이력서

김찬혁 남 1993년 (만 33세)

휴대폰 | 010-5524-3072
Email | cksgur6512@naver.com
전화번호 | 031-235-3072
주소 | 경기 화성시 송산동

학력	경력	인턴·대외활동 / 해외경험	자격증 / 어학
한신대학교	현대오토에버㈜	신한DS nocode-해커톤 대회	통신선로기능사
대학교(4년)	재직 중	외 2	
졸업	총 8년 2개월		

CISCO | TMS | UTM | VBScript | C | Python | IPS | DDOS | Shell Script | Wireshark | cloudflare | RestAPI | SaaS | Cloud | 자동화

학력

2014. 03 ~ 2018. 02 졸업	**한신대학교** 정보통신학부
2011 졸업	**수원공업고등학교**

경력 총 8년 2개월

2026. 01 ~ 재직중	**현대오토에버㈜** 인프라보안기술팀 대리 팀원 주요직무 | 보안엔지니어,인프라보안기술팀
2022. 04 ~ 2025. 12 3년 9개월	**신한디에스** 보안인프라팀 대리 팀원 주요직무 | 정보보안, 네트워크관리, 방화벽
2018. 03 ~ 2022. 02 4년	**굿어스** ITO사업부 대리 팀원 주요직무 | 방화벽,네트워크엔지니어

경력기술서

==========
네트워크 정보보안 담당자 경력기술서
==========

==========
1. 핵심 기술 스택
==========

[Cloudflare SE]
WAF(Managed/Custom Ruleset), API Shield, Bot Management, Rate Limiting,
DDoS Protection(L3/L4/L7), Magic Transit, Workers, Logpush, DNS, SSL/TLS,
Cache/Performance

[On-Prem 보안 솔루션]
모니터랩 AIWAF, Trendmicro TippingPoint IPS, Cisco IPS, IDS, Anti-DDoS,
Paloalto, Secui BlueMax, Fortigate, FireMon, TMS, DDoS(DDX),
리눅스 백신, APT 구축 및 운영

[엔드포인트 및 내부 보안]
NAC, E-DLP, N-DLP, 매체제어, 망연계, V3(EPP), DRM, S/W 관리

[자동화 및 개발]
Python, REST API, Cloudflare API, Workers, n8n, Uptime Kuma,
Flask + SocketIO

[클라우드]
AWS Public Cloud UTM(Paloalto VM) 구축 및 운영, Cloudflare Cloud WAF

[보안 컴플라이언스]
ISMS-P, ISO 27001, PCI-DSS, 방송통신 위원회, 망분리 위원회,
지주감사, 금융감독원

[네트워크 장비]
Cisco, Extream, HPE, Alteon L4 유지보수 및 장애 조치

==========
2. 주요 업무 경험
==========

1) Cloudflare SE
WAF, API Shield, Bot Management, Rate Limiting, DDoS Protection 등
기술 전반 담당.

2) 보안 솔루션 및 장비 구축/운영
WAF, IPS/IDS, Anti-DDoS, 차세대 방화벽, 엔드포인트 보안 등
On-Prem 보안 솔루션의 구축, 정책 고도화, 취약점 대응, POC/BMT
업무 전반 수행.

3) 자동화 및 개발
Cloudflare API와 Workers, REST API 기반으로 모니터링, 백업,
취약점 탐지 자동화 Tool을 자체 개발 및 운영.

4) 보안 컴플라이언스 대응
ISMS-P, ISO 27001, PCI-DSS, 방송통신 위원회, 망분리 위원회,
금융감독원, 지주감사 인터뷰 및 지적사항 조치 업무 수행.

5) 클라우드 인프라 운영
AWS Public Cloud UTM(Paloalto VM) 구축 및 정책 자동화 연동 업무 담당.

6) 네트워크 장애 대응
모듈 교체, supervisor failover, 파워 및 지빅 교체, OS 업그레이드 등
네트워크 장비 장애 조치 수행.

