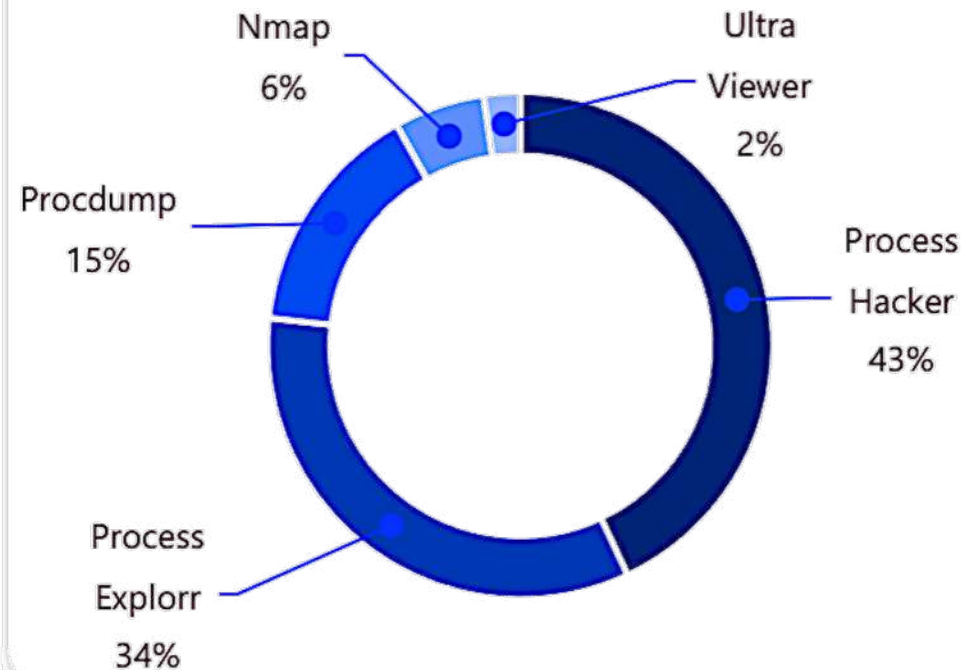
2023년,
가장 많은 위협으로 탐지된
해킹툴

Top 5 Malicious Tools:

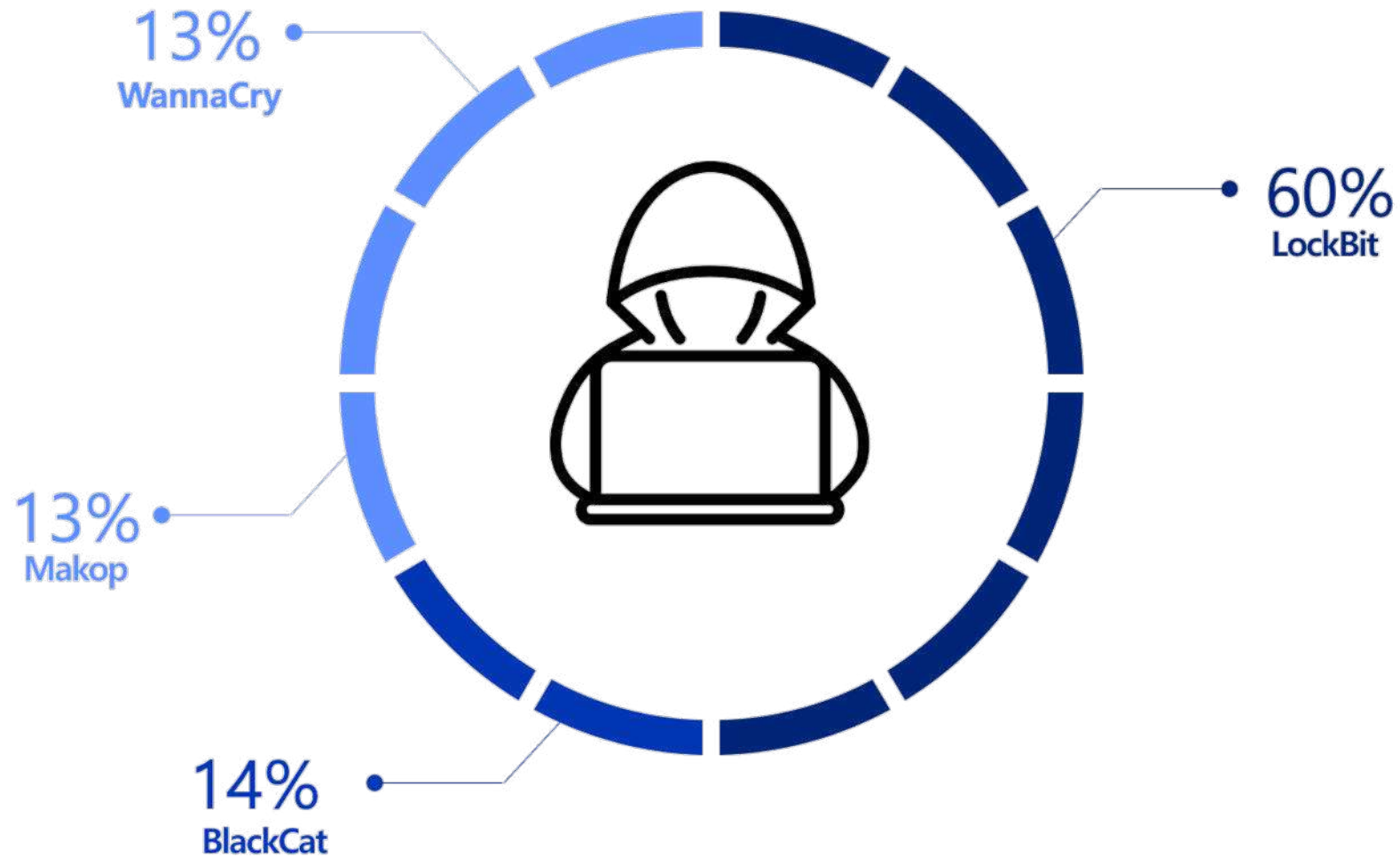


위협헌팅 중,
IOA (Indicators of Attack) 위협으로 탐지된
일반 시스템 관리툴

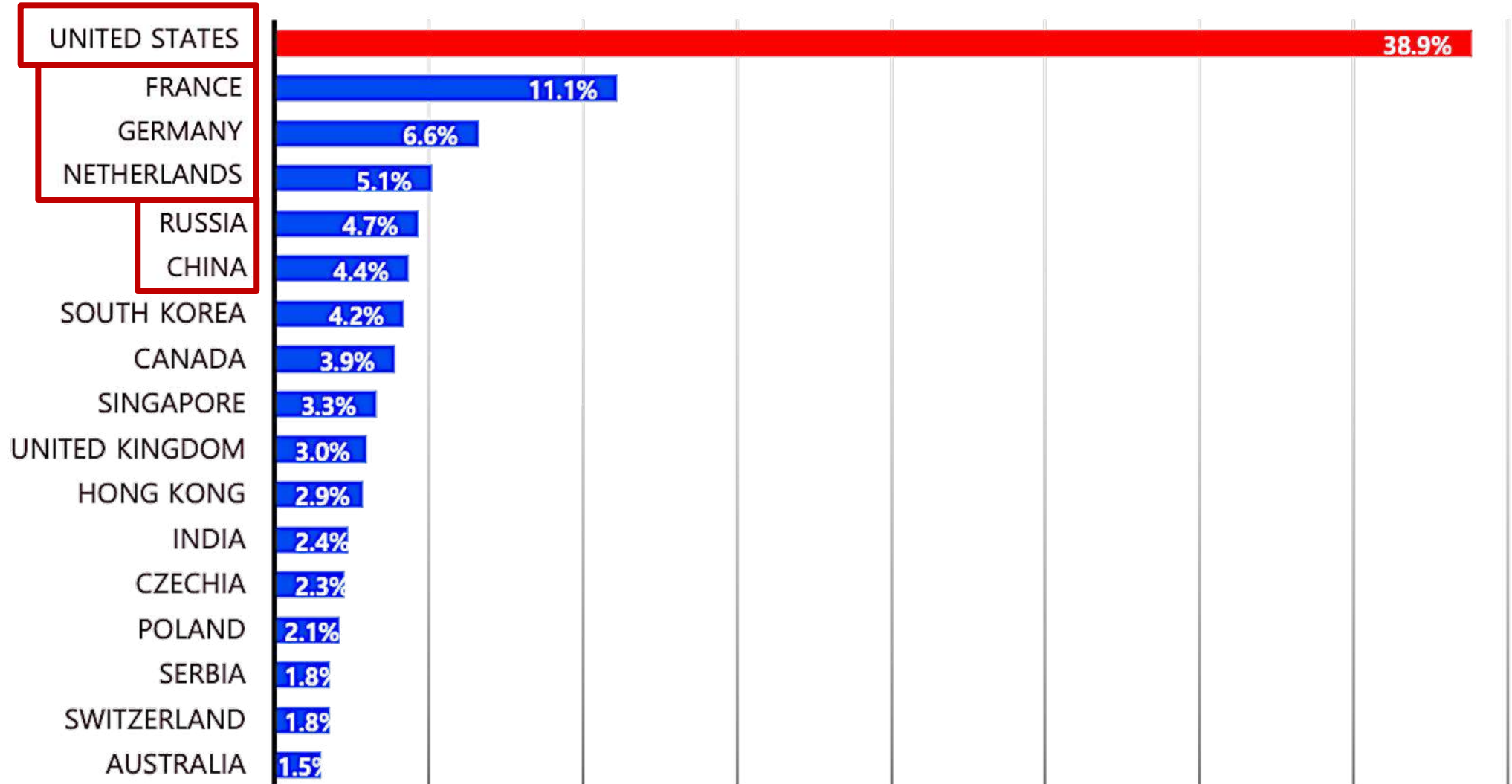
Top 5 Native Utilities:



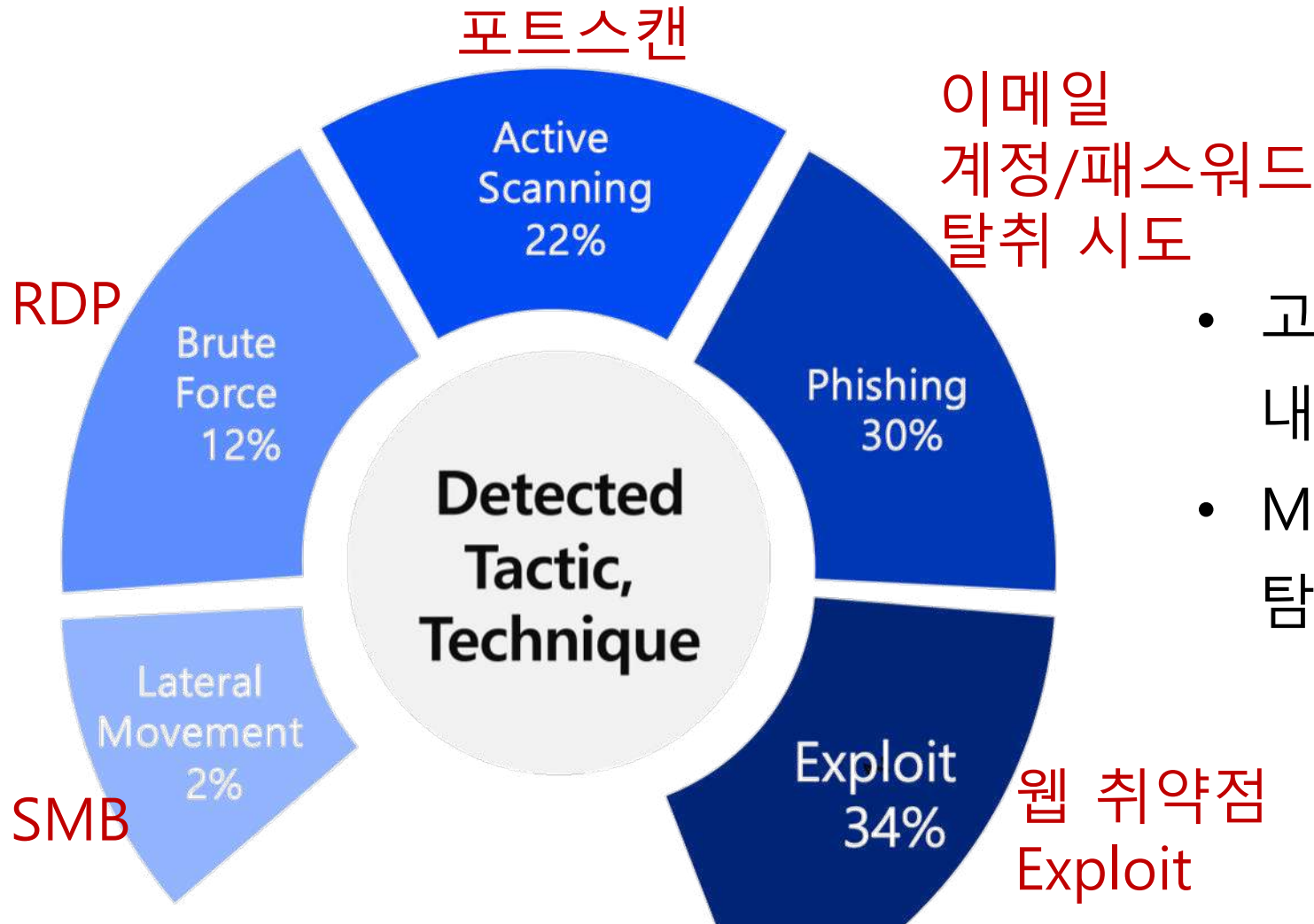
2023년 가장 많이 탐지된, 랜섬웨어



Suspicious IP – 지리적 국가 정보



네트워크 관점, 내부까지 들어온 위협



- 고객사의 네트워크 경계를 통과하여 내부 백본까지 도달한 위협.
- Managed NDR 서비스를 통해서, 탐지 및 대응 후, 분류한 공격 유형

자주 탐지되는, 침투 전술 유형

(3위)

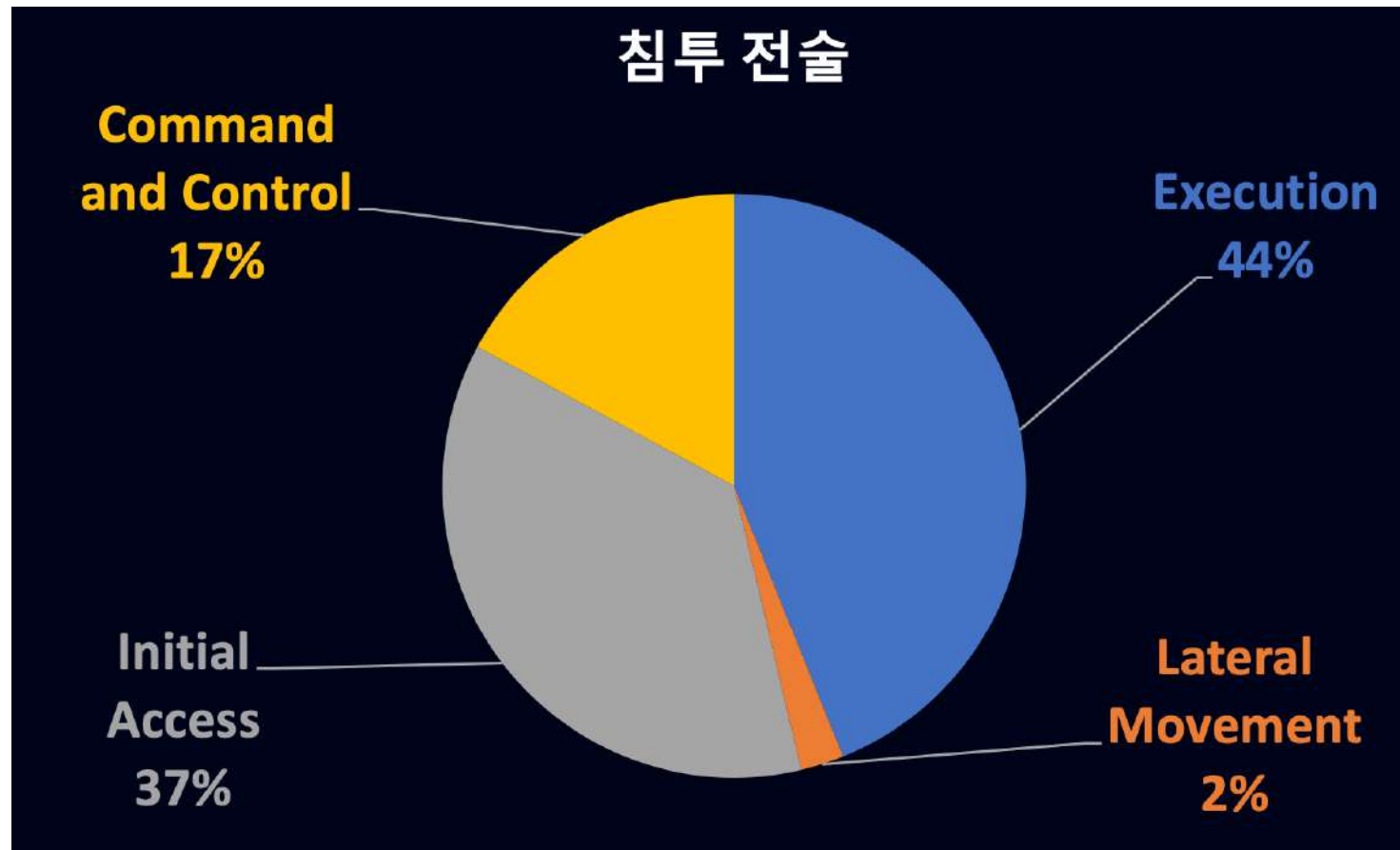
- RDP, SSH, VPN 등, 정상 접속으로 위장.

또는,

- Execution, Initial Access 성공이후, 장악

(2위)

- 피싱 이메일 (계정),
- Web/SQL 익스플로잇



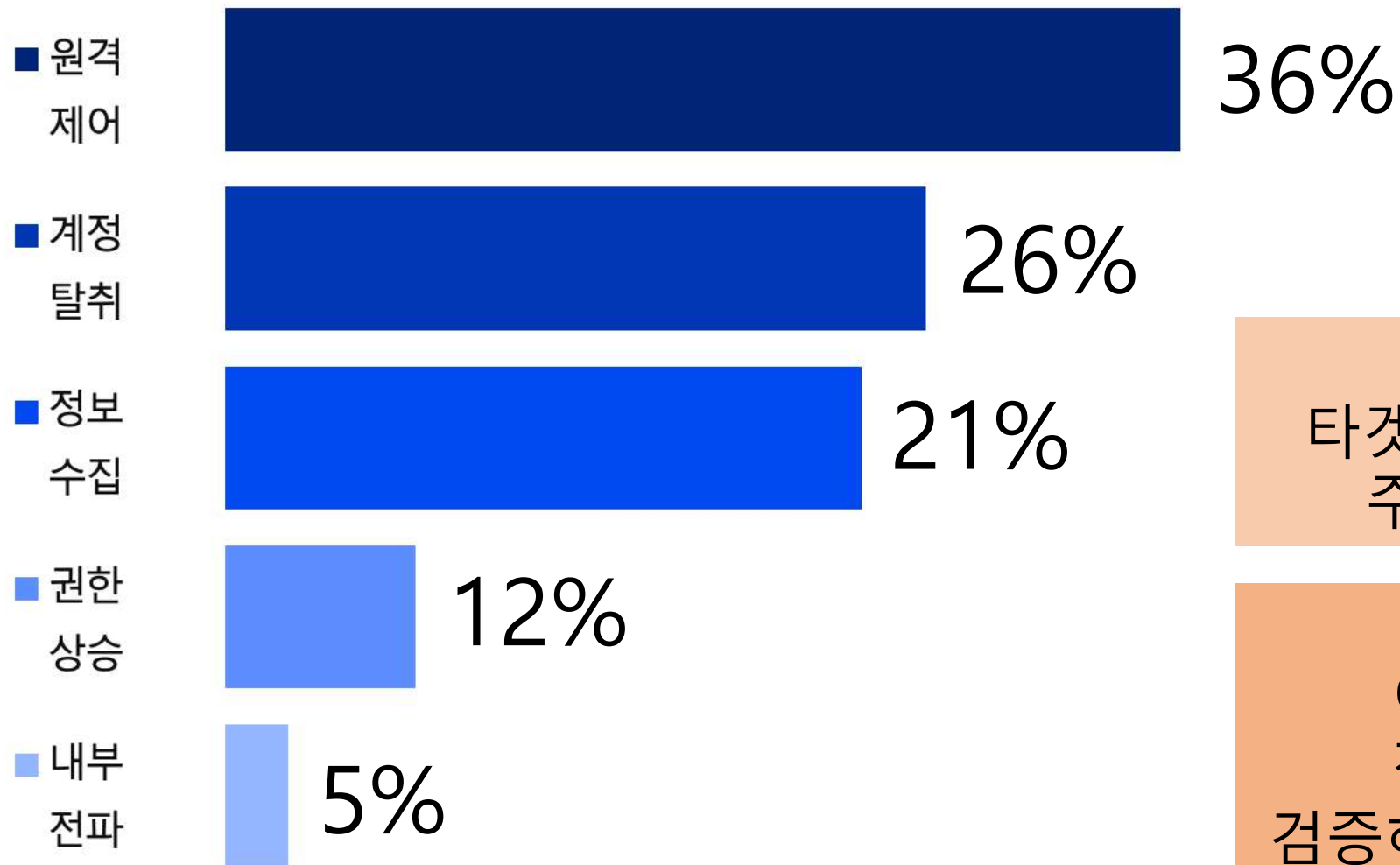
(1위)

