# [네이버 클라우드 플랫폼]

# Security Monitoring 신청서

## 신청하시기 전에 주의사항

* Security Monitoring 서비스는 외부에 공개 되어 있는 고객의 VM에 대한 보안 관제 서비스를 제공합니다.
* 외부에 공개되어 있다는 기준은 VM에 Public IP가 할당되어 있거나, Load Balancer에 연동되어 있다는 것을 의미합니다.
* Anti-Virus 상품의 경우는 외부 공개 여부와 상관없이 사용 가능합니다.
* Load Balancer 상품을 사용하시는 경우, Load Balancer 설정 시 TCP로 설정하시는 경우에는 “Proxy Protocol”을 체크해 주셔야 정확한 출발지 IP가 로깅 됩니다.

## 고객 기본 정보

|  |  |  |
| --- | --- | --- |
| **고객명** | |  |
| **계정명** | |  |
| 담당자 연락처 (1) | 전화(내선)번호 |  |
| 휴대폰번호 |  |
| 이메일 |  |
| 담당자 연락처 (2) | 전화(내선)번호 |  |
| 휴대폰번호 |  |
| 이메일 |  |
| 서비스 정보 | 서비스명 |  |
| 서비스 URL |  |
| 서비스 설명 |  |

## 신청 서비스

|  |  |
| --- | --- |
| 신청 서비스 구분 | 신청 구분 |
| IDS (침입탐지서비스) |  |
| Anti-DDoS (DDoS공격방어서비스) |  |
| WAF (웹방화벽서비스) |  |
| IPS (침입방지서비스) |  |
| Anti-Virus (서버백신서비스) |  |

### IDS (침입탐지서비스)

|  |  |
| --- | --- |
| 상품설명 | IDS (침입탐지서비스)란?  네트워크를 통해 인입되는 공격을 탐지하는 보안 솔루션으로 고객님의 서비스를 24시간 365일 모니터링 함으로써 안전하게 서비스가 운영될 수 있도록 지원합니다.  IDS를 통해 고객님의 서비스로 인입되는 공격이 탐지될 경우 공격 정보 전달해 드림으로써 대응이 가능하시도록 지원해 드립니다. |
| 제공  서비스  내역 | 보안사고 의심 이벤트 발생시 탐지 및 분석 보고서 전달  탐지 정책 운영 및 관리  고객 요청에 따른 집중 모니터링 지원  탐지 예외 처리 적용  주간/월간 보고서 제공 |

#### 서비스 신청 구간

|  |  |
| --- | --- |
| 신청 구간 | 신청 구분 |
| 1 ~ 10 |  |
| 11 ~ 30 |  |
| 31 ~ 70 |  |
| 71 ~ 100 |  |
| 101 ~ 150 |  |
| 151 ~ 200 |  |

#### 서비스 신청 정보

|  |  |
| --- | --- |
| 서비스 개시일 | 2018년 월 일 |

#### 대상 서버 정보

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| VM명 | 공인 IP 주소 | 로드밸런서명 | 공인 서비스 포트 | 사설 IP | 사설 서비스  포트 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

### IPS (침입방지서비스)

|  |  |
| --- | --- |
| 상품설명 | IPS (침입방지서비스)란?  네트워크를 통해 인입되는 공격을 탐지/차단하는 보안 솔루션으로 고객님의 서비스를 24시간 365일 모니터링하고 공격에 대해 실시간 차단함으로써 안전하게 서비스가 운영될 수 있도록 지원합니다.  IPS를 통해 고객님의 서비스로 인입되는 공격이 탐지될 경우, 공격을 차단해 드림으로써 대응이 가능하시도록 지원해 드립니다. |
| 제공  서비스  내역 | 고객 서비스에 특화된 탐지 정책 적용  탐지 예외 처리 적용  주간/월간 보고서 제공 |
| 참고사항 | 서비스 개시 후 1개월 모니터링 모드로 운영하며, 운영 결과를 검토한 후 차단 모드로 운영합니다.  서비스 개시 즉시 차단 모드를 반영할 경우에는 오탐에 의한 정상 트래픽도 차단 될 수 있습니다. |

#### 서비스 신청 구간

|  |  |
| --- | --- |
| 신청 구간 | 신청 구분 |
| 0 ~ 200Mbps |  |
| 200Mbps ~ 300Mbps |  |
| 300Mbps ~ 500Mbps |  |
| 500Mbps ~ 1Gbps |  |
| 1Gbps ~ |  |

#### 서비스 신청 정보

|  |  |
| --- | --- |
| 서비스 개시일 | 2018년 월 일 |

#### 대상 서버 정보

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| VM명 | 공인 IP 주소 | 로드밸런서명 | 공인 서비스 포트 | 사설 IP | 사설 서비스  포트 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