==========

3. Cloudflare (기술 전반 담당)
==========

Cloudflare의 거의 모든 기술 전반에 대한 운영 담당.

[주요 운영 기능]
- WAF: Managed Ruleset, Custom Rule, OWASP Core Ruleset 운영
- API Shield: API 엔드포인트 보호, Schema Validation, mTLS 인증
- Bot Management: 봇 식별 및 차단/허용 정책 운영
- Rate Limiting: 엔드포인트별 임계값 설정 및 어뷰징 방어
- DDoS Protection: L3/L4/L7 DDoS 방어 정책 운영
- Magic Transit: BGP 기반 네트워크 레이어 보호
- DNS / SSL TLS: 도메인 관리, 인증서 발급/갱신, HTTPS 강제
- Workers: Edge 컴퓨팅을 통한 커스텀 로직 구현
- Logpush: 보안 이벤트 로그 외부 SIEM 전송

[Magic Transit BGP 전환 테스트]
- DDoS 공격 시나리오 기반 Magic Transit BGP 전환 테스트 수행
- 실제 공격 발생 시 서비스 트래픽이 Cloudflare 네트워크로 정상
전환되는지 검증 작업 진행.
- 전환 전후 서비스 정상 여부 확인 및 결과 보고서 작성

[온프렘 WAF에서 Cloudflare로의 도메인 전환 프로젝트]
- 온프렘 WAF EOS 도래에 따른 Cloudflare 클라우드 WAF 전환 프로젝트 수행
- 현행 환경 파악 및 기존 보안 정책 분석
- DNS 마이그레이션, SSL/TLS 설정, Origin 보안 강화
- WAF Ruleset 재현 (Managed Ruleset, Custom Rule, Rate Limiting)

[기술 이슈 대응 (Case Open)]
- Cloudflare 기술 이슈 발생 시 Case Open을 통한 원인 분석 및 대응
- 로그 분석, 재현 테스트, Cloudflare 엔지니어 협업을 통한 이슈 해결

==========
4. 보안 솔루션 및 장비 구축/운영
==========

On-Prem 환경의 보안 솔루션 전반에 대해 구축, 정책 고도화, 운영,
취약점 대응 업무 수행. 외곽 보호(WAF/IPS/Anti-DDoS)부터
내부 보안(엔드포인트, DLP, 매체제어)까지 전 영역 담당.

4-1. 웹 애플리케이션 방화벽 (WAF)

- 신규 보호 도메인 등록 및 차단 정책 전환
- 미등록 도메인 탐지 및 현행화 관리
- SSL/TLS 인증서 갱신 및 만료 관리
- 탐지 룰 튜닝 및 오탐 대응
- 운영 정책 표준화 및 도메인별 보안 수준 관리

4-2. 침입 방지/탐지 시스템 (IPS / IDS)

[Trendmicro TippingPoint IPS / Cisco IPS 운영]
- 시그니처 정기 업데이트 및 정책 최적화
- 탐지 이벤트 분석 및 대응, 오탐 처리
- IPS 에이징 변경 및 정기 점검

[IDS 운영]
- IDS 탐지 이벤트 실시간 분석 및 후속 대응
- 위협 패턴 분석 및 차단 정책 반영

4-3. Anti-DDoS 운영 (DDX 등)

- Anti-DDoS 정책 운영 및 공격 트래픽 분석
- DDX 에이징 변경 및 정기 시그니처 업데이트
- DDoS 대응 훈련 정기 수행
- 자체 개발 Tool(Ti-Blocker) 연계를 통한 취약 IP 자동 차단

4-4. 차세대 방화벽 (Paloalto, Secui, Fortigate, FireMon)

- 차세대 방화벽 구축으로 인한 시스템 안정화
- 펌웨어 및 라이선스 관리
- 대외 IPSec VPN 구간 통신을 위한 라우팅 전환 및
공인 IP 변환 작업 (NAT 작업)
- 시스템별 정책 고도화 작업 (중복 정책, Hiware 사용자, NTP 서버, 개발 관리 대역, 신한카드 솔루션)
- 장기 미사용 정책 및 기간 만료 정책 관리
- FireMon을 활용한 통합 정책 관리 및 정책 최적화
- 통신 트러블 슈팅 지원 (패킷 분석, 라우팅 수정, 인터페이스별 존 수정)

