Eyeon Security

EyeOn AiSOAR

주소: 서울특별시서초구서초대로255 2층(고덕빌딩) | 사업자등록번호: 215-87-70318 | 통신판매업신고번호: 제2019-서울서초-2940호 | Tel: 02-2105-4400 (영업문의: 내선 1 / 보안관제 기술문의: 내선 2) | Fax: 02-2105-4456

EyeOn AiSOAR (Eyeonsecurity AiSOAR)

EyeOn AiSOAR란?

Eyeon Security

EyeOn AiSOAR(Eyeonsecurity AiSOAR)는 AI 기반의 **보안 위협 대응 자동화 솔루션**으로
침해 위협 이벤트를 실시간으로 탐지하고 대응하여 보안 운영 효율을 향상시키고 위협 대응 시간을 혁신적으로 단축할 수 있습니다.

Security Orchestration and Automation

다양한 보안 도구와 시스템을 연동하여 작업을 중앙 집중화하고 자동화하여 사고 대응 프로세스를 가속화할 수 있습니다.

Security Incident Response Platform

보안 위협이 발생했을 때 자동 차단 및 다양한 보안 대응을 지원해 사고 피해를 최소화합니다.

Threat Intelligence Platform

사이버 위협과 관련된 정보를 수집, 분석, 관리하여 최신 공격 기법에도 대응할 수 있도록 보안 체계를 강화합니다.

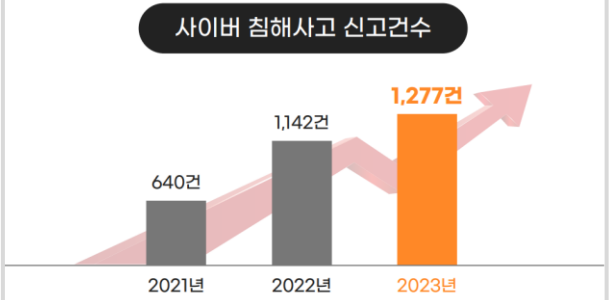
EyeOn AiSOAR (Eyeonsecurity AiSOAR)

AiSOAR는 당신의 보안을 혁신적으로 레벨업 합니다

Eyeon Security

탐지 대응 고도화

현대의 사이버 공격은 매우 빠르게 진화하고 있으며, 피해 건수도 날로 증가하고 있습니다. EyeOn AiSOAR는 새롭고 다양한 패턴의 위협을 탐지하고 학습해 자동으로 대응합니다.



출처 : KISA 사이버 위협 동향 보고서

비용 절감

보안 자동화를 구축하여 데이터 침해 라이프 사이클이 짧아질 수록 침해 대응 비용이 낮아지는 효과를 얻을 수 있습니다.

200일 이내 침해사고 해결 기업
약 23% 비용 절감
평균 102만 달러 (한화 약 14억 1100만원)

출처 : IBM 데이터 침해 비용 보고서

효율적 인력 관리

EyeOn AiSOAR (보안 오케스트레이션, 자동화 및 대응)를 사용하여 단순 반복 업무의 자동화를 통해 작업 효율성을 크게 향상시키고, 휴먼 에러 리스크를 줄였습니다. 또한, 자동 대응이 어려운 복잡한 이슈는 보안 전문가들이 처리함으로써 보다 전문화된 서비스를 제공합니다.

EyeOn AiSOAR (Eyeonsecurity AiSOAR)

보안 이벤트 대응 흐름도

Eyeon Security

SOAR를 활용하여 사전에 정의된 대응 절차와 정책을 기반으로 자동화된 대응을 수행하고, 중요 이벤트에 대해서는 전문 CERT에서 대응 합니다.

자동화 대응 (SOAR)

분석

침해위협 이벤트 티켓

① IPS, WAF, EDR 침해위협 이벤트
② 임계치 기반 이벤트
③ 상관관계 분석 이벤트
④ 키워드 이벤트

장애 이벤트 티켓

① 임계치 기반 이벤트
② 키워드 기반 이벤트

위협 IP 평판 분석 알림

① IP 평판 점수 기준
② 공격 History 기준

조치

위협 IP 자동 차단

① 이기종 장비 차단
② 보안 이벤트 기준
③ 악성 IP 평판 기준
④ 위협 IP TOP20 기준
⑤ 고객 협의 기준

차단 IP 자동 관리

① 차단 IP 자동 생성
② 위협 IP 그룹 관리
③ 위협 IP 수량 관리
④ 수량 초과 IP 자동 삭제

전파

처리 결과 전파

① 위협 정보 전파
② 위협 IP 차단 전파
③ 위협 IP 평판 전파
④ 위협 IP History 전파

위협 등급별 전파

① 상위 등급 이벤트 전파
② 등급별 전파 (Email, SMS, KAKAO)
③ 긴급 시 유선 연락

CERT 대응

침해위협 분석 결과 전파

① 침해위협 테스트 진행
② 취약점 유/무 확인
③ 해킹 사고 확인 시 침해사고 조사 대응 안내

침해위협 대응 (차단/조치)

① 공격 IP 차단 고객 안내
② 공격 IP 차단 진행
③ 취약점 조치 권고

신규 취약점 분석 및 룰셋 적용

① Exploit 정보 수집
② 분석 보고서 작성
③ 신규 탐지 패턴 개발
④ 보안장비 및 SIEM 적용
⑤ 탐지 테스트 진행
⑥ SIEM&SOAR 적용

EyeOn AiSOAR (Eyeonsecurity AiSOAR)

보안 이벤트 대응 구성도

Eyeon Security

구간별 특징	공격 예시 웹취약점 공격(SSL)	인프라 구성 예시

FW 구간
- 보안솔루션 탐지 유무와 관계 없이 차단 가능
- 공격 유무 판단 불가

* 공격IP 실시간 차단하여 위험 노출 최소화

허용

IPS 구간
- 다양한 애플리케이션 취약점 탐지 가능
- 암호화 통신 탐지 불가

미탐지

WAF 구간
- 암호화 통신 탐지 가능
- 보호 대상 도메인 외 탐지 불가능

Target 1,2,3 취약

SERVER 구간
- Agent 기반 보안 솔루션 설치 시 탐지 가능
- 보안 솔루션 미설치 시 탐지 불가

Target1 취약

FW

실시간 공격IP 차단

IPS

공격 데이터 수집

WAF

위험 노출

Target1
Agent 미설치

Target2
Agent 설치

위험 노출

Target3
미보호대상

Target4
보호대상

EYEON AI SOAR

대 응
FW 차단 대응
위협 보고

악성 판정

분 석
KISA 연계 분석
공격 IP 위험도 분석
수집 데이터 분석

주의 판정

고도화
미대응 데이터 분석
공격 통계 분석

SMS EMAIL 알림톡

보안 담당자
실시간 위협 보고서
월간 대응 보고서
긴급 이벤트 :
카카오톡 즉시 알림

보안 관제 센터
신규 취약점 분석
시나리오 고도화
공격 영향도 분석

EyeOn AiSOAR (Eyeonsecurity AiSOAR)

주요기능

Eyeon Security

침해 위협 이벤트 프로파일링 탐지

긴급 상황 탐지 및 즉시 차단

SQL Injection 탐지

웹 애플리케이션에서 SQL 명령어를 삽입해 데이터베이스를 조작하려는 시도를 탐지합니다.

- **기능** : 5분간 100건 이상의 SQL Injection 시도가 있을 경우 즉시 알림 및 공격 IP 자동 차단

- **효과** : SQL Injection 정보 유출 방지공격으로 인한 웹사이트 및 데이터베이스 지연 및 데이터 유출 방지

정찰 및 공격 이벤트 탐지

Cyber Kill Chain 단계에서 1단계 정찰 이후 추가 공격을 탐지합니다.