- CMD, Powershell 실행 행위

(4위)

- SMB 취약점 이용

탐지된 위협 – 목적은 무엇이었나?



우리 기업을
타겟팅하는 위협의 목적은
주기적으로 변합니다.

오늘은
어떤 목적의 위협이
접근해 오고 있는지
검증하는 체계가 필요합니다.

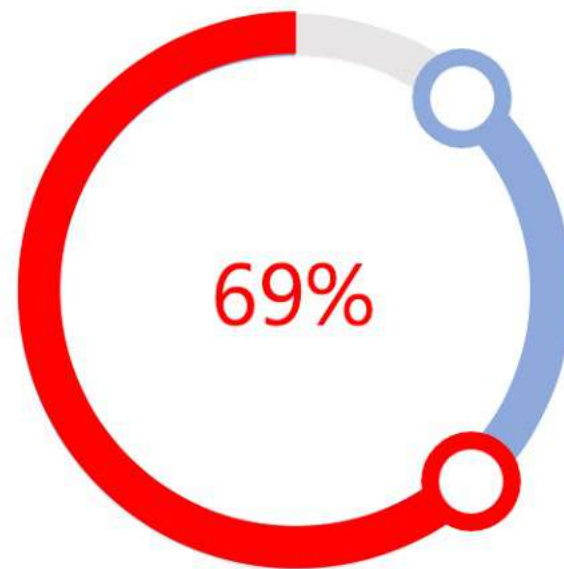
Attack Surface Management 결과

(특히 중견, 중소기업 실태)



원격 접속 프로토콜 오픈

누구나 접근할 수 있도록 외부에
원격 접속 프로토콜이 노출된 환경



RDP

93%의 노출된 환경 중 RDP는 69%를
차지

RDP, Telnet, SSH, FTP,
HTTP/HTTPS 로그인
(업무웹, 보안장비 등),
MSSQL, MYSQL 등



Freemium Threat Cleaning Service

" 보안사고 (랜섬웨어 등) 기업, 언제든지 연락주십시오.
파고네트웍스의 현재 고객이 아니어도 상관없습니다! "

프리미엄 위협 탐지 및 대응, 클리닝 서비스 제공 !!

- 랜섬웨어 피해 기업
- 보안사고 의심되는 기업
- 현재 인프라에 잔존하는 악성코드 클리닝 원하는 기업



EPP

Endpoint Protection Platform

EDR

Endpoint Detection & Response

NDR

Network Detection & Response

XDR

eXtended Detection & Response

- '프리미엄 위협 탐지 및 대응, 클리닝 서비스' 신청 고객도 정식 고객과 동일한 수준의 서비스 제공
- 현재 고객사 인프라에 존재하는 Known / Un-known 위협 추가 탐지 및 클리닝 서비스 입증
- 기존 보안 솔루션 변경없이, 그대로 프리미엄 서비스 프로그램 진행
- 다양한 산업군 지원
: 기업, 생산 / 제조망, 연구기관, 에너지, 반도체, 화학, 식음료, 헬스케어, 리테일, 국방, 대학, 호텔, 로펌, 카페, 병원, 주차관제, 클라우드, IT서비스, 호스팅 서버 등
- 다양한 플랫폼 지원
: PC, 서버, POS, 모바일, OT/ICS Windows Linux 시스템 클라우드, 데이터센터, 지점, 매장, 대리점, 공장, 재택근무PC



MDR-as-a-Service / SOC-as-a-Service / CERT-as-a-Service
Protecting Enterprise For "IT, Cloud, OT/ICS" Infrastructure

sales@pagonetworks.com