4-5. 악성코드 대응 (백신 / APT)

- 리눅스 서버 백신, APT Security Contents 업데이트 작업
- V3 악성코드 탐지/차단 운영 및 엔진 최신화
- 최신 소프트웨어 배포 (PMS)
- APT 탐지 이벤트 분석 및 대응

4-6. 엔드포인트 및 내부 보안

[NAC (네트워크 접근제어)]
- 네트워크 접근제어, PC on/off 관리
- 인사 DB View Table 중앙 관리
- User Agent 서버 AD 계정 연동 진행 및 점검 (VBScript)

[DLP / 개인정보 보호 (E-DLP, N-DLP)]
- 개인정보 탐지 솔루션 운영 (PcFilter, Privacy-i)
- 데이터 유출 방지 정책 운영 및 모니터링

[매체제어]
- 보안 USB 관리 및 불용 USB 관리
- 화면보호기, 워터마크 정책 적용

[망연계]
- 망간 자료 전송 및 망간 스트리밍 정책 관리 및 운영
- 망분리 정책 검토 및 반영

[DRM 및 S/W 관리]
- 문서 암호화, 화면 캡쳐 제어, 공용 폴더 암호화
- NetClient 비인가 S/W 관리 및 운영
- 인터넷 도메인 및 화이트 리스트 관리

4-7. 클라우드 보안 (AWS Cloud Paloalto UTM)

- AWS Console Security Group(SG) 및 ACL을 통한 접근 통제
- 온프레미스 FireMon과 Public Cloud VM(Paloalto) 간 정책 자동화
솔루션 연동 및 운영
- 방화벽 관리자를 위한 Paloalto 운영 메뉴얼 제작
(AWS Cloud 방화벽 구축 및 운영 기술)
- Windows Instance, Paloalto VM, 외부 사용자 간 트래픽 허용 시
발생할 수 있는 문제점, 로그 확인 방법, 관리자 사용 메뉴얼,
AWS 구축 매뉴얼 최신화 및 교육
- AWS 인프라 구성: VPC, Private/Public Subnet, Internet Gateway,
NLB, Routing, Elastic IP, EC2 Instance (Windows, Paloalto),
Windows Server 구축, NAT, Policies 구성

4-8. 네트워크 장비 유지보수 (삼성 반도체)

Cisco, Extream, HPE, Alteon L4 Switch, Router 유지보수 및 장애 조치
- 모듈 교체, supervisor failover, Power 복구, Fan 교체, 회선 포설 등
- 회선 CRC err-count 증가 (트래픽 누락 발생)로 인한 업링크 Gbic 교체
- 회선 Err-disabled 발생 시 로그 확인 및 단말 사용 여부에 따른 차단 해제
- 단말 모듈 Muxbuffer 발생 후 강제 fail-over 진행 및 Crash 파일 덤프 분석을 위한 로그 백업, 보고서 작성
- 각 벤더 모듈별 장비 점검 및 OS 업그레이드

==========
5. 자동화 및 개발
==========

운영 효율 향상과 취약점 사전 대응을 위해 다양한 자동화 Tool을
자체 개발 및 사용 중.

[자동화 Tool 통합 현황]

(1) Cloudflare API 자동 백업
- 분류: Cloudflare
- 기능: WAF 정책 및 DNS 설정 정기 자동 백업
- 기술: Cloudflare API, Python

(2) Uptime Kuma 구축
- 분류: Cloudflare
- 기능: 도메인 상태 점검, SSL 인증서 만료 모니터링, Alert 구성
- 기술: Uptime Kuma, Webhook

(3) n8n 워크플로우
- 분류: Cloudflare
- 기능: 보안 솔루션 취약 버전 자동 탐지 및 Alert 발송
- 기술: n8n, REST API

(4) Workers 기반 자동화
- 분류: Cloudflare
- 기능: Edge 로직을 통한 모니터링 강화 및 취약점 개선
- 기술: Cloudflare Workers, JavaScript

(5) Ti-Blocker (자체 개발)
- 분류: On-Prem
- 기능: abuseipdb API와 Anti-DDoS 트래픽 대조를 통한

취약 Top 10 IP 자동 분별 및 자동 차단
- 기술: Python, abuseipdb API

(6) Paloalto REST API 자동화 Tool
- 분류: Paloalto
- 기능: 다중 장비 Commit, Resource, License, Backup 등
가용성 점검 자동화
- 기술: Python, Paloalto XML/REST API

(7) 신한그룹 방화벽 모니터링 시스템
- 분류: 신한그룹
- 기능: BlueMax 다중 장비 실시간 모니터링, 동적 장비 관리
- 기술: Python Flask + SocketIO, WebSocket, NGF REST API

[Cloudflare 자동화 상세]

1) Cloudflare API 정책 자동 백업
Cloudflare API를 활용한 WAF 정책 및 DNS 설정 자동 백업 시스템 구축.
정기적 백업으로 정책 변경 이력 관리 및 복구 체계 확보.

2) Uptime Kuma 도메인 및 인증서 모니터링
보호 대상 도메인 상태 실시간 점검. SSL 인증서 만료 사전 알림 체계
구축 및 Alert 발송을 통한 장애 사전 대응.

3) n8n 기반 취약 버전 자동 탐지
운영 중인 보안 솔루션의 취약 버전 정보 자동 수집. 자동 Alert
발송으로 솔루션 버전 현행화 관리.

4) Cloudflare Workers 활용
Edge에서 동작하는 커스텀 로직을 통해 모니터링 강화. 취약점
사전 차단 및 자동화 기능 확장.

[On-Prem 자동화 상세]

Ti-Blocker (취약 IP 자동 분별 Tool)
- abuseipdb API와 온프렘 Anti-DDoS 공격 트래픽 데이터를 연동
- 실시간 공격 트래픽 분석을 통한 취약 Top 10 IP 자동 분별
- 분별된 IP 자동 방어 등록으로 대응 시간을 단축

[Paloalto 및 방화벽 자동화 상세]

1) 신한카드 Paloalto UTM REST API 자동화 Tool 개발 (Python)
- 다중 장비 Commit, Resource, License, Backup 등 가용성 점검 자동화
- Paloalto NGF XML 및 REST API 활용

2) 신한 그룹사 방화벽 모니터링 자동화
- BlueMax 다중 장비 연동, 실시간 모니터링, 동적 장비 관리
- Backend: Python Flask + SocketIO
- Frontend: HTML/CSS/JavaScript
- 통신: WebSocket을 통한 실시간 데이터 전송
- API: NGF REST API와 연동

==========

6. 보안 컴플라이언스 대응

==========

ISMS-P, ISO 27001, PCI-DSS 등 주요 보안 인증 및 감사 대응 경험 보유.

[대응 컴플라이언스]
- ISMS-P (정보보호 및 개인정보보호 관리체계 인증)
- ISO 27001 (정보보안 경영시스템 국제 표준)
- PCI-DSS (지급카드 산업 데이터 보안 표준)
- 방송통신 위원회 보안 감사
- 망분리 위원회 대응
- 금융감독원 감사
- 지주감사 대응

[주요 대응 활동]
- 방통위 보안감사 인터뷰 지원
- 보안감사 대응을 위한 정책 고도화
- 감사 지적 사항 조치
- 정보통신 망분리 정책 취합 및 결재
- ISMS-P 및 ISO 27001 인증 심사 대응 및 개선 사항 조치
- PCI-DSS 카드 데이터 보호 정책 운영 및 점검

==========

Cloudflare Edge Security와 On-Prem 보안 장비를 모두 운영하며,
자동화 도구 자체 개발을 통해 운영 효율과 보안 수준을 동시에 끌어올리는
네트워크 정보보안 전문가 입니다.

