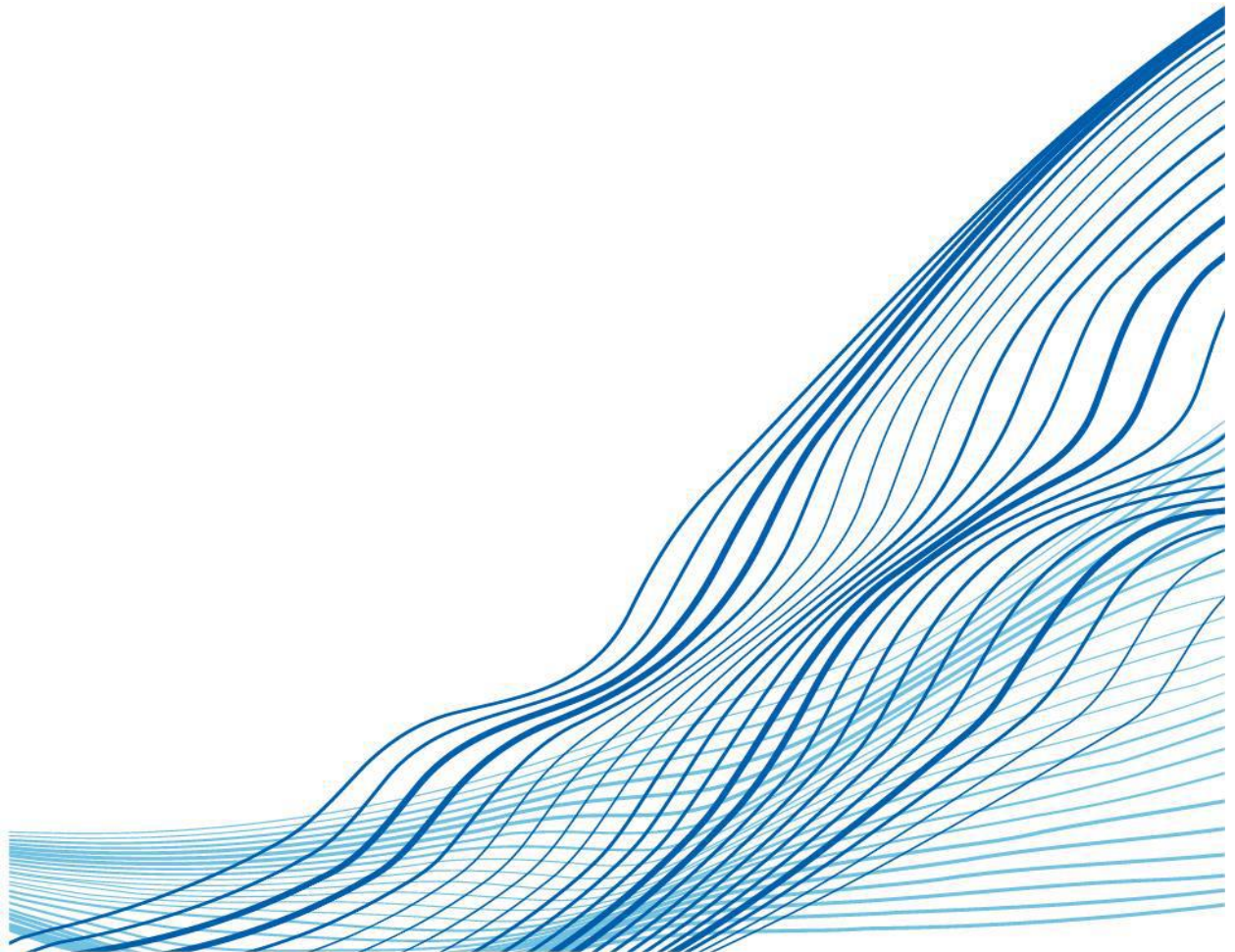




가비아 보안 관제 서비스 SLA



* SLA 종합평가 결과서

OO월 순수 원격 보안관제 서비스 수준 종합 평가 결과서

1. 서비스명 : 000 순수 보안 관제 서비스

2. 종합 평가 점수 및 등급 : 00 / 00

종합평가점수	95점 이상	90점 이상	85점 이상	80점 이상	80점 미만
평가 등급	S (탁월)	A (우수)	B (보통)	C (미흡)	F (불량)

	서비스 구분	SLA 항목	가중치	목표 수준		평가 결과	
				기대 수준	기본 수준	측정 결과	평가 점수
1	모니터링 서비스	보안 시스템 가용성 모니터링	15%	100%	98%		
2	보안관제 서비스	보안 관제 시스템 가동률	5%	99%	98%		
		침해 위협 분석 이벤트 처리율	15%	100%	98%		
		침해 위협 전파시간	15%	30분 미만	60분 미만		
		문의사항 응답률	5%	100%	98%		
3	보안 장비 운영	접근제어 정책 처리 적용	5%	20분 미만	30분 미만		
		위협 탐지 패턴 정책 처리 적용	5%	30분 미만	60분 미만		
		보안 시스템 정기 백업	5%	100%	98%		
4	장애 대응	장애 평균 전파 시간	10%	20분 미만	30분 미만		
		HOT LINE 운영률	5%	100%	98%		
	보고서	보고서 제출	5%	100%	98%		
가중치 합계			100%	-			

* SLA 세부 평가 기준

1. 모니터링 서비스

항목	내용		
SLA 항목	1.1 보안 시스템 가용성 모니터링		
측정 대상	보안 관제 계약 대상 보안 시스템 가용성		
항목 정의	보안 시스템의 가용성 상태 모니터링 및 감시(트래픽 및 퍼포먼스)		
측정 방법	<ul style="list-style-type: none"> - 당월 업무일수 분단 위 수치 측정 - 장애 예외 사항 등의 불가항력의 시간을 제외한 분 단위 측정 $\{(\text{해당 월의 일수} \times 24\text{시간} - \text{모니터링 예외 시간}) / \text{실 서비스 시간}\} \times 100$		
목표 수준	기대 수준		최소 수준
	100%		98%
측정 기준	100%이상	98%	98%미만
	1	0.8	0.6
측정 주기	매월 단위		
측정 도구	모니터링 시스템 (ESM, NMS, Observium)		
기타	- 장애 예외 사항 참조		

2. 보안관제 서비스

항목	내용		
SLA 항목	2.1 보안 관제 시스템 가동률		
측정 대상	보안 관제 시스템 (SIEM) 운영 시간		
항목 정의	보안 장비가 연동된 SIEM의 정상 가동 시간 점검		
측정 방법	<ul style="list-style-type: none"> - 당월 업무일수 분단 위 수치 측정 - 장애 예외 사항 등의 불가항력의 시간을 제외한 분 단위 측정 $\{(\text{해당 월의 일수} \times 24\text{시간} - \text{모니터링 예외 시간}) / \text{실 서비스 시간}\} \times 100$		
목표 수준	기대 수준		최소 수준
	99%		98%
측정 기준	99%이상	98%	98%미만
	1	0.8	0.6
측정 주기	매월 단위		
측정 도구	보안관제센터 통합관제 시스템 (SIEM)		
기타	- 장애 예외 사항 참조		
항목	내용		
SLA 항목	2.2 침해 위협 분석 이벤트 처리율		
측정 대상	보안 관제 시스템 (SIEM)에서 발생한 침입 탐지 이벤트		
항목 정의	사전 정의된 내/외부의 침해 이벤트를 분석 후 누락 없는 처리 여부 측정		
측정 방법	<ul style="list-style-type: none"> - SIEM에서 발생한 이벤트 건수를 기준으로 측정 $(\text{SIEM 침입탐지 이벤트 처리건수}) / (\text{SIEM 침입탐지 발생 이벤트건수}) \times 100$		
목표 수준	기대 수준		최소 수준
	100%		98%
측정 기준	100%이상	98%	98%미만
	1	0.8	0.6
측정 주기	매월 단위		
측정 도구	보안관제센터 통합관제 시스템 (SIEM)		
기타			

가비아 보안서비스 SLA

항목	내용		
SLA 항목	2.3 침해 위협 전파 시간		
측정 대상	보안 관제 시스템 (SIEM) 발생된 침입 탐지 이벤트 전파시간		
항목 정의	사전 정의된 내/외부의 침해 이벤트를 분석 후 신속한 침입 탐지 대응 수행 여부 측정		
측정 방법	<ul style="list-style-type: none"> - SIEM에서 발생된 이벤트 발생시간 대비 침입 탐지 대응 보고서 발송시간 차이 측정 - 월 단위 발생된 전체 건 별 전파 시간 측정 <p>전체 침입 탐지 대응 보고서 발송 시간(침입 탐지 대응 보고서 발송시간-침입탐지 이벤트 발생 시간)/전체 침입 탐지 이벤트 건수</p>		
목표 수준	기대 수준		최소 수준
	30분 미만		60분 미만
측정 기준	30분 미만	60분 미만	60분 이상
	1	0.8	0.6
측정 주기	매월 단위		
측정 도구	보안관제센터 통합관제 시스템 (SIEM), 침입 탐지 대응 보고서		
기타	탐지 시스템(SIEM, IPS, WAF등)에서 탐지되지 않은 침입탐지 이벤트는 특정 대상에서 제외함		
항목	내용		
SLA 항목	2.4 문의사항 응답률		
측정 대상	문의 사항 응답 현황		
항목 정의	이메일, 보안포털 등 증빙 가능한 요청 내용에 대한 누락 없는 응답률 측정		
측정 방법	<ul style="list-style-type: none"> - 문의사항 건수 = E-mail과 같이 증빙할 수 있는 방법으로 문의한 건수 - 문의사항 대응 건수 = E-mail과 같이 증빙할 수 있는 방법으로 대응한 건 <p>(문의 사항 대응 건수 / 문의사항 건수) X 100</p>		
목표 수준	기대 수준		최소 수준
	100%		98%

가비아 보안서비스 SLA

측정 기준	100%이상	98%	98%미만
	1	0.8	0.6
측정 주기	매월 단위		
측정 도구	E-Mail, 보안 포털		
기타			

3. 보안 장비 운영

항목	내용		
SLA 항목	3.1 접근제어 정책 처리 적용		
측정 대상	접근제어 정책 처리 현황 (방화벽 정책)		
항목 정의	접근제어 정책 처리에 대한 신속한 처리 현황 측정		
측정 방법	<ul style="list-style-type: none"> - 증빙 가능한 보안 포털, E-Mail을 통한 정책 신청에 대한 처리 시간 측정 - 월 단위 발생된 전체 건 별 처리 시간 측정 <p>전체 접근제어 정책 처리 시간(접근제어 정책 처리 시간-접근제어 정책 요청 시간) / 접근제어 정책 건수</p>		
목표 수준	기대 수준		최소 수준
	20분 미만		30분 미만
측정 기준	20분 미만	30분 미만	30분 이상
	1	0.8	0.6
측정 주기	매월 단위		
측정 도구	보안 포털, E-Mail		
기타			
항목	내용		
SLA 항목	3.2 위협 탐지 패턴 정책 처리 적용		
측정 대상	위협 탐지 패턴 정책 처리 현황		
항목 정의	위협 탐지 패턴 정책 처리에 대한 신속한 처리 현황 측정		
측정 방법	<ul style="list-style-type: none"> - 증빙 가능한 보안 포털, E-Mail을 통한 정책 신청에 대한 처리 시간 측정 - 월 단위 발생된 전체 건 별 처리 시간 측정 <p>전체 위협탐지 정책 처리 시간(위협탐지정책 처리 시간- 위협탐지 정책 요청 시간) / 위협탐지 정책 건수</p>		
목표 수준	기대 수준		최소 수준
	30분 미만		60분 미만
측정 기준	30분 미만	60분 미만	60분 이상
	1	0.8	0.6
측정 주기	매월 단위		

가비아 보안서비스 SLA

측정 도구	보안 포털, E-Mail		
기타			
항목	내용		
SLA 항목	3.3 보안 시스템 정기 백업		
측정 대상	보안 관제 서비스 계약된 보안 시스템 중 협의된 시스템		
항목 정의	보안 시스템의 장애 대응을 위한 백업 현황 측정		
측정 방법	<ul style="list-style-type: none"> - 백업 대상 선정 및 백업 주기 협의 - 월 단위 발생된 전체 건 별 처리 건수 측정 <p>(백업 진행 완료 건수/전체 정기 백업 건수) X 100</p>		
목표 수준	기대 수준		최소 수준
	100%		98%
측정 기준	100%이상	98%	98%미만
	1	0.8	0.6
측정 주기	매월 단위		
기타	<ul style="list-style-type: none"> - 백업 자산에 대한 선정 및 대수 확인 - 백업 주기 협의 (일/주/월) - 백업 방안은 가비아 방안을 우선으로 하며, 미적용시 SLA 측정 불가 		

4. 장애 대응

항목	내용		
서비스 구분	4. 장애 대응		
SLA 항목	4.1 장애 사항 평균 전파 시간		
측정 대상	보안 관제 계약 대상 보안 시스템		
항목 정의	보안 시스템의 실시간 관제로 장애 발생에 대한 신속한 대응 측정		
측정 방법	<ul style="list-style-type: none"> - 보안 시스템에 대한 장애 발생 시 대비 보고 시간 측정 (Health Check등) - 간헐적인 순단 현상 제외 <p>전체 장애 보고 시간(장애 보고 시간- 장애 발생 시간) / 장애 발생 건수</p>		
목표 수준	기대 수준	최소 수준	
	20분 미만	30분 미만	
측정 기준	20분 미만	30분 미만	30분 미만
	1	0.8	0.6
측정 주기	매월 단위		
측정 도구	모니터링 시스템 (ESM, NMS, Observium등)		
기타	<ul style="list-style-type: none"> - 장애 보고 방법(시간) : E-Mail, SMS, 유선(보고시간) - 장애 발생 시간 : 모니터링 시스템 측정 시간 		
항목	내용		
SLA 항목	4.2 HOT LINE 운영률		
측정 대상	HOST LINE CALL 전화		
항목 정의	365*24 운영중인 HOT LINE 운영 콜에 대한 측정		
측정 방법	<ul style="list-style-type: none"> - 당월 업무일수 분단 위 수치 측정 - HOT LINE운영 예외 시간 : 장애 예외 사항 등의 불가항력의 시간을 제외한 분 단위 측정 <p>$\{(\text{해당 월의 일수} \times 24\text{시간} - \text{HOT LINE운영 예외 시간}) / \text{실 서비스 시간}\} \times 100$</p>		
목표 수준	기대 수준	최소 수준	
	100%	98%	

가비아 보안서비스 SLA

측정 기준	100%이상	98%	100%이상
	1	0.8	0.6
측정 주기	매월 단위		
측정 도구	보안관제센터 대표 전화		
기타			

5. 보고서

항목	내용		
SLA 항목	5.1 보고서 제출		
측정 대상	보안 관제 월간 보고서		
항목 정의	월간 보안 관제 산출물		
측정 방법	$(\text{제출된 보고서 건수}) / (\text{제출되어야 할 보고서 건수}) \times 100$		
목표 수준	기대 수준		최소 수준
	100%		99%
측정 기준	100%이상	99%	99%이상
	1	0.8	0.6
측정 주기	매월 단위		
측정 도구	월간 보안 관제 보고서		
기타			

*** 장애 예외 사항**

장애 예외 사항
<ul style="list-style-type: none">- "갑"과 "을"의 사전협의 및 통보에 의한 서비스 중단 시각.- 망 사업자(KT, LG U+ 등)의 회선 장애로 인한 서비스 중단 시간(근거자료 제출).- 장애 탐지 후 담당자 부재로 인하여 유선으로 장애 통보가 어려운 경우.- 천재지변으로 인한 서비스 중단 시 (태풍, 홍수, 지진 등)

*** 서비스 수준 제재(Penalty) 및 보상(Rewards)**

서비스 수준 제재 및 보상
<ul style="list-style-type: none">- 제재는 시범 운영 결과를 바탕으로 서비스 목표 수준이 설정된 익월부터 발효하는 것을 원칙으로 함- 제재 금액은 월 서비스 대가의 10%로 설정 운영하고, 서비스 수준 종합평가 등급이 'F등급' 이하인 경우에 적용 (제재 금액 = 월 서비스 대가 x 10%)- 서비스 수준 불이행이 발생한 경우, 상호 발생 원인을 규명한 후 협의를 통해 제재 금액 지급 대상으로 확정- 보상은 제재 금액을 면제하는 것으로 함- 서비스 수준에 대한 제재와 보상은 매월 측정하며 상호 협의에 의하여 확인한 후 처리함