01 용어 정리

용어 정리

Threat Prevention은 멀웨어·봇·익스플로잇·피싱 같은 위협을 게이트웨이에서 탐지·차단 하는 보안 묶음입니다. 이 가이드를 읽는 데 바탕이 되는 핵심 용어를 흐름에 따라 풀어 둡니다.

위협 방지 블레이드들

Threat Prevention은 여러 Software Blade의 합주입니다. **IPS**(침입 방지)는 시그니처·행위·선제 보호로 네트워크 공격을 막 고, **Anti-Bot & Advanced DNS** 는 감염된 봇을 찾아 C&C(명령·제어) 통신을 차단 하며, **Anti-Virus** 는 게이트웨이에서 멀웨어를 감염 전에 탐지 합니다.

알려지지 않은 위협을 막는 **SandBlast** 제품군에는 두 기술이 있습니다 — **Threat Emulation** 은 의심 파일을 가상 샌드박스에서 실행해 악성 행위를 탐지 하고, **Threat Extraction** 은 파일에서 악용 가능한 요소를 제거한 안전한 사본을 즉시 전달 합니다(흔히 **CDR**, Content Disarm & Reconstruction이라 부름). **Zero Phishing** 은 머신러닝으로 알려진·미지의 피싱 사이트를 실시간 차단 합니다(솔루션 개요).

이 모든 것의 두뇌가 **ThreatCloud** 입니다. Check Point의 전 세계 위협 센서가 모으는 클라우드 기반 실시간 위협 인텔리전스 로, 한 곳에서 발견된 위협 정보가 다른 보호 기능에 즉시 공유됩니다.

두 가지 접근 — Custom과 Autonomous

R82의 Threat Prevention은 두 갈래 로 운영됩니다. **Custom Threat Prevention** 은 관리자가 프로파일과 규칙을 직접 짜 세밀하게 제어 하는 전통 방식이고, **Autonomous Threat Prevention** 은 용도별로 미리 만들어진 프로파일을 골라 쓰는 간편 방식 입니다(Custom 시작하기, Autonomous 프로파일).

정책을 이루는 개념

Profile(프로파일) 은 어떤 보호를 켜고 어떤 동작을 할지 정한 설정 묶음 입니다. Custom에는 Optimized·Strict·Basic 기본 프로파일이, Autonomous에는 Perimeter·Cloud/Data Center·Internal·Guest·Monitor 등 6개 가 있습니다.

프로파일이 보호를 켤지 정하는 세 가지 잣대가 있습니다 — **Confidence Level**(공격을 정확히 식별한다는 확신 정도), **Severity**(공격 성공 시 피해 심각도), **Performance Impact**(게이트웨이 성능에 주는 영향) 입니다. 그리고 보호가 트래픽을 만났을 때의 **동작** 은 **Prevent**(차단)·**Detect**(허용하되 로그)·**Ask**(사용자에게 확인)·**Inactive**(끔) 입니다(Custom 정책과 프로파일).

규칙 묶음 전체가 **Rule Base** 이고, 규칙이 적용되는 대상 범위가 **Protected Scope** 입니다. 여러 **Policy Layer** 로 나누면 레이어마다 동작을 따로 계산하고, 여러 레이어에 걸리면 가장 엄격한 동작 을 적용합니다.

메일·연동 관련 용어

MTA(Mail Transfer Agent) 는 게이트웨이가 SMTP 메일을 받아 검사한 뒤 다음 홉으로 중계 하게 해, 메일 검사 시 연결 타임아웃을 막습니다(Custom 운영). **ICAP** 는 투명 프록시를 확장하는 프로토콜 로 서드파티 콘텐츠 검사 장비와 연동하고(ICAP), **Threat Indicator** 는 IP·파일 해시·URL 같은 관찰 가능 징후(observable)를 모은 위협 피드 입니다(Threat Indicators).

분석 도구로는 **Cyber Attack View**(공격 벡터별 시각화)와 **MITRE ATT&CK**(공격 전술·기법 지식 베이스)가 있습니다(Cyber Attack View).

02 Threat Prevention 솔루션 개요

Threat Prevention 솔루션 개요

오늘날 멀웨어는 매일 시그니처를 바꿔 기존 방어를 우회 합니다. Check Point Threat Prevention은 이에 맞서 감염 전·후를 아우르는 다층 방어 를 하나의 플랫폼으로 묶습니다. 이 장은 어떤 보호 기능이 있는지, 그리고 그것을 운영하는 두 가지 방식을 잡습니다.

위협 방지 보호 기능

여러 보호가 각자 다른 각도에서 위협을 막고, 공격 데이터를 서로 공유 해 더 강해집니다.

IPS 는 침입 방지의 핵심 으로, 수천 개 시그니처와 행위·선제 보호를 제공합니다. 알려진 익스플로잇·취약점(CVE)·프로토콜 오용·아웃바운드 멀웨어 통신·터널링 시도 를 탐지·차단하며, 방화벽이 HTTP를 허용하도록 설정돼 있어도 drive-by-download 같은 공격을 식별해 막 습니다.

Anti-Bot & Advanced DNS 는 이미 감염된 봇을 잡 습니다. 봇은 컴퓨터를 장악해 Anti-Virus를 무력화하고 C&C에 접속해 데이터 탈취·스팸·DoS 를 일으키는데, Anti-Bot은 C&C 주소, 봇넷 계열별 통신 지문, 봇 행위 를 식별해 아웃바운드 통신을 차단합니다. **Anti-Virus** 는 들어오고 나가는 파일을 검사해 감염 전에 멀웨어를 차단 하며, ThreatSpect 엔진과 ThreatCloud로 파일·URL 평판을 조회합니다.

SandBlast 는 시그니처로 못 잡는 미지의 위협 을 막습니다. **Threat Emulation** 은 파일을 가상 샌드박스에서 실행해 익스플로잇 단계에서 악성 행위를 탐지 하고(이메일 첨부·웹 다운로드·FTP/SMB·API로 받은 파일 대상), **Threat Extraction** 은 파일에서 악용 가능한 콘텐츠를 제거한 안전한 사본을 즉시 전달 해 업무 흐름을 끊지 않습니다. **Zero Phishing** 은 머신러닝과 특허 검사로 알려진·zero-day 피싱 사이트를 실시간 차단 합니다.

이 모두를 잇는 두뇌가 **ThreatCloud** 입니다 — 예컨대 Threat Emulation이 새로 찾아낸 위협의 시그니처가 ThreatCloud에 올라가 다른 보호 기능들이 즉시 활용 합니다.

두 가지 운영 방식 — Custom vs Autonomous

R82에서는 Threat Prevention을 두 갈래 로 운영합니다. 어느 쪽을 쓸지가 이 가이드 전체를 가르는 큰 줄기입니다.

Custom Threat Prevention 은 관리자가 프로파일과 규칙을 직접 설계 합니다. Optimized·Strict·Basic 프로파일을 바탕으로 Confidence·Severity·Performance 잣대를 손수 조정 하고 Rule Base를 짜므로, 정밀한 제어가 필요할 때 적합합니다 (Custom 시작하기).

Autonomous Threat Prevention 은 용도별로 미리 만들어진 6개 프로파일 중 하나를 고르면 정책이 자동 생성 됩니다 — Perimeter·Cloud/Data Center·Internal Network·Guest·Monitor 등. 빠르고 단순하게 강력한 보호를 켜고 싶을 때 적합합니다 (Autonomous 프로파일).

두 방식 모두 UserCheck·ICAP·Anti-Spam·HTTPS Inspection·Threat Indicators·분석 뷰 같은 공통 기능 을 공유하며, 이 가이드 뒷부분에서 함께 다룹니다.

> 참 고
>
> 각 보호 기능을 Software Blade 관점에서 짧게 본 소개는 Security Gateway 가이드의 Software Blade 총람에도 있습니다. 이 가이드는 그 위협 방지 부분을 깊이 파고듭니다.

03 Custom — 시작하기

Custom — 시작하기

Custom Threat Prevention 은 원하는 만큼 정밀하게 보호 수준을 조정 하거나, 그냥 기본(out-of-the-box) 설정을 그대로 쓸 수 있습니다. 이 장은 블레이드를 켜고, 기본 정책을 이해하고, 정책을 설치하는 흐름을 정리합니다.

블레이드 켜기

먼저 게이트웨이/클러스터 객체에서 Custom Threat Prevention 블레이드를 켭 니다. R82부터 **Anti-Virus** 와 **Anti-Bot & Advanced DNS** 는 새 게이트웨이에 기본으로 켜져 있습니다(단, Legacy VSX Virtual System에서는 수동으로 켜야 함).

나머지는 **General Properties** > **Network Security** 탭에서 켭니다. **IPS** 는 선택 후 마법사를 따라가고, **SandBlast Threat Emulation** 을 켜면 마법사가 Emulation Location(ThreatCloud / 로컬 어플라이언스 / 다른 어플라이언스) 을 묻고 Threat Extraction 활성화 여부 도 함께 제안합니다. **Threat Extraction** 을 켜면 웹 다운로드 검사가 자동으로 켜지며(이메일 첨부 검사는 MTA 구성 필요), **Zero Phishing** 은 마법사에서 자동 설정(권장, `tp_dummy` 더미 인터페이스 생성) 또는 게이트웨이 FQDN 을 고릅니다.

> 권 장
>
> ThreatCloud Emulation을 쓰려면 게이트웨이가 인터넷에 연결 되어야 하고 DNS·프록시 설정이 올바라야 합니다. 클라우드 에뮬레이션은 게이트웨이의 CPU·RAM·디스크를 거의 안 쓰 면서 항상 최신 OS 환경으로 검사합니다.

기본 정책 이해하기

블레이드를 하나라도 켜면 미리 정의된 규칙 하나가 Rule Base에 자동 추가 됩니다. 이 규칙은 모든 트래픽(Protected Scope = Any)을 **Optimized** 프로파일로 검사 하고, 로그를 남기며 모든 게이트웨이에 설치됩니다.

Optimized 프로파일의 결과는 이렇습니다 — Confidence가 Medium 이상이고 Performance Impact가 Medium 이하이며 Severity가 Medium 이상이면 **Prevent(차단)**, Confidence가 Low이고 Performance Impact가 Medium 이상이며 Severity가 Medium 이상이면 **Detect(탐지만)** 입니다. 즉 확신이 높고 성능 영향이 적은 위협은 막고, 애매한 것은 일단 지켜보는 균형입니다(이 잣대의 의미는 정책과 프로파일에서 자세히).

기본 규칙으로 충분하지 않으면 직접 규칙을 짭니다(프로파일·규칙 구성).

정책 설치

Custom Threat Prevention은 Access Control과 별개의 전용 정책 을 가집니다. Threat Prevention 정책만 따로 설치 하면 게이트웨이 성능 영향을 줄일 수 있습니다. **Install Policy** 에서 **Threat Prevention 을 선택** 하고 설치 모드(게이트웨이별 독립 / 같은 버전 일괄)를 고른 뒤 설치합니다.