==========

인턴·대외활동

2025. 05 ~ 2025. 05
1개월

신한DS nocode-해커톤 대회 기타

n8n 자동화 Tool 과 Ai Agent를 이용한 자동화 솔루션 구현

2017. 09 ~ 2017. 09
1개월

삼성전자 사회활동

경기 남부지역 고등학생 대상인 삼성전자 드림樂서 진로박람회에 학부 대표로 선발되어 졸업작품을 출품, 전시

2016. 12 ~ 2017. 02
3개월

(주)해성옵틱스 인턴

MES 관리

라인에 구동중인 MES 관리

장비상태 확인, 실적 입력에 대한 정확성 체크, 불편사항 확인 후 보고

MES-ERP 데이터 비교

MES와 ERP실적 연동으로 데이터 일일 비교 및 오류사항 보고

일일실적 데이터 차이 유무 비교

자격증

2010. 07	**통신선로기능사** 한국방송통신전파진흥원

수상

2017년 **동계 현장실습(인턴쉽) - 최우수** 한신대학교

한신대학교 공학교육혁신센터와 컴퓨터공학부, 정보통신학부에서 공동주관하는 동계 인턴쉽에서 최우수 수여

2017년 **창의적 종합설계 경진대회(동상)** 한신대학교

라즈베리파이 통신모듈을 이용한 방범 시스템 개발

- 라즈베리파이에 연결된 웹캠과 PC를 연동하여 영상을 Wi-Fi 통신으로 PC로 전송하여 모션 인식 알고리즘을 통해 사용자의 편리함과 개인 보안시스템 시장의 활성화를 촉진시킨다는 목적으로 프로젝트를 진행했다. 또한 남녀노소를 구분하지 않고 프로그램 사용자들이 서비스를 안전하게 이용할 수 있도록 하여 범죄의 예방 등 개개인의 삶에 윤택함을 제공한다. LTE 모뎀을 이용한 SMS 전송은 통신사의 부가서비스 없이 가입자식별모듈(USIM) 장착만으로 서비스를 이용할 수 있다는 점에서 자유도가 크다고 할 수 있다. 움직임 감지시 관리자는 원격지에서 휴대폰으로 SMS를 수신 받아 보안 상황을 확인할 수 있도록 하고자 하며, 원격으로 받은 영상데이터를 통해 보다 편리한 보안시스템을 운영할 수 있도록 한다.

개발내용

1. C# .NET 기반의 AForge.net의 라이브러리를 사용하여 움직임이 탐지된 이미지들을 PC로 전송받아 자동 영상저장과 경보음 발생과 더불어 LTE 모뎀을 이용한 문자메시지 전송을 수행하도록 구현

2. 카메라에서 촬영하는 동영상을 MJPEG의 형태로 변환시켜주는 mjpeg-streamer 라이브러리를 이용하여 구축

3. Visual Studio 개발환경 하의 Windows Form을 이용하여 영상처리와 SMS 전송을 효율적으로 통제할 수 있는 환경을 설계 및 구현

4. 감지 민감도 조정 및 감지 방식 선택

5. 감지On/Off 시 영상 녹화 기능 구현

6. LTE 모뎀을 이용한 시리얼 통신 구현과 동시에 SMS 전송 기능 구현

포트폴리오

포트폴리오	PORTFOLIO.pptx

취업우대사항

보훈대상 여부	-	**취업보호대상 여부**	-	**고용지원금대상 여부**	-
병역사항	[군필] 2011. 02 ~ 2012. 11 육군 병장 제대			**장애여부**	-

희망근무조건

고용형태	정규직
희망근무지	서울전지역, 경기전지역
희망연봉	면접 후 결정
지원분야	직무 | 보안엔지니어 > 정보보안, 네트워크관리 산업 | 정보보안 > 네트워크보안, 방화벽, 정보보안, VPN, 백신프로그램 FW, APT, UTM, ddos, IPS

위의 모든 기재사항은 사실과 다름없음을 확인합니다.

작성자 : 김찬혁