- **기능** : 60분 이내 Port Scanning 이벤트 발생 후 추가 공격 이벤트가 발생하면 즉시 탐지 및 알림 발송

- **효과** : 조기에 정찰 및 공격을 탐지하여 추가적인 공격 예방

취약점 스캐닝 이벤트 탐지

여러 유형의 스캐닝 공격(예: 포트 스캐닝, 네트워크 스캐닝 웹 스캐닝 등)을 탐지합니다.

- **기능** : 스캐닝 관련 이벤트가 5가지 이상 발생 시 즉시 알림 발송

- **효과** : 다양한 스캐닝 시도를 조기에 발견하여 취약점 공격 방지

최신 공격 이벤트 탐지

새로운 공격 기법에 의한 침입 시도를 탐지합니다.

- **기능** : 최신 공격 기법 탐지 시 카카오톡으로 알림을 발송하여 즉각적인 대응 가능

- **효과** : 최신 위협에 대한 빠른 대응으로 보안 수준 유지

EyeOn AiSOAR (Eyeonsecurity AiSOAR)

주요기능

Eyeon Security

침해 위협 이벤트 프로파일링 탐지

긴급 상황 탐지 및 즉시 차단

다량 접근 탐지/차단

SSH, FTP, RDP, MySQL 등의 다량 접근 시도를 탐지하고 차단합니다.

- **기능** : 방화벽을 통해 다량의 접근 시도를 실시간으로 감지하고 차단

- **효과** : 불필요한 접근 시도를 차단하여 시스템 안전성 높임

방화벽 로그 기반 차단

방화벽 로그를 분석하여 비정상적인 접근 시도를 탐지합니다.

- **기능** : 5분간 방화벽 로그에서 특정 임계치를 초과하는 접근 시도와 Abuse Score가 30% 이상일 경우 차단

- **효과** : 비정상적인 접근 시도를 신속히 차단하여 시스템 보안 강화

CTAS 해킹 공격 IP 차단

CTAS(Cyber Threat Analysis & Sharing System)에서 공표한 해킹 공격 IP를 실시간으로 차단합니다.

- **기능** : CTAS 해킹 공격 IP가 공표되면 평판 분석 후 즉시 해당 IP 차단

- **효과** : 알려진 위협 IP로부터의 공격을 사전 차단

EyeOn AiSOAR (Eyeonsecurity AiSOAR)

주요기능

Eyeon Security

장애 모니터링

지속 시간 기반 알림

시스템 장애나 문제 발생 시 지속 시간에 기반한 알림을 발송합니다.

- **기능** : 알림이 발생하고 지속 시간이 5분 이상일 경우 알림 발송

- **효과** : 장기적인 문제를 조기에 발견하여 대응함

빈도 기반 알림

짧은 시간 동안 반복적으로 발생하는 장애를 모니터링합니다.

- **기능** : 1시간 동안 알림이 5회 이상 발생하면 이를 보고

- **효과** : 반복되는 문제를 신속히 파악하고 대응함

장애 로그 전송

장애 발생 시점 전후의 로그를 수집하여 분석합니다.

- **기능** : 장애 발생 5분 전부터 장애 발생 시점까지의 로그 전송

- **효과** : 장애의 원인을 정확히 분석하고 재발 방지 대책을 수립

EyeOn AiSOAR (Eyeonsecurity AiSOAR)

주요기능

Eyeon Security

IP 평판 조회

IP 평판 알림

공격 이벤트에 연루된 IP의 평판을 조회하여 악성 IP를 식별합니다.

- **기능** : IP의 Abuse Score가 30% 이상일 경우 알림 발송

- **효과** : 평판이 나쁜 IP를 조기에 식별하고 대응

- **예시** : 공격 IP 182.98.175.134 (score 40%, 여러 번 공격에 사용된 IP) 탐지 시 알림 발송

즉시 차단 서비스

자동 차단

보안솔루션에서 탐지된 공격 IP를 즉시 방화벽에서 차단합니다.

- **기능** : 웹방화벽에서 탐지된 공격 IP를 Fortigate, Paloalto와 같은 NGFW에서 자동으로 차단**(1분 이내 즉시 차단, 공격 IP 자동 관리)**

- **효과** : 공격 IP를 신속히 차단하여 추가적인 피해 예방

침해 위협 보고서

공격 이력 확인

특정 공격 IP가 타 사이트에서의 공격 이력을 조회하여 종합적인 위협 정보를 제공합니다.

- **기능** : 발생한 공격 IP에서 다른 사이트로의 공격 이력을 확인

- **효과** : 공격자의 행동 패턴을 파악하여 보다 효과적인 대응 전략을 수립

EyeOn AiSOAR (Eyeonsecurity AiSOAR)

기대효과

Eyeon Security

01. 실시간 탐지 및 대응

기존 보다 향상된 탐지 범위와 다양한 위협에 대해 프로파일링 기법을 적용하여 실시간으로 탐지하고 신속히 대응함으로써 기업의 보안 수준을 향상시킵니다.

02. 효율적인 보안 관리

운영인력이 진행하던 위협 IP 차단 등의 반복적이고 루틴한 작업을 자동화하여 업무 효율성을 높이고, 인력의 부담을 줄입니다.

03. 위협 인텔리전스

보안 분석의 복잡한 공격 패턴을 식별하고 최신 공격 기법과 위협 정보를 지속적으로 업데이트하여 대응 체계를 강화합니다.

04. 비용 절감

자동화된 보안 솔루션을 통해 인력 및 운영 비용을 절감할 수 있습니다.

05. 신뢰성 강화

중요, 긴급 보안이벤트에 대하여 별도의 시스템으로 알림을 수신하여 중요 사안을 놓치지 않습니다.

EyeOn AiSOAR (Eyeonsecurity AiSOAR)

침해위협 보고서 샘플

Eyeon Security

분석 내용

발생시간	공격유형				Action	Search
2024-06-25 11:16:34	취약 페이지 접근 탐지				deny	조회
출발지 IP	**출발지 국가**	**목적지 IP**	**목적지 국가**	**목적지 포트**	**프로토콜**	**Count**
1.1.1.1	UA	2.2.2.2	KR	80	TCP	80
Domain						
Demo.eyeonsec.co.kr						
URL						
/test/attacher						

위협 IP 1.1.1.1 에서 취약 페이지 접근 탐지 포함 80 건의 공격 시도가 deny 되었습니다.

해당 위협IP는 총 47 건의 공격 레포트가 보고된 악성 공격자로 확인되어 방화벽 선차단 진행하였습니다.
상세 내용은 아래 참고 부탁드립니다.

위협 IP 정보

Threat IP	Country Name	ISP	Domain	Malware Score	Search
1.1.1.1	RU	Dmitry Viktorovich Petrov	Attaker.com	93%	조회

Threat reports

#1. [Brute_Force, Web_App_Attack]
report Date: 20240624T17:10:22+00:00
comment: Fail2Ban Ban Triggered₩nHTTP Exploit Attempt

#2. [Web_App_Attack]
report Date: 20240624T16:59:29+00:00
comment: Directory Traversal on: /.env.bak

#3. [Brute_Force]
report Date: 20240624T16:04:20+00:00
comment: XSS (Cross Site Scripting) & Git Exposure attempt.111

#4. [Web_App_Attack]
report Date: 20240624T12:58:19+00:00
comment: Web Attack

#5. [Web_Spam]
report Date: 20240624T12:15:37+00:00
comment: Scanner : /.env.bak

대응 현황 (공격 IP 차단)

IP 차단 적용 장비	Vdom	Address Name	Group Name	Result
EYEON_FW_3.3.3.3	root	SOAR_Attack_1.1.1.1	EOS_Attack_1.1.1.1	차단 완료
EYEON_FW_4.4.4.4	DB Zone	SOAR_Attack_1.1.1.1	EOS_Attack_1.1.1.1	차단 완료

*차단 IP는 EOS Attack IP1~4 그룹에 순차 적용되며 그룹당 250개씩 최대 1000개까지 등록되고 초과 시 이전 그룹 초기화 후 등록됩니다.
차단 IP에 대한 차단해제 및 예외처리가 필요하실 경우 관제센터로 회신 부탁드립니다.

HISTORY (위협 IP의 최근 3일 탐지 내역)

일시	이벤트 ID	공격유형	Action	Log count
20240624 23:55:58	SR240624AW100013156	취약 페이지 접근 탐지	deny	1
-	-	-	-	-
-	-	-	-	-

* 일부 항목만 발췌된 샘플입니다.

EyeOn AiSOAR (Eyeonsecurity AiSOAR)

월간 정기 보고서 샘플

Eyeon Security

대외비문서

본 문서는 기밀 자료가 포함되어 있습니다.
허가된 사람 이외에는 도용, 공유, 유출을 주의하시기 바랍니다.

보안관제서비스 5월 정기 보고서

[redacted] 님

Eyeon Security 보안관제 서비스
SOAR (Security Orchestration, Automation and Response)

II.보안관제 서비스 > 침해위협 대응 현황

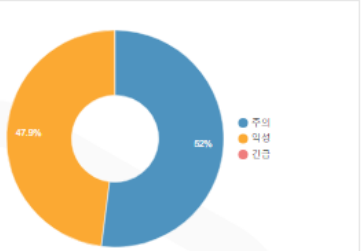
· 침해위협 분석 현황

이벤트 분석
총 10,972 건 분석 완료

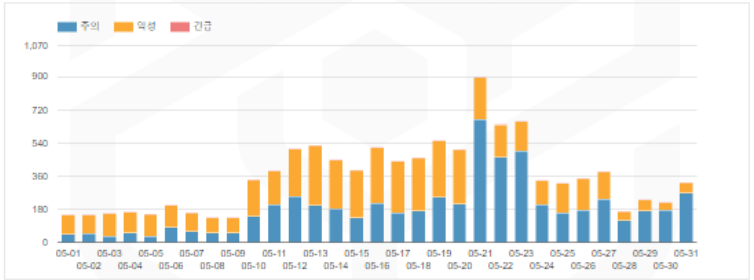
분석결과		
주의	악성	긴급
5,707 건	5,260 건	5 건

대응 내용	
위협 전파	방화벽 차단
10,972 건	IP 1,546 건

위협도 분포도



· 일별 분석 현황



· 총평

금월 총 10,972 건의 이벤트 분석 완료하였습니다.
일 평균 354건 의 침해위협 이벤트가 발생하였으며 5월 21일 에 가장 많은 공격 시도가 발생하였습니다.
이벤트 분석 결과 긴급 이벤트 5건, 악성 이벤트 5,260건, 주의 이벤트 5,707건, 발생하였으며 Apache.HTTP.Server.cgi-bin.Path.Traversal 공격시도가 가장 많이 탐지 되었습니다.

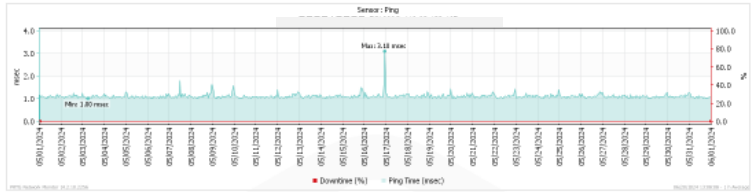
총 10,972 건의 이벤트 분석 결과 전파 완료하였으며 악성 공격 IP 총 1,546 건 방화벽 차단 내용 하였습니다.

*사단 대상의 경우 방화벽 SOAR 선사단 기능 추가가 필요한 서비스 입니다. 수동사단 내역은 보고서에 반영되지 않습니다.

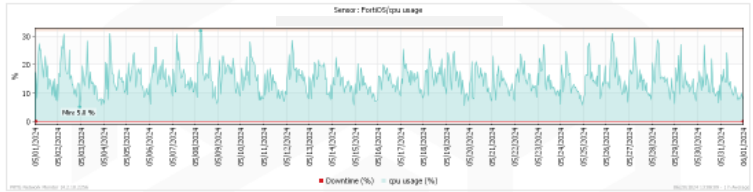
보안관제서비스 월간 보고서 [redacted]

III.NMS(Network Management System)

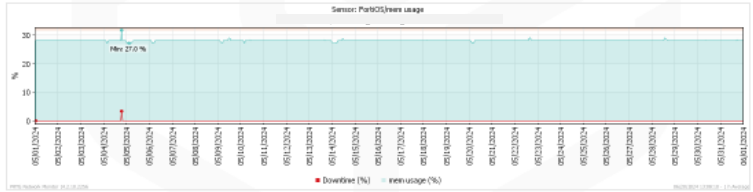
· ICMP Status



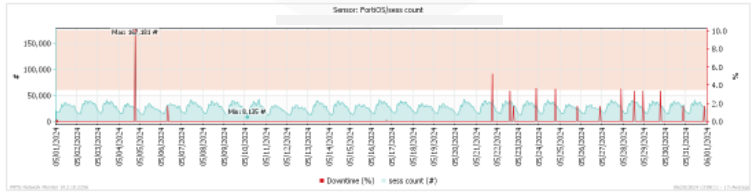
· CPU Status



· Memory Status



· Session Status



보안관제서비스 월간 보고서

* 일부 항목만 발췌된 샘플입니다.

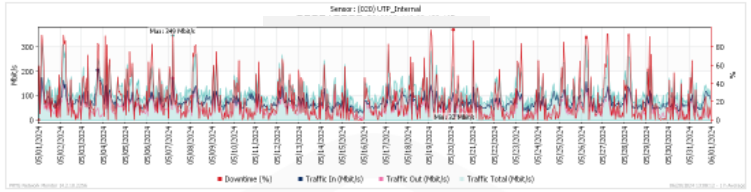
EyeOn AiSOAR (Eyeonsecurity AiSOAR)

월간 정기 보고서 샘플

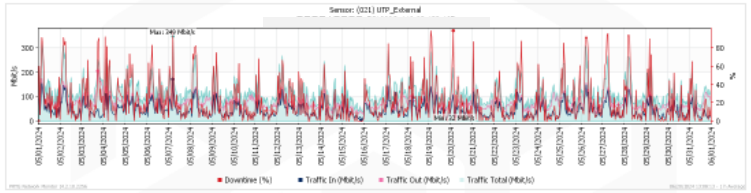
Eyeon Security

III.NMS(Network Management System)

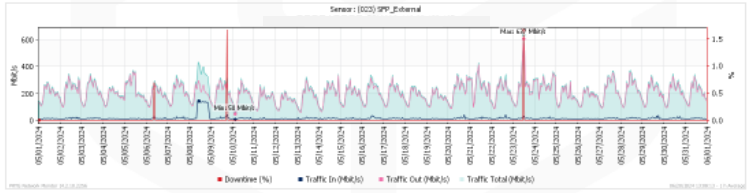
- Traffic Status



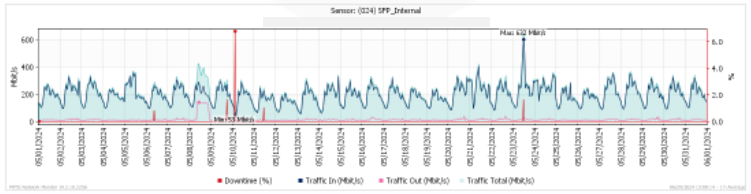
- Traffic Status



- Traffic Status



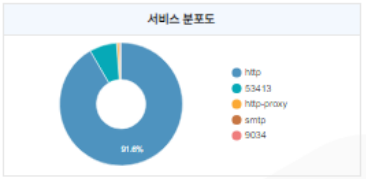
- Traffic Status

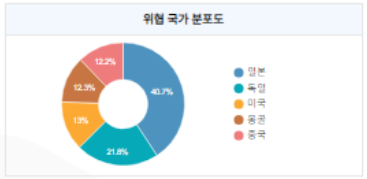


보안관제서비스 월간 보고서

V.IPS > 차단 분석

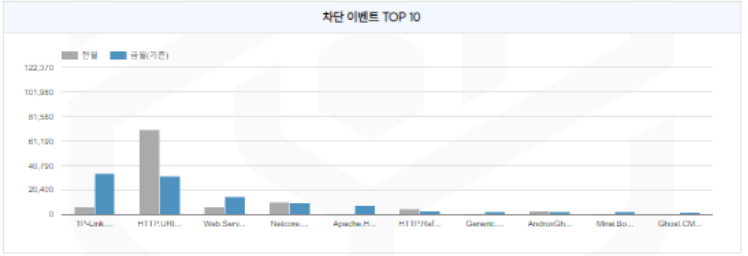
- 차단 로그 현황





Port	건수
http	124,020
53413	9,727
http-proxy	798
smtp	448
9034	365

국가 코드	건수
일본	40,717
독일	21,773
미국	12,971
몽골	12,251
중국	12,210



No	이벤트명	전월	금월(기준)	증감
1	TP-Link.Archer.AX21.Unaut...	6,332	34,061	438%
2	HTTP.URI.SQL.Injection	70,348	31,631	-55%
3	Web.Server.Password.File....	6,253	15,020	140%
4	Netcore.Netis.Devices.Har...	10,454	9,727	-7%
5	Apache.HTTP.Server.cgi-bi...	178	7,338	4,022%
6	HTTP.Referer.Header.SQL.I...	4,755	2,593	-45%
7	Generic.XXE.Detection	234	2,325	894%
8	AndroxGh0st.Malware	2,819	2,201	-22%
9	Mirai.Botnet	77	2,148	2,690%
10	Ghost.CMS.static-theme.js...	18	1,599	8,783%

보안관제서비스 월간 보고서

VI. 별첨 > 보안정보 제공 내역

No.	일시	게시판 구분	제목
1	2024-05-31 12:41:49 AM	보안 권고문	美 CISA 발표 주요 Exploit 정보공유(Update: 2024-05-29)
2	2024-05-31 12:41:17 AM	보안 동향	Weekly Security Premium Report 제 153 호 발간! 인공지능과 유머니티
3	2024-05-30 02:46:22 AM	보안 동향	개인정보보호위원회 사칭 보이스피싱 주의보!
4	2024-05-30 02:45:18 AM	보안 권고문	정부기관 사칭 피싱메일 주의 및 도메인 보안설정 권고
5	2024-05-30 02:44:57 AM	보안 권고문	美 CISA 발표 주요 Exploit 정보공유(Update: 2024-05-28)
6	2024-05-29 06:57:35 AM	보안 동향	사이버 보안에도 마감이 있나요? 네, 있습니다.
7	2024-05-27 01:01:09 AM	보안 권고문	GitLab 제품 보안 업데이트 권고
8	2024-05-27 01:00:27 AM	보안 권고문	美 CISA 발표 주요 Exploit 정보공유(Update: 2024-05-23)
9	2024-05-27 12:59:06 AM	보안 동향	안랩, 경기 성남 탄천 수진습지생태원에서 환경정화 봉사활동 진행
10	2024-05-24 12:48:48 AM	보안 동향	개인정보 유출한 카카오에 '과징금 151억'... 역대 최대 금액
11	2024-05-24 12:42:22 AM	보안 권고문	Atlassian 제품 보안 업데이트 권고
12	2024-05-23 12:24:07 AM	보안 동향	과기정통부, 2024 년도 소프트웨어 중심대학 17 개교 선정
13	2024-05-23 12:21:46 AM	보안 권고문	Veeam 제품 보안 업데이트 권고
14	2024-05-23 12:21:26 AM	보안 권고문	Rockwell Automation 제품 보안 주의 권고
15	2024-05-23 12:19:50 AM	보안 권고문	GitHub 제품 보안 업데이트 권고
16	2024-05-22 04:23:14 AM	보안 동향	클라우드 환경에서 디도스, 데이터 유출, 원격 코드 실행 공격 가능케 하는 취약점 발견돼
17	2024-05-22 04:22:07 AM	보안 권고문	美 CISA 발표 주요 Exploit 정보공유(Update: 2024-05-20)
18	2024-05-22 04:21:42 AM	보안 권고문	Mozilla 제품 보안 업데이트 권고
19	2024-05-22 04:21:19 AM	보안 권고문	Fortinet 제품 보안 업데이트 권고
20	2024-05-21 04:32:37 AM	보안 권고문	Git 제품 보안 업데이트 권고
21	2024-05-21 04:32:21 AM	보안 권고문	Intel 제품 보안 업데이트 권고
22	2024-05-21 04:31:33 AM	보안 동향	안랩의 인공지능 관련 소프트웨어에서 최고로 위험한 취약점 발견돼
23	2024-05-20 12:53:09 AM	보안 권고문	MS 5월 보안 위한에 따른 정기 보안 업데이트 권고
24	2024-05-20 12:52:43 AM	보안 권고문	美 CISA 발표 주요 Exploit 정보공유(Update: 2024-05-16)
25	2024-05-20 12:52:24 AM	보안 동향	[보안기업 특징주] 아이씨티케이, 코스닥 상장 첫날 84% 급등하며 투자자 관심↗
26	2024-05-16 12:29:36 AM	보안 동향	개인정보위, 윤석열 정부 출범 2 년 개인정보 정책 성과 어땠나
27	2024-05-16 12:29:02 AM	보안 권고문	美 CISA 발표 주요 Exploit 정보공유(Update: 2024-05-13)
28	2024-05-16 12:28:33 AM	보안 권고문	美 CISA 발표 주요 Exploit 정보공유(Update: 2024-05-14)
29	2024-05-14 12:04:41 AM	보안 동향	10 년 동안 사라졌다 새롭게 등장한 APT 단체 카데도
30	2024-05-14 12:03:12 AM	보안 권고문	수산아이앤티 제품 보안 업데이트 권

이하 생략

+상세 내역은 Mypage에서 확인 가능합니다.

보안관제서비스 월간 보고서

* 일부 항목만 발췌된 샘플입니다.

Eyeon Security

감사합니다.

365일 24시간 빈틈없는 보안, 아이온시큐리티

인공지능 보안관제, 고객 맞춤 보안장비 및 솔루션의 공급, 전문가로 구성된 보안 컨설팅까지 전문성과 신뢰성을 겸비한 보안 전문 회사입니다.

보안에 대한 열정과 철저한 전문가 정신으로 고객님께 신뢰받는 기업이 되겠습니다.
국내 최고 IT 보안 전문 기업으로 발돋움 하는 그날까지 고객님과 함께 전진하겠습니다!

02-2105-4400
영업문의: 내선 1
보안관제 기술문의: 내선 2

주소 : 서울특별시 서초구 서초대로 255 2층 (고덕빌딩) | 사업자등록번호 : 215-87-70318
통신판매업신고번호 : 제2019-서울서초-2940호 | Fax : 02-2105-4456
Tel : 02-2105-4400 (영업문의 : 내선 1 / 보안관제 기술문의 : 내선 2)