> 참 고
>
> 실제 트래픽은 대부분 HTTP가 아니라 HTTPS이므로, Threat Prevention 효과를 극대화하려면 HTTPS Inspection을 함께 켜는 것이 권장됩니다. 모든 블레이드를 끄려면 **Install Policy** → **Uninstall Threat Prevention Policy** 를 누릅니다.

설치 후에는 Logs & Events로 트래픽을 보며 예외(Exception)를 더하거나 Rule Base를 다듬 어 갑니다.

04 Custom — 정책과 프로파일

Custom — 정책과 프로파일

Custom Threat Prevention의 심장은 **프로파일** 입니다. 어떤 보호를 켜고 어떤 동작을 할지 를 프로파일이 정하고, 규칙이 그 프로파일을 트래픽에 입힙니다. 이 장은 정책의 큰 흐름과 프로파일의 잣대를 정리합니다.

정책 만드는 흐름

이상적으로는 모든 보호를 Prevent로 두고 싶지만, 게이트웨이가 중요한 트래픽에 집중하고 가장 우려스러운 위협만 보고 하게 하려면 설정을 효과적으로 적용해야 합니다. 큰 흐름은 블레이드 켜기 → IPS·Malware DB 최신화 → (선택) Policy Package·Policy Layer 만들기 → 각 레이어에 프로파일을 Action으로 하는 규칙 구성 → 정책 설치 입니다. 관리자별로 Threat Prevention 권한(정책·설정·프로파일·보호별 읽기/쓰기) 을 권한 프로파일로 나눌 수 있습니다.

Policy Layer — 레이어별 계산

Rule Base는 여러 Policy Layer 로 나눌 수 있습니다(서비스·네트워크 기준). 각 레이어는 동작을 따로 계산 하며, 한 연결이 여러 레이어의 규칙에 걸리면 가장 엄격한 동작과 설정 을 적용합니다. 예를 들어 IPS 레이어에서 Prevent, Threat Prevention 레이어에서 Detect면 → Prevent 가 적용됩니다(단, 특정 보호에 Inactive 예외가 있으면 그 보호는 Detect로). 한 레이어뿐이면 처음 매칭된 규칙이 적용됩니다.

프로파일이란

프로파일 은 활성화할 보호와 켤 블레이드를 정한 설정 묶음 입니다. 프로파일이 보호를 켤지는 성능 영향, 위협 심각도, 식별 확신, 블레이드별 설정 에 따라 정해지며, IPS·Anti-Bot·Anti-Virus·Threat Emulation·Threat Extraction에 적용됩니다. 프로파일이 없으면 활성화 설정·확신 수준마다 규칙을 따로 만들어야 하니, 프로파일이 맞춤화와 효율을 함께 줍니다.

기본 제공 프로파일은 셋입니다 — **Optimized**(흔한 제품·프로토콜을 최신·인기 공격으로부터 잘 보호, 성능 양호 — 기본값), **Strict**(모든 제품·프로토콜을 폭넓게 보호하나 성능 영향 큼), **Basic**(비-HTTP 프로토콜 위주로 서버를 보호, 성능 영향 최소) 입니다.

세 가지 잣대와 동작

프로파일이 보호를 켤지 정하는 핵심 잣대가 셋입니다.

Performance Impact(성능 영향) 는 보호가 게이트웨이 성능에 주는 부담 으로, "High 이하 / Medium 이하 / Low 이하 / Very low" 중 어디까지 켤지 정합니다. **Severity(심각도)** 는 공격 성공 시 예상 피해 로 "Low 이상 / Medium 이상 / High 이상 / Critical" 중 어디부터 보호할지 정합니다. **Confidence Level(확신 수준)** 은 탐지한 것이 실제 공격이라는 확신 으로, 낮으면 정상 트래픽을 오탐할 수 있습니다.

이 잣대에 따라 보호가 트래픽을 만났을 때의 **동작** 이 정해집니다 — **Prevent**(파일·트래픽 차단), **Detect**(통과시키되 로그), **Ask**(사용자가 허용 여부 결정할 때까지 차단), **Inactive**(보호 끔) 입니다. Optimized 프로파일이 확신 Medium/High는 Prevent, 확신 Low는 Detect 로 두어 오탐을 줄이는 것이 그 예입니다.

프로파일 만들기·관리

기본 프로파일(Basic·Optimized·Strict)은 보거나 쓸 수는 있어도 바꿀 수는 없 습니다. 그래서 새로 만들거나(New), 복제(Clone)해서 수정합니다. 새 프로파일은 기본적으로 모든 블레이드를 포함하며, HTTPS Inspection이 켜져 있으면 Threat Emulation·Anti-Bot·Anti-Virus가 HTTPS 트래픽도 분석합니다.

작업은 모두 **Security Policies** > **Threat Prevention** > **Custom Policy Tools** > **Profiles** 에서 합니다 — New·View·Edit·Clone·Delete·Where Used(어디 쓰이는지) . 변경 이력은 Logs & Events의 Audit 로그 로 추적합니다. 만든 프로파일은 규칙의 Action 셀에서 선택 해 게이트웨이에 입힙니다(IPS 레이어에는 프로파일의 IPS 설정만 적용). 실제 규칙 구성은 프로파일·규칙 구성에서 이어집니다.

05 Custom — 프로파일·규칙 구성

Custom — 프로파일·규칙 구성

이 장은 프로파일 안에서 각 블레이드를 어떻게 세부 설정하고, 규칙과 예외를 어떻게 짜는지 를 다룹니다. 원문 분량이 가장 큰 장(70여 페이지)이라, 여기서는 무엇을 조정할 수 있는지 의 큰 줄기를 잡고 화면 단위 절차는 원문 해당 절을 참고하세요.

규칙의 구조

Threat Prevention 규칙은 **Name**, **Protected Scope**(보호 대상 범위), **Action**(프로파일), **Track**(로깅), **Install On**(설치 대상) 으로 이뤄집니다. 핵심은 **Protected Scope** 로, 누가 연결을 열었는지와 무관하게 "보호할 대상"을 지정 합니다(기본값 Any). Action 칸에는 앞 장에서 만든 프로파일을 넣습니다.

프로파일 안의 블레이드별 설정

한 프로파일 안에서 각 보호를 세부 조정할 수 있습니다.

IPS Profile 설정 으로 Confidence·Severity·Performance Impact 잣대와 보호별 동작 을 정하고, **Anti-Bot & Advanced DNS·Anti-Virus 설정** 으로 검사 대상·동작 을 조정합니다. **Threat Emulation** 은 에뮬레이션 위치(ClkoudCloud/로컬), 검사할 파일 유형·프로토콜, 에뮬레이션 환경 을, **Threat Extraction** 은 제거할 콘텐츠 종류와 사본 전달 방식 을, **Zero Phishing** 은 검사 방식 을 정합니다. **Mail 설정** 으로 메일 검사 동작도 프로파일에 둡니다.

각 설정의 의미는 솔루션 개요에서 본 각 블레이드의 역할 그대로이며, 프로파일은 그 보호들을 얼마나 공격적으로 적용할지 를 조율하는 손잡이입니다.

예외 규칙(Exception Rules)

때로는 전체 정책은 강하게 두되 특정 대상·특정 보호만 예외 로 다뤄야 합니다. **Exception Rule** 로 특정 보호(Protection)를 특정 범위에 대해 Prevent/Detect/Inactive로 바꾸거나 다른 추적 설정 을 줄 수 있습니다. 예를 들어 정상 업무 트래픽이 오탐으로 막히면, 그 보호만 해당 범위에서 예외 처리해 오탐을 풀어 줍니다.

정책과 프로파일에서 본 Policy Layer의 "가장 엄격한 동작" 원칙과 함께, 예외는 정밀 제어의 마지막 손질 역할을 합니다. 더 깊은 엔진 설정(Snort 시그니처·IPS 최적화·Allow List 등)은 고급 설정에서 다룹니다.

06 Custom — 고급 설정

Custom — 고급 설정

기본 프로파일·규칙을 넘어 엔진 수준에서 Threat Prevention을 다듬는 설정들을 모은 장입니다. 대부분 깊은 튜닝이니, 여기서는 무엇을 조정할 수 있는지 를 짚습니다.

Threat Prevention 엔진 설정

Threat Prevention Engine 설정 으로 검사 엔진의 동작 방식 을 조정합니다. 특히 **Snort Signature 지원** 으로 업계 표준 Snort 시그니처를 IPS에 가져와 활용할 수 있어, 외부 위협 인텔리전스를 폭넓게 받아들입니다.

IPS 최적화와 Allow List

IPS 최적화(Optimizing IPS) 는 성능과 보호의 균형을 맞추는 작업입니다. 정책과 프로파일에서 본 Performance Impact 잣대를 환경에 맞게 조절해, 과한 검사로 인한 성능 저하 없이 중요한 보호만 켭니다.

Allow List(허용 목록) 로 신뢰하는 트래픽·파일을 검사에서 제외 해 오탐과 불필요한 부하를 줄입니다. 프로파일·규칙 구성의 예외 규칙이 "특정 보호를 끄는" 쪽이라면, Allow List는 "특정 대상을 통째로 신뢰하는" 쪽입니다.

VSX 게이트웨이에서의 설정

VSX 게이트웨이 에서 Threat Prevention을 쓸 때의 별도 설정도 여기서 다룹니다. VSX 가이드에서 본 것처럼 가상 시스템마다 보안이 독립적이므로, 각 Virtual System 컨텍스트에서 Threat Prevention 설정 을 적용합니다(Legacy VSX에서는 Anti-Virus·Anti-Bot도 수동으로 켜야 함 — Custom 시작하기 참고).

이런 고급 설정은 Security Gateway 객체, Manage & Settings > Blades > Threat Prevention > Advanced Settings, 그리고 게이트웨이 명령줄 에 흩어져 있으며, 세부 값은 Check Point Support의 SK 문서와 함께 신중히 다룹니다.

07 Custom — 운영(MTA·모니터링·업데이트)

Custom — 운영(MTA·모니터링·업데이트)

Custom Threat Prevention을 실제로 굴리면서 다루는 작업들 — 메일 검사를 위한 MTA, 모니터링, 정기 업데이트, SSH 검사, ThreatCloud, 문제 해결 — 을 모았습니다.

MTA — 게이트웨이를 메일 전송 에이전트로

게이트웨이가 SMTP 메일을 검사할 때, 검사에 시간이 걸려 메일 클라이언트의 연결이 타임아웃 되는 일이 있습니다. **MTA(Mail Transfer Agent)** 가 이를 막습니다 — MTA가 먼저 이전 홉에서 메일을 받아 필요한 검사를 한 뒤, 다음 홉으로 중계 하는 것입니다. SMTP·TLS 암호화 트래픽을 지원 블레이드로 검사합니다.

설정은 SmartConsole에서 메일 서버를 나타내는 Host 객체를 만들고(MTA 규칙의 Next Hop), 게이트웨이에서 MTA를 활성화 하는 흐름입니다. 이메일 첨부를 Threat Emulation·Threat Extraction으로 검사하려면 MTA가 필수 입니다.

> 참 고
>
> MTA는 Autonomous Threat Prevention에서는 지원되지 않 습니다(쓰려면 Custom으로). VSX 게이트웨이에서도 동작하며 구성은 비-VSX와 같습니다. 메일을 검사만 하고 서버로 전달하지 않는 Backward Compatibility 모드 도 있습니다.

모니터링

Logs & Events 페이지에서 Threat Prevention 트래픽 로그 를 봅니다. 이 데이터로 블레이드 사용 현황을 이해하고 효과적인 Rule Base를 만들 며, 페이지에서 바로 Rule Base를 갱신할 수도 있습니다. 더 정교한 분석 뷰는 Cyber Attack View에서 다룹니다.

정기 업데이트와 ThreatCloud

위협 방지는 최신 보호가 생명 입니다. **Scheduled Updates** 로 IPS 데이터베이스·Malware 데이터베이스·Threat Emulation 엔진·이미지를 정기적으로 자동 갱신 합니다. 이 갱신의 원천이 **ThreatCloud** 로(솔루션 개요), 전 세계 위협 센서가 모은 실시간 인텔리전스 를 게이트웨이가 받아 보호에 반영합니다.

SSH Deep Packet Inspection

SSH Deep Packet Inspection 으로 암호화된 SSH 트래픽 속을 들여다봐 그 안에 숨은 위협을 검사합니다. 게이트웨이 명령줄에서 구성·파일로 설정하며, Autonomous 쪽에도 같은 기능이 있습니다(Autonomous 고급·운영).

문제 해결

Threat Prevention이 예상대로 동작하지 않으면 **Troubleshooting** 절차를 따릅니다. 블레이드 상태, 정책 설치 여부, 로그 를 확인하고, 오탐이면 예외 규칙·Allow List로 풀며, 성능 문제면 IPS 최적화로 조정합니다. 깊은 진단은 참조 장이 가리키는 커널 디버그·CLI를 활용합니다.

08 Autonomous — 6개 프로파일과 구성

Autonomous — 6개 프로파일과 구성

Autonomous Threat Prevention 은 Custom과 정반대 철학입니다. 잣대를 손수 조정하는 대신, 용도별로 미리 만들어진 프로파일 하나를 고르면 정책이 자동 생성 됩니다. 이 장은 6개 프로파일과 그 적용 흐름을 정리합니다.

6개 프로파일

Autonomous는 상황에 맞춰 고르는 6개 프로파일 을 제공합니다.

Recommended for Perimeter(기본값) — 경계 게이트웨이용 최적 보안 으로, 웹 브라우징·데이터센터·수신 메일·FTP를 보호합니다. Custom의 Optimized 프로파일과 가장 비슷하고, 한 게이트웨이에 여러 보호가 필요할 때 권장됩니다. **Strict Security for Perimeter** — 경계 게이트웨이용 최대 보안 입니다.

Cloud/Data Center — 데이터센터용 으로 서버와 east-west 트래픽을 폭넓게 보호하고, **Internal Network** — 내부 사용자·서버 간 트래픽을 최대 보안 으로 지킵니다. **Recommended for Guest Network** — 게스트(Wi-Fi) 망을 비침습적으로 모니터링(Detect 모드) 하고, **Monitor** — 로그·리포트 생성용 Detect 모드 입니다.

각 프로파일은 IPS, File & URL Reputation, ThreatCloud, Sandbox, Sanitization(CDR), C&C protection, Zero Phishing 같은 기술을 용도에 맞게 조합합니다. 예컨대 Guest·Monitor는 차단 대신 탐지(Detect)만 합니다.

구성 흐름

적용은 단순합니다. **Gateways & Servers** 에서 게이트웨이의 **Threat Prevention** 탭에서 **Autonomous Threat Prevention** 을 선택 해 켜고, **Security Policies** > **Autonomous Threat Prevention** > **Policy** 에서 프로파일을 고른 뒤 설치 하면 됩니다.

어떤 프로파일이 맞을지 모를 때는 프로파일 이름 옆 드롭다운의 **Help me decide** 를 누르면 프로파일별 차이를 비교한 표 가 열려, 환경에 맞는 것을 고를 수 있습니다. 각 프로파일은 자신이 쓰는 기술 목록을 함께 보여 줍니다.

정리하면, Custom이 "직접 조립"이라면 Autonomous는 "용도를 고르면 끝" 입니다. 고급 설정·블레이드별 세부는 블레이드별 설정과 고급·운영에서 이어집니다(단, ICAP·MTA처럼 Autonomous에서 지원되지 않는 기능은 Custom으로 전환해야 함).

09 Autonomous — 블레이드별 설정

Autonomous — 블레이드별 설정

Autonomous 프로파일을 고른 뒤에도, 게이트웨이에서 각 보호 블레이드를 세부 설정 할 수 있습니다. 이 장은 Threat Emulation·Threat Extraction·Zero Phishing·IPS의 Autonomous 설정을 정리합니다.

Threat Emulation

게이트웨이에서 **Threat Emulation** 을 설정합니다. 핵심은 에뮬레이션 위치(ThreatCloud / 로컬 어플라이언스 / 다른 어플라이언스)와 검사할 파일 유형·프로토콜 입니다. 솔루션 개요에서 본 대로, 의심 파일을 가상 샌드박스에서 실행해 익스플로잇 단계에서 악성 행위를 탐지 하는 기능이며, 더 깊은 에뮬레이션 조정은 고급·운영에서 다룹니다.

Threat Extraction

Threat Extraction 은 파일에서 악용 가능한 콘텐츠(액티브 콘텐츠·임베디드 객체)를 제거한 안전한 사본을 즉시 전달 합니다(CDR). 게이트웨이에서 제거할 콘텐츠 종류, 원본 검사 방식, 사본 전달 방식 을 설정합니다. 이메일 첨부까지 검사하려면 MTA가 필요하지만 MTA는 Custom 전용 이라는 점에 유의하세요.

Zero Phishing

Zero Phishing 은 머신러닝으로 알려진·zero-day 피싱 사이트를 실시간 차단 합니다. Custom 시작하기에서 본 것처럼, FQDN 설정(자동 `tp_dummy` 인터페이스 또는 직접 등록)이 필요하며, In-Browser Zero Phishing이 브라우저의 HTML 폼을 실시간 검사 합니다. 게이트웨이가 공인 IP로 동작하도록 포털을 구성합니다.

IPS Protections

IPS Protections 에서 개별 IPS 보호(protection)를 보고 조정 합니다. 솔루션 개요에서 본 대로 IPS는 수천 개 시그니처와 행위·선제 보호 를 제공하며, Autonomous에서는 프로파일이 적절한 보호 세트를 자동으로 적용하되, 필요하면 특정 보호를 개별 조정 할 수 있습니다.

정리하면, Autonomous는 프로파일이 큰 그림을 자동으로 잡고, 이 장의 블레이드별 설정으로 세부를 다듬는 구조입니다.

10 Autonomous — 고급·운영

Autonomous — 고급·운영

Autonomous Threat Prevention을 더 다듬고 운영하는 설정들 — 고급 설정, 고급 Threat Emulation, 정기 업데이트, SSH 검사, ThreatCloud, 개요·모니터링·문제 해결 — 을 모았습니다. 대부분 Custom 쪽과 짝을 이루며 같은 개념입니다.

고급 설정

Configuring Advanced Threat Prevention Settings 로 엔진 동작 등 고급 항목 을 조정하고, **Advanced Threat Emulation Settings** 로 에뮬레이션 환경·동작을 더 세밀하게 다듬습니다(블레이드별 설정의 Threat Emulation에서 이어짐).

업데이트·SSH·ThreatCloud

Custom 운영과 마찬가지로, **Scheduled Updates** 로 IPS·Malware DB·에뮬레이션 엔진을 정기 자동 갱신 하고, **SSH Deep Packet Inspection** 으로 암호화된 SSH 트래픽 속 위협을 검사 하며, **ThreatCloud** 에서 전 세계 실시간 위협 인텔리전스 를 받아 보호에 반영합니다. 두 트랙이 같은 ThreatCloud를 공유하므로, 한 곳에서 발견된 위협이 양쪽 모두에 즉시 반영됩니다.

개요·모니터링·문제 해결

Autonomous Threat Prevention Overview 화면에서 전체 상태를 한눈에 보고, **Monitoring** 으로 Logs & Events에서 트래픽을 분석하며, 예상대로 동작하지 않으면 **Troubleshooting** 절차로 블레이드 상태·정책 설치·로그 를 확인합니다.

정리하면, Autonomous의 운영은 Custom과 같은 도구·개념(업데이트·SSH·ThreatCloud·모니터링)을 공유 하되, 정책 설계의 수고를 6개 프로파일이 대신 짊어진다는 점만 다릅니다.

11 UserCheck

UserCheck

여기서부터는 Custom과 Autonomous 양쪽에 똑같이 적용되는 공통 기능 입니다. 그 첫 번째가 **UserCheck** — 위협을 막는 김에 사용자에게 직접 말을 거는 기능입니다.

UserCheck란

UserCheck 를 켜면, 규칙에 따라 게이트웨이가 사용자에게 직접 메시지를 보내 위험하거나 규정에 어긋나는 행동을 알립니다. 이렇게 사용자가 스스로 보안 사고를 막고 조직 정책을 익히게 돕고, 기록된 사용자 응답을 바탕으로 정책을 다듬 을 수 있습니다. UserCheck 객체를 만들어 Rule Base에서 사용자와 소통합니다.

Threat Prevention 쪽에서 UserCheck를 지원하는 블레이드는 Anti-Bot, Anti-Virus, Threat Emulation, Threat Extraction, Zero Phishing 이며, Access Control 쪽(Application Control·URL Filtering·Content Awareness)과 DLP도 지원합니다(Security Gateway 가이드의 UserCheck).

동작과 구성

사용자에게 메시지를 띄우는 방식은 두 가지입니다 — 게이트웨이의 **UserCheck Web Portal** 로 리디렉션 하거나, 단말에 **UserCheck Client** 를 설치 하는 것입니다. 그러면 사용자는 해당 메시지를 보고 필요한 동작(허용/차단 확인 등)을 직접 수행합니다.

특히 정책과 프로파일에서 본 **Ask** 동작이 UserCheck와 맞물립니다 — 보호가 파일·트래픽을 일단 막고, 사용자가 "이 연결을 보내도 되는지" 확인할 때까지 기다린 뒤, 그 결정을 Ask User 로그에 남깁니다.

구성의 큰 줄기는 Security Gateway 가이드·Security Management 가이드의 UserCheck에서 본 그대로입니다 — 게이트웨이에서 UserCheck를 켜고, Web Portal의 Main URL·인증서·접근 인터페이스를 구성 한 뒤, Rule Base에서 UserCheck 객체로 메시지를 연결합니다. Custom·Autonomous 어느 쪽이든 같은 방식으로 동작합니다.

12 ICAP

ICAP

ICAP(Internet Content Adaptation Protocol) 는 투명 프록시를 확장하는 가벼운 HTTP 유사 프로토콜 로, 보통 바이러스 검사·콘텐츠 필터에 쓰입니다. Threat Prevention에서는 게이트웨이를 서드파티 콘텐츠 검사 장비와 연동 하는 데 활용합니다.

> 참 고
>
> ICAP는 Autonomous Threat Prevention에서는 옵션이 나타나지 않 습니다. 쓰려면 **Custom Threat Prevention** 으로 전환해야 합니다.

ICAP의 동작

ICAP는 요청·응답 프로토콜 로, HTTP/1.1과 의미·사용이 비슷하지만 HTTP 자체나 HTTP 위에서 도는 앱 프로토콜은 아닙니다. RFC 3507로 표준화되어, 서로 다른 벤더의 장비가 통신할 수 있습니다.

핵심은 두 역할입니다. **ICAP Client** 는 HTTP/HTTPS 메시지를 ICAP Server로 보내 "콘텐츠 적응(content adaptation)"을 요청 하고, **ICAP Server** 는 받은 메시지에 변환 서비스를 적용해 (보통 수정된) 응답을 돌려 줍니다. 게이트웨이는 ICAP Client, ICAP Server, 또는 둘 다로 설정할 수 있습니다(Security Gateway 가이드의 ICAP도 참고).

ICAP 메서드는 셋입니다 — **REQMOD**(요청 수정), **RESPMOD**(응답 수정), **OPTIONS**(서버 설정 정보 조회) 입니다.

HTTPS와 함께 쓰기

ICAP는 HTTPS Inspection과 맞물려 강력해집니다. 흐름의 한 예는 이렇습니다 — 게이트웨이가 HTTPS 연결을 프록시 서버로 전달 → ICAP Client(RESPMOD)가 복호화 → 복호화된 콘텐츠를 ICAP Server에 보내 판정(verdict) 요청 → 판정에 따라 프록시가 허용/차단 합니다.

이렇게 토폴로지 변경 없이 서드파티 ICAP 장비와 연동 해, 기존 콘텐츠 검사 인프라를 Check Point 게이트웨이와 함께 쓸 수 있습니다. 세부 구성(Client/Server 설정, 응답 코드 등)은 원문 해당 절을 참고하세요.

13 Anti-Spam과 메일 보안

Anti-Spam과 메일 보안

끝없이 늘어나는 원치 않는 이메일(스팸)은 디스크·대역폭·CPU를 잡아먹고 업무 시간을 빼앗는 보안 위협이 됐습니다. **Anti-Spam and Mail** 은 네트워크에 도달하는 스팸 대부분을 중앙에서 손쉽게 걸러 냅니다. Custom·Autonomous 양쪽에 공통으로 적용됩니다.

Anti-Spam의 기능

스팸을 막는 방식이 여러 겹입니다.

핵심은 **Content based Anti-Spam**(콘텐츠 기반 분류 엔진) 으로, 메일 내용을 분석해 스팸을 분류합니다. **IP Reputation Anti-Spam** 은 IP 평판 서비스로 연결 시점에 스팸 대부분을 차단 하고, **Block List Anti-Spam** 은 IP·발신자 주소로 특정 발신자를 차단 합니다.

메일 자체의 위협도 막습니다 — **Mail Anti-Virus** 는 메일을 스캔해 멀웨어를 걸러 내고, **Zero Hour Malware Protection** 은 신속 대응 시그니처로 갓 등장한 멀웨어를 차단 하며, **IPS** 가 메일 보호용 침입 방지 를 더합니다.

운영

Anti-Spam 검사로 생긴 로그는 Security Management Server로 보내져 **Logs & Events** 뷰에서 보입니다(Cyber Attack View·로그). 여기서 Anti-Spam 활동의 상세 뷰·리포트를 보거나 맞춤 생성 할 수 있습니다.

메일 검사를 제대로 하려면 게이트웨이를 MTA로 구성 해 SMTP 메일을 받아 검사한 뒤 중계하게 하는 것이 핵심입니다(단, MTA는 Custom 전용). 정리하면 Anti-Spam은 콘텐츠·IP 평판·블록 리스트로 스팸을 거르고, Anti-Virus·Zero Hour·IPS로 메일 속 위협까지 함께 막는 메일 보안 묶음입니다.

14 HTTPS Inspection

HTTPS Inspection

오늘날 트래픽은 대부분 HTTPS로 암호화 되어 있어, 그 속에 위협이 숨어도 게이트웨이가 그대로는 못 봅니다. **HTTPS Inspection** 은 게이트웨이가 외부 서버와 새 TLS 연결을 맺어 복호화·검사 하게 해, Threat Prevention의 효과를 끌어올립니다. Custom·Autonomous 공통 기능입니다.

> 권 장
>
> 트래픽 대부분이 HTTPS이므로, Threat Prevention 블레이드를 켤 때 HTTPS Inspection도 함께 켜 야 Anti-Bot·Anti-Virus·Threat Emulation 등이 암호화 트래픽까지 검사할 수 있습니다 (Custom 시작하기, 정책과 프로파일).

두 가지 방향

Outbound HTTPS Inspection 은 내부 클라이언트가 외부 서버로 보내는 트래픽 을 악성으로부터 보호하고, **Inbound HTTPS Inspection** 은 인터넷에서 내부 서버로 오는 악성 요청 으로부터 보호합니다.

게이트웨이는 인증서를 써서 클라이언트와 보안 사이트 사이의 중개자 가 되어, 새 TLS 연결로 복호화한 뒤 검사합니다. 모든 데이터는 HTTPS Inspection 로그에 비공개로 보관 되며, HTTPS Inspection 권한이 있는 관리자만 로그 전체 필드 를 볼 수 있습니다.

흐름 요약

나가는 연결을 예로 들면 — HTTPS 요청이 게이트웨이에 도착 → 게이트웨이가 검사 → HTTPS Inspection 규칙과 매칭되는지 확인 → 매칭되면 복호화해 검사, 안 되면 페이로드는 그대로 둡니다. 즉 규칙에 걸릴 때만 복호화 합니다.

이 기능은 Security Management 가이드의 HTTPS Inspection·Security Gateway 가이드에서도 다루며, R82부터 정책이 Inbound·Outbound로 분리 됩니다. 인증서를 전용 하드웨어에 보관하려면 HSM을, 서드파티 검사 장비 연동은 ICAP를 함께 보세요. 규칙·인증서 구성의 세부는 원문 해당 절을 참고합니다.

15 Threat Indicators

Threat Indicators

Check Point 패키지와 ThreatCloud 피드만으로는 부족할 때가 있습니다. **Threat Indicators** 는 Anti-Bot·Anti-Virus·IPS 엔진에 직접 위협 피드를 더해 , 자체 위협 인텔리전스나 외부 소스를 활용하게 해 줍니다. Custom·Autonomous 공통 기능입니다.

Indicator와 Observable

Indicator(지표) 는 사이버 영역에서 악성 활동을 나타내는 관찰 가능 항목(observable)의 묶음 으로, 그것을 어떻게 해석하고 다룰지에 대한 정보를 함께 담습니다. **Observable(관찰 항목)** 은 관찰할 수 있는 사건이나 상태 속성 으로, 예를 들어 IP 주소, MD5·SHA1·SHA256 파일 시그니처, URL, 메일 발신자 주소 입니다.

지표는 인텔리전스·자체 분석·정부·파트너 등 에서 나오며, 특정 관찰 패턴과 부가 정보 로 공격을 표현합니다. 즉 "이 IP/해시/URL이 보이면 위협"이라는 식의 맞춤 위협 목록 을 엔진에 주입하는 것입니다.

지표 파일 올리기

지표는 SmartConsole과 CLI 양쪽 으로 올릴 수 있습니다. SmartConsole에서는 파일이 Check Point CSV 형식 또는 STIX XML(STIX 1.0) 형식 이어야 하고, 모든 레코드의 필드 수가 같아야 로드됩니다.

올리기 전에 해당 프로파일 > Indicators > Activation에서 **Enable indicator scanning** 을 켜 둬야 합니다. 그다음 Custom이면 **Security Policies** > **Threat Prevention** > **Custom Policy** > **Custom Policy Tools** > **Indicators**, Autonomous면 **Autonomous Policy** > **Autonomous Policy Tools** > **Indicators** 로 가서, **New** > **New IOC file** 로 고유한 이름을 주고 파일을 import 합니다(중복 파일·중복 이름 불가).

이렇게 Threat Indicators는 Check Point 기본 피드 위에 조직만의 위협 정보를 얹어 탐지 범위를 넓히는 도구입니다.

16 Cyber Attack View·MITRE·참조

Cyber Attack View·MITRE·참조

마지막 장은 위협을 한눈에 보는 분석 뷰 와, API·로그·CLI 같은 참조 자료를 모았습니다. 모두 Custom·Autonomous 공통입니다.

Cyber Attack View — 공격을 한눈에

Cyber Attack View - Gateway 는 공격 벡터별로 네트워크에 대한 사이버 공격을 시각화 해, 주의가 필요한 이벤트를 짚어 줍니다. **Logs & Events** > **New Tab** > **Views** 에서 `cyber` 로 검색해 엽니다. 차트 막대를 더블클릭하면 다음 드릴다운 단계로 파고들어 개별 공격까지 추적할 수 있습니다.

MITRE ATT&CK

MITRE ATT&CK 은 전 세계 보안 커뮤니티가 쓰는 위협 모델·기법 지식 베이스 입니다. 이를 통해 공격자가 우리 네트워크에 쓴 상위 기법(technique)과 전술(tactic) 을 드러내 보안 사고를 검토할 수 있습니다.

동작 원리는 이렇습니다 — Threat Emulation(SandBlast)이 악성 파일을 찾으면, 그 공격에 쓰인 기법·전술을 해당 로그에 덧붙 입니다(따라서 Threat Emulation 블레이드가 켜져 있어야 MITRE 정보가 로그에 들어감). 함께 제공되는 **Cyber Attack Timeline** 위젯은 기간별로 Anti-Bot·Anti-Virus·IPS·Threat Emulation 로그 수 를 보여 줘 대규모 공격 발생 여부를 가늠하게 합니다.

API·로그 필드·CLI 참조

Threat Prevention API 로 트래픽에서 가로챈 파일을 게이트웨이에 올려 검사 할 수 있습니다. 예컨대 HR 포털이 외부 이력서를 받을 때, 파일을 따로 보관해 사용자에게 업로드 완료를 알린 뒤 API로 검사 를 보내면 대기 시간을 없앨 수 있습니다. Cloud API(Anti-Virus·Threat Emulation, ThreatCloud 직접 접근 시 Threat Extraction까지)와 게이트웨이 Local API(API 키 생성 후 사용) 가 있습니다.

Log Fields 는 Threat Prevention 로그에 담기는 필드의 의미 를 정리한 참조로, 로그를 해석하거나 Cyber Attack View 쿼리를 짤 때 바탕이 됩니다.

명령줄·커널 참조는 다른 가이드와 마찬가지로 전용 문서로 넘깁니다 — Command Line Reference는 R82 CLI Reference Guide, 커널 파라미터·커널 디버그는 R82 Quantum Security Gateway Guide (Security Gateway 가이드의 명령줄·커널 참조)를 참고하세요. 요지는 Cyber Attack View·MITRE로 위협을 분석하고, API로 검사를 자동화하며, 로그 필드·CLI 참조로 깊이 파고든다 는 것입니다.