### WAF (웹방화벽서비스)

|  |  |
| --- | --- |
| 상품설명 | WAF (웹방화벽서비스) 이란?  WAF는 웹 공격을 전문적으로 탐지/방어하는 보안 솔루션으로 고객님의 서비스를 24시간 365일 모니터링 함으로써 안전하게 서비스가 운영될 수 있도록 지원합니다.  웹 서비스를 운영중인 고객님의 서비스로 웹 취약점을 이용한 공격이 인입 될 경우 WAF 전용 솔루션을 통해 고객님의 서비스로 인입되는 웹 공격을 탐지/방어해 드림으로써 대응이 가능하시도록 지원해 드립니다. |
| 제공  서비스  내역 | 고객 서비스에 특화된 탐지 정책 적용  탐지 예외 처리 적용  주간/월간 보고서 제공 |
| 참고사항 | 서비스 개시 후 1개월 모니터링 모드로 운영하며, 운영 결과를 검토한 후 차단 모드로 운영합니다.  서비스 개시 즉시 차단 모드를 반영할 경우에는 오탐에 의한 정상 트래픽도 차단 될 수 있습니다. |

#### 서비스 신청 구간

|  |  |
| --- | --- |
| 신청 구간 | 신청 구분 |
| 0 ~ 200Mbps |  |
| 200Mbps ~ 300Mbps |  |
| 300Mbps ~ 500Mbps |  |
| 500Mbps ~ 1Gbps |  |
| 1Gbps ~ |  |

#### 서비스 신청 정보

|  |  |
| --- | --- |
| 서비스 개시일 | 2018년 월 일 |

#### 서비스 대상 정보

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| VM명 | 공인 IP 주소 | 로드밸런서명 | 공인 서비스 포트 | 사설 IP | 사설 서비스  포트 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

### Anti-DDoS (DDoS공격방어서비스)

|  |  |
| --- | --- |
| 상품설명 | Anti-DDoS (DDoS 공격 방어 서비스)이란?  DDoS 공격을 전문적으로 탐지/방어하는 보안 솔루션으로 고객님의 서비스를 24시간 365일 모니터링 함으로써 안전하게 서비스가 운영될 수 있도록 지원합니다.  DDoS(Distributed Denial of Service) 공격은 고객님의 서비스가 정상적으로 운영이 될 수 없도록 하는 공격 유형으로써 Anti-DDoS (DDoS 공격 방어 서비스)을 통해 고객님의 서비스로 인입되는 DDoS 공격이 탐지될 경우 방어해 드림으로써 대응이 가능하시도록 지원해 드립니다. |
| 제공  서비스  내역 | 고객 서비스에 특화된 탐지 정책 적용  학습을 통한 고객 맞춤형 임계치 설정  DDoS 공격 발생시 공격 트래픽은 차단 정상 사용자의 트래픽은 접속 허용  고객 요청에 따른 DDoS 공격 자동 방어 및 대응 현황 보고  주간/월간 보고서 제공 |
| 참고사항 | 서비스 개시 후 2주간의 트래픽 학습 기간이 필요합니다.  학습 기간 중 공격이 탐지될 경우 수동 방어로 대응합니다. |

#### 서비스 신청 구간

|  |  |
| --- | --- |
| 신청 구간 | 신청 구분 |
| 0 ~ 200Mbps |  |
| 200Mbps ~ 300Mbps |  |
| 300Mbps ~ 500Mbps |  |
| 500Mbps ~ 1Gbps |  |
| 1Gbps ~ |  |

#### 서비스 신청 정보

|  |  |
| --- | --- |
| 서비스 개시일 | 2018년 월 일 |

#### 서비스 대상 정보

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| VM명 | 공인 IP 주소 | 로드밸런서명 | 공인 서비스 포트 | 사설 IP | 사설 서비스  포트 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

### Anti-Virus (서버백신서비스)

|  |  |
| --- | --- |
| 상품설명 | Anti-Virus (서버백신서비스)란?  악성코드를 탐지/방어하는 보안 솔루션으로 고객님의 서비스를 24시간 365일 모니터링 함으로써 안전하게 서비스가 운영될 수 있도록 지원합니다.  고객님이 운영 중이신 서버에 악성코드가 감염될 경우 Anti-Virus 솔루션을 통해 악성코드의 감염을 차단함으로써 고객님의 서비스가 안정적으로 운영될 수 있도록 지원해 드립니다. |
| 제공  서비스  내역 | 윈도우/리눅스 운영체제 지원  악성코드 의심 이벤트 발생시 탐지 보고서 제공  고객 요청 시 특정 파일/폴더에 대한 예외 처리 제공 |

#### 서비스 신청 정보

|  |  |
| --- | --- |
| 서비스 개시일 | 2018년 월 일 |

#### 서비스 대상 정보

|  |  |  |
| --- | --- | --- |
| VM명 | 사설 IP | 운영체제 정보 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |