SIEM 수집로그 우선순위 목록: 실무자 지침

Australian Government

Australian Signals Directorate

National Cyber Security Centre

a part of GCHQ

Communications Security Establishment

Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications

Centre canadien pour la cybersécurité

Te Tira Tiaki

Government Communications Security Bureau

National Cyber and Information Security Agency

ASD는 이 간행물에 기여한 파트너들에게 감사의 말씀을 전합니다.

목차

소개

이 발행물에서 작성 기관은 사이버 보안 실무자에게 보안 정보 및 이벤트 관리(SIEM) 플랫폼에서 우선적으로 수집해야 하는 로그에 대한 자세한 권장 사항을 제공합니다. 이 문서의 권장 사항은 일반적인 조언으로 간주해야 하며, 각 조직은 로그의 수집, 중앙 집중화 및 분석을 특정 환경과 위험 프로필에 맞게 조정해야 합니다. 또한 실무자는 SIEM에서 수집하는 데이터 소스의 수와 유형을 한 번에 모두 추가하기보다는 점진적으로 늘려가는 접근 방식을 채택해야 합니다. 작성 기관에서는 각 운영 체제에 맞는 정보가 있는 경우 공급업체별 지침을 참조할 것을 권장합니다.

따라서 이 문서는 일반적으로 조직의 SIEM 구축 및 유지 관리를 담당하는 팀을 대상으로 합니다. 그러나 헌트 또는 블루팀도 우선순위 이벤트 ID에 대한 지침을 시작점으로 삼아 적대적 활동을 검색하거나 조직 네트워크에서 정상적 비즈니스 활동(비이상행위)의 기준을 구축할 수도 있습니다.

용어에 대한 참고 사항: 모든 SIEM 플랫폼에는 로그 수집 기능이 있습니다. 일부 SOAR(보안 오케스트레이션, 자동화 및 대응) 플랫폼도 이 기능을 수행하거나 SIEM이 내장되어 있습니다. 조직에서 SIEM이 내장된 SOAR 플랫폼을 사용하는 경우, 다음 권장 사항이 로그 수집과 관련이 있습니다.

이 문서의 시리즈

이 게시글은 SIEM/SOAR 플랫폼에 대한 세 가지 지침 중 하나입니다:

SIEM 및 SOAR 플랫폼 구현하기: 경영진 지침

이 문서는 경영진을 대상으로 작성되었습니다. SIEM/SOAR 플랫폼을 정의하고, 그 장점과 과제를 간략하게 설명하며, 경영진과 관련된 구현에 대한 광범위한 권장 사항을 제공합니다.

SIEM 및 SOAR 플랫폼 구현하기: 실무자 지침

이 문서는 사이버 보안 실무자를 대상으로 합니다. 기술적인 세부 사항에서는 SIEM/SOAR 플랫폼을 정의하고, 장점과 과제를 간략하게 설명하며, 구현을 위한 모범 사례를 제공합니다.

SIEM 수집을 위한 우선 순위 로그: 실무자 지침

이 문서는 사이버 보안 실무자를 위한 것으로, SIEM 수집을 위해 우선순위를 정해야 하는 로그에 대한 자세한 기술 지침을 제공합니다. 엔드포인트 탐지 및 대응 도구, Windows/Linux 운영 체제, 클라우드 및 네트워크 장치를 포함한 로그 소스를 다룹니다.

이 지침은 로깅 전략 개발에 대한 높은 수준의 권장 사항을 제공하는 '이벤트 로깅 및 위협 탐지 모범사례(Best practices for event logging and threat detection)'와 함께 읽어야 합니다.

위험 고려 사항

앞서 언급한 바와 같이 로깅에 대한 결정은 조직의 특정 환경과 위험 프로필에 기반하여 이루어져야 합니다. 아래 권장 사항은 시작점을 제공하지만, 조직은 위협과 위험을 모델링하고 위험 프로필과 가장 관련성이 높은 데이터 소스를 선택하는 것이 중요합니다.

조직은 각 데이터 소스에 대해 다음 항목들을 평가해야 합니다:

- 목적 또는 사용 사례 - 작성 기관은 단순히 기록하기 위한 로깅을 지양합니다.
- 우선순위 - 우선순위가 높은 데이터 소스를 신규 SIEM 배포시 먼저 수집하고 정기적으로 상태를 점검해야 합니다. 이 문서에서는 데이터 소스의 광범위한 범주에 따른 권장 우선순위 순서를 제시합니다.
- 생성되는 로그의 양 - 예를 들어 방화벽이나 DNS 로그는 정보의 중요성을 희석시킬 정도로 시스템에 영향을 주는 대량의 로그를 생성할 수 있습니다.
- 분석적 가치 - 예를 들어, 대량의 데이터 소스는 시간적 이상 징후를 탐지하는 쿼리에 활용할 수 있습니다. 또한 다른 데이터 소스와의 상관관계를 분석하는데도 활용할 수도 있습니다(예: 위협 인텔리전스에서 식별한 악성 IP 주소에 대한 대용량 방화벽 로그 분석).

아키텍처 고려 사항

이 게시물의 핵심 전제는 로깅의 아키텍처가 2단계 프로세스를 포함한다는 것입니다:

1. 로그 생성, 수집 및 중앙 집중화 지점으로의 전송
2. 소스에서 직접 또는 중앙 집중화 지점에서 SIEM이 해당 로그를 수집

조직은 다양한 소스를 로깅하고 이러한 로그를 중앙 위치로 전송해야 하는 법적 또는 규제상의 이유가 있을 수 있습니다. 그러나 작성 기관에서는 모든 로그의 중앙 리포지토리로 SIEM을 사용하는 것을 강력히 권장하지 않습니다. SIEM은 조직의 위험 프로필에 따라 특정 보안 로그를 중앙 집중화하는 용도로만 사용해야 합니다.

우선순위가 지정된 로깅 목록

이 문서에서는 데이터 소스 범주별로 느슨한 우선순위에 따라 로깅 이벤트 표를 제시합니다. 이 로깅 표는 완전한 것이 아니며 모든 조직에 적용 가능한 순서도 아닙니다. 작성 기관은 조직이 일반적인 엔터프라이즈 네트워크 환경에서 본 우선순위를 출발점으로 삼을 것을 권장합니다. 조직은 로그 신뢰성, 각 로그 또는 로그 유형이 제공하는 가시성, 잠재적 가능성, 수집이 성능에 미치는 영향, 그리고 이러한 데이터를 유지 관리하고 분석하는 데 드는 조직적 비용을 고려해야 합니다. 또한 조직은 고유한 위협, 역량, 요구 사항에 따라 우선순위를 조정해야 할 수도 있습니다.

AD(Active Directory) 이벤트 ID의 경우 그룹 정책 변경 사항이 본 문서 말미에 참조용으로 추가되었습니다.

SIEM 수집을 위한 우선순위 로그 각주 범례

다음 작성 기관 문서는 이 문서 내에서 참조되며 문서 전체에 각주로 표시됩니다:

CCST – Cloud Computing Security for Tenants | Cyber.gov.au
https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/cloud-security-guidance/cloud-computing-security-tenants

CCSCSP – Cloud Computing Security for Cloud Service Providers | Cyber.gov.au
https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/cloud-security-guidance/cloud-computing-security-cloud-service-providers

DMADC – Detecting and mitigating Active Directory compromises | Cyber.gov.au
https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/detecting-and-mitigating-active-directorycompromises

WELF – Windows Event Logging and Forwarding | Cyber.gov.au
https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-monitoring/windows-event-logging-and-forwarding

HMWW – Hardening Microsoft Windows 10 and Windows 11 Workstations | Cyber.gov.au
https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/hardening-microsoft-windows-10-andwindows-11-workstations

자세한 로깅 안내

다음 범주의 데이터 소스는 우선순위에 따라 느슨하게 분류한 것입니다.

1. 엔드포인트 탐지 및 대응(EDR) 로그

엔드포인트 탐지 및 대응(EDR) 로그		
카테고리	**하위 카테고리**	**이벤트**
AmCache	프로세스 생성 시 사용되는 레지스트리 파일	전체 대상
바이러스 백신	서명 감지	전체 대상
	평판 알림	전체 대상
	기타 탐지	전체 대상
네트워크 연결 및 포트	포트(최근 또는 활성)	전체 대상
	프로토콜(최근 또는 활성)	전체 대상
	IP(최근 또는 활성)	전체 대상
동적 링크 라이브러리	잘못된 경로 DLL	전체 대상
예약된 작업	기존	수정 내역만 해당
	생성	전체 대상
파일 이벤트	무단 파일 액세스 시도가 실패한 경우	전체 대상
	실행	전체 대상
	다운로드	전체 대상
파일 시스템 변경 사항	사용자 프로필 생성	전체 대상
	사용자 프로필 레지스트리 키	수정 내역만 해당
	사용자 프로필 파일	수정 내역만 해당
시스템 정보	시스템 이름	전체 대상
	호스트 이름	전체 대상
	타임스탬프	전체 대상
	시간대	전체 대상
	OS 정보	전체 대상
	프로세서	전체 대상
DNS 캐시	도메인 이름 확인	전체 대상
	네트워크 연결.	전체 대상
Windows 레지스트리	마지막 수정 시간	전체 대상
	수정 사항	전체 대상
	하이브 위치	전체 대상

엔드포인트 탐지 및 대응(EDR) 로그		
카테고리	**하위 카테고리**	**이벤트**
Windows 서비스	서비스 이름	전체 대상
	설명 이름	전체 대상
	서비스 설명	전체 대상
	PID	전체 대상
	경로	전체 대상
	인자	전체 대상
	서비스 상태	전체 대상
	서비스 유형	전체 대상
	ServiceDLL	전체 대상
	레지스트리 키 마지막 수정 타임스탬프	전체 대상
명령 기록	최근에 실행한 명령	전체 대상
Prefetch	시스템 부팅	전체 대상
	애플리케이션 시작	전체 대상
대체 데이터 스트림	Any	전체 대상
브라우저 기록	입력한 URL 캐시	전체 대상
심캐시	PE 파일 메타데이터	수정 내역만 해당
쉘백	GUI 기본 설정	전체 대상
레지스트리	레지스트리 수정	전체 대상
LNK 파일	바로 가기 실행	생성/수정 내역만 해당
백그라운드 활동 중재자(BAM)	프로세스 활동	수정 내역만 해당
점프 목록	실행	생성/수정 내역만 해당

2. 네트워크 장치 로그

네트워크 장치 로그		
기능	**하위 카테고리**	**이벤트**
방화벽	Ingress 데이터 흐름	거부 내역만 해당
	Egress	거부 내역만 해당
	Egress	허용 내역만 해당
	Ingress(선택 사항)	허용 내역만 해당
	실행 상태	수정 내역만 해당
	구성	수정 내역만 해당
	구성 읽기/덤프	전체 대상
	인증 및 권한 부여	전체 대상
	시스템 변경 이벤트	전체 대상
코어 라우터/스위치	Ingress	NetFlow 항목
	인증 및 권한 부여	전체 대상
	Egress	NetFlow 항목
	실행 상태	수정 내역만 해당
	시스템 변경 이벤트	전체 대상
	구성 읽기/덤프	전체 대상
	구성	수정 내역만 해당
라우터/스위치	라우팅 테이블	수정 내역만 해당
	인증 및 권한 부여	전체 대상
	중요 서버/서비스(서브넷-VLAN)	NetFlow 항목
	관리자/IT 보안(서브넷-VLAN)	NetFlow 항목
	개발 서브넷 및 VLAN	NetFlow 항목
	실행 상태	수정 내역만 해당
	시스템 변경 이벤트	전체 대상
	구성 읽기/덤프	전체 대상
	구성	수정 내역만 해당
침입 탐지/방지 시스템	보안 알림	알림 내역만 해당
	인증 및 권한 부여	전체 대상
	실행 상태	수정 내역만 해당
	인증 및 권한 부여	전체 대상
	시스템 변경 이벤트	전체 대상
	구성 읽기/덤프	전체 대상
	구성	수정 내역만 해당

네트워크 장치 로그		
기능	**하위 카테고리**	**이벤트**
애플리케이션 레이어 게이트웨이	콘텐츠 검사 로그	전체 대상
	인증 및 권한 부여	전체 대상
	실행 상태	수정 내역만 해당
	시스템 변경 이벤트	전체 대상
	구성 읽기/덤프	전체 대상
	구성	수정 내역만 해당
네트워크 액세스 제어(NAC)	NAC 인증 이벤트	전체 대상
경계 방화벽	Ingress 데이터 흐름	거부 내역만 해당
	인증 및 권한 부여	전체 대상
	Egress	허용 내역만 해당
	Ingress(선택 사항)	허용 내역만 해당
	실행 상태	수정 내역만 해당
	구성	수정 내역만 해당
	구성 읽기/덤프	전체 대상
	시스템 변경 이벤트	전체 대상
보더 라우터/로드 밸런서	Ingress	NetFlow 항목
	인증 및 권한 부여	전체 대상
	Egress	NetFlow 항목
	실행 상태	수정 내역만 해당
	시스템 변경 이벤트	전체 대상
	서비스/프로세스 다시 시작	전체 대상
	서비스/프로세스 다시 로드	전체 대상
	구성 읽기/덤프	전체 대상
	구성	수정 내역만 해당
웹 프록시	웹 쿼리 로그	전체 대상
	인증 및 권한 부여	전체 대상
	SSL/TLS 검사	전체 대상
	실행 상태	수정 내역만 해당
	서비스/프로세스 다시 시작	전체 대상
	서비스/프로세스 다시 로드	전체 대상
	시스템 변경 이벤트	전체 대상
	구성 읽기/덤프	전체 대상
	구성	수정 내역만 해당

네트워크 장치 로그		
기능	**하위 카테고리**	**이벤트**
가상 사설망(VPN)	허용된 연결	전체 대상
	거부된 연결	전체 대상
	인증 및 권한 부여	전체 대상
	구성 읽기/덤프	전체 대상
	실행 상태	수정 내역만 해당
	시스템 변경 이벤트	전체 대상
	구성	수정 내역만 해당
	구성 읽기/덤프	전체 대상
	타임스탬프	전체 대상
	이벤트 유형 [연결됨, 연결 끊김, 실패 또는 알 수 없음]	전체 대상
	오리진 ID	전체 대상
	출처 유형	전체 대상
	사용자 ID	전체 대상
	조직 ID	전체 대상
	세션 ID	전체 대상
	세션 유형	전체 대상
	VPN 프로필	전체 대상
	공용 IP	전체 대상
	할당된 IP	전체 대상
	다음에서 연결	전체 대상
	연결 해제 이유	전체 대상
	호스트 이름	전체 대상
	OS 버전	전체 대상
	VPN 버전	전체 대상
	사용자 에이전트	전체 대상
메일 어플라이언스	IP 및 도메인 평판	전체 대상
	발신자	전체 대상
	수신자	전체 대상
	제목	전체 대상
	첨부 파일 이름	전체 대상

3. Microsoft 도메인 컨트롤러

다음 이벤트 ID와 관련된 그룹 정책 변경 사항은 이 문서 끝에 있는 추가 참고자료를 참조하세요.

Microsoft 도메인 컨트롤러 로그 유형		
카테고리	**하위 카테고리**	**이벤트 ID**
계정 로그온	자격증명 유효성 검사 감사	4776(S, F)
	Kerberos 인증 서비스 감사	**4768**[1] (S, F)
	케르베로스 서비스 티켓 작업 감사	**4769**[2] (S, F)
계정 관리	**컴퓨터 계정 관리 감사**[3]	**4741**[4], 4742, 4743
	기타 계정 관리 이벤트 감사[5]	4739
		4727, 4728, 4729, 4730,
	보안 그룹 관리 감사[6]	4731, 4732, 4733, 4734,
		4735, 4737, 4754, 4755,
		4756, 4757, 4758, 4764
	DCSync	4928, 4929
		4675[8], 4720, 4722, 4723,
		4724[9], 4725, 4726,
	사용자 계정 관리 감사[7]	**4738**[10], **4740**[11], 4767,
		4780, 4781, 4794, 5376,
		5377

1 자세한 내용은 DMADC 표 2, 표 6, 표 10, 표 14를 참조하세요.
2 자세한 내용은 DMADC 표 1, 표 10을 참조하세요.
3 자세한 내용은 WELF를 참조하세요.
4 자세한 내용은 DMADC, 표 4를 참조하십시오.
5 자세한 내용은 WELF를 참조하십시오.
6 자세한 내용은 WELF를 참조하십시오.
7 자세한 내용은 WELF를 참조하십시오.
8 자세한 내용은 DMADC 표 15를 참조하십시오.
9 자세한 내용은 DMADC 표 4를 참조하십시오.
10 자세한 내용은 DMADC 표 2, 표 15를 참조하십시오.
11 자세한 내용은 DMADC 표 3을 참조하십시오.

인증서 서비스	서비스 장애	**39**[12]
	서비스가 시작되지 않음	**40**[13]
	호환되지 않는 SID	**41**[14]
	인증서 내보내기	**70**[15]
	CA 데이터베이스 백업	**4876**[16]
	인증서 요청	**4886**[17]
	인증서 발급	**4887**[18]
	템플릿 업데이트	**4899** [19]
	템플릿 보안 업데이트	**4900**[20]
상세 추적	DPAPI 활동 감사	4695
	감사 프로세스 생성[21]	**4688**[22], 4696
	감사 프로세스 종료[23]	4689
	프로세스 생성 이벤트에 명령줄 포함[24]	4688
DS 액세스	디렉터리 서비스 액세스 감사	4661, **4662**[25]
	디렉터리 서비스 변경 감사	**5136**[26], 5137, 5138, 5139, 5141
덤핑	섀도 복사본	**8222**[27]
페더레이션 서비스[28]	구성 변경	**307**[29]
	이벤트 ID 307 지원을 위한 추가 정보	**510**[30]
	서명 인증서 내보내기	**1007**[31]
	감사 로그 지우기	**1102**[32]
	토큰 발행	**1200**[33]
	새로운 자격 증명 유효성 검사	**1202**[34]

12 자세한 내용은 DMADC 표 6을 참조하세요.
13 자세한 내용은 DMADC 표 6, 표 18을 참조하세요.
14 자세한 내용은 DMADC 표 6, 표 18을 참조하세요.
15 자세한 내용은 DMADC 표 7을 참조하십시오.
16 자세한 내용은 DMADC 표 7을 참조하십시오.
17 자세한 내용은 DMADC 표 6을 참조하십시오.
18 자세한 내용은 DMADC 표 6을 참조하십시오.
19 자세한 내용은 DMADC 표 6, 표 19를 참조하십시오.
20 자세한 내용은 DMADC 표 6, 표 19를 참조하십시오.
21 자세한 내용은 HMWW를 참조하십시오.
22 자세한 내용은 DMADC 표 5, 표 8을 참조하십시오.
23 자세한 내용은 HMWW를 참조하십시오.
24 자세한 내용은 HMWW를 참조하십시오.
25 자세한 내용은 DMADC 표 8, 표 12를 참조하십시오. 카나리아를 사용하여 탐지하기를 참조하세요.
26 자세한 내용은 DMADC 표 1, 표 2를 참조하십시오.
27 자세한 내용은 DMADC 표 9를 참조하세요.
28 자세한 내용은 DMADC 표 12를 참조하세요.
29 자세한 내용은 DMADC 표 12, 표 20을 참조하세요.
30 자세한 내용은 DMADC 표 12, 표 20을 참조하십시오.
31 자세한 내용은 DMADC 표 12, 표 20을 참조하십시오.
32 자세한 내용은 DMADC를 참조하십시오.
33 자세한 내용은 DMADC 표 12, 표 20을 참조하십시오.
34 자세한 내용은 DMADC 표 12, 표 20을 참조하십시오.

Kerberos	로그온 티켓	4678
	서비스 티켓	4679
	갱신된 티켓	**4770**[35]
LDAP	Bind	**2889**[36]
로그온 및 로그오프	**계정 잠금 감사** [37]	**4625**[(38)] (F)
	로그오프 감사 [39]	4634(s), 4647(s)
	로그온 감사 [40]	**4624**[41], **4625**[42], **4627**[43], 4634, 4647, **4648**[44], 4779
	특별 로그온 감사 [45]	4964(s), 4672(s)
개체 액세스	커널 개체 감사	**4663**[(46)] (S)
	기타 개체 액세스 이벤트 감사[47]	4671(-), 4691(s), 5148(f), 5149(f), 4698(s), 4699(s), 4700(s), 4701(s), 4702(s), 5888(s), 5889(s), 5890(s)
권한 사용	민감한 권한 사용 감사	**4673**[(48)](S, F), **4674**[(49)](S, F) 4985(S, F)
정책 변경	감사 인증 정책 변경	4670(s), 4706(s), 4707(s) 4716(s), 4713(s), 4717(s), 4718(s), 4739(s), 4864, 4865(s), 4866(s), 4867(s)
	감사 승인 정책 변경	**4703**[(50)] (S, F)
	감사 정책 변경[51]	4719(S, F)
	기타 정책 변경 감사[52]	4719(S, F)

35 자세한 내용은 DMADC 표 5를 참조하십시오.
36 자세한 내용은 DMADC 표 3을 참조하십시오.
37 자세한 내용은 HMWW를 참조하십시오.
38 자세한 내용은 DMADC 표 2, 표 3을 참조하십시오.
39 자세한 내용은 WELF를 참조하십시오.
40 자세한 내용은 WELF를 참조하십시오.
41 자세한 내용은 DMADC 표 3, 표 4, 표 5, 표 11을 참조하십시오.
42 자세한 내용은 DMADC를 참조하십시오.
43 자세한 내용은 DMADC 표 11을 참조하십시오.
44 자세한 내용은 DMADC 표 3을 참조하십시오.
45 자세한 내용은 HMWW를 참조하십시오.
46 자세한 내용은 DMADC 표 8, 표 16을 참조하십시오.
47 자세한 내용은 DMADC 표 8, 표 16을 참조하십시오.
48 자세한 내용은 DMADC 표 16을 참조하십시오.
49 자세한 내용은 DMADC 표 6을 참조하십시오.
50 자세한 내용은 DMADC 표 16을 참조하십시오.
51 자세한 내용은 WELF를 참조하십시오.
52 자세한 내용은 WELF를 참조하십시오.

시스템	IPsec 드라이버 감사	4960(s), 4961(s), 4962, 4963, 4965, 5478, 5479(s), 5480(f), 5483(f), 5484(f), 5485(f)
	보안 상태 변경 감사	4608(s), 4616(s), 4621(s)
	보안 시스템 확장 감사	4610, 4611, 4614, 4622, **4697**[53]
	시스템 무결성 감사[54]	4612, 4615, 4618, 5038, 5056, 5061, 5890, 6281, 6410
	지역 보안 기관 하위 시스템 서비스	**3033**[55], **3063**[56]

4. 액티브 디렉터리(AD) 및 도메인 서비스 보안 로그

다음 이벤트 ID와 관련된 그룹 정책 변경 사항은 이 문서 끝에 있는 추가 참조를 참조하세요.

액티브 디렉터리(AD) 및 도메인 서비스 보안 로그		
카테고리	**하위 카테고리**	**이벤트 ID**
시스템 무결성	보안 이벤트 패턴 발생	4618
로그온/로그오프	리플레이 공격 - 탐지됨	4649
	특수 그룹에 새 로그온 할당	4964
디렉터리 서비스 액세스	개체에 대한 작업이 수행되었습니다.	**4662**[57]
개체 액세스	권한 - 변경됨	4670
	역할 분리 활성화	4897
권한 있는 사용	권한 있는 서비스 - 호출	**4673**[58]
프로세스 추적	감사 가능한 보안 데이터의 보호가 시도되었습니다.	4694
사용자 권한[59]	사용자 권한 - 조정됨	**4703**[60]
	사용자 권한 - 할당됨	4704
	사용자 권한 - 제거됨	4705
도메인	새 트러스트 생성	4706
	트러스트 제거됨	4707

53 자세한 내용은 DMADC 표 16을 참조하세요.
54 자세한 내용은 WELF를 참조하십시오.
55 자세한 내용은 DMADC 표 16, 표 18을 참조하십시오.
56 자세한 내용은 DMADC 표 16을 참조하십시오.
57 자세한 내용은 DMADC 표 8, 표 12를 참조하십시오.
58 자세한 내용은 DMADC 표 16을 참조하십시오.
59 자세한 내용은 HMWW를 참조하십시오.
60 자세한 내용은 DMADC 표 16을 참조하십시오.

AD(Active Directory) 및 도메인 서비스 보안 로그		
카테고리	**하위 카테고리**	**이벤트 ID**
계정 관리	계정 비밀번호 재설정	4724
	도메인 정책 - 변경[61]	4739
보안 지원 글로벌 그룹	회원 - 추가됨	4728
	구성원 - 제거됨	4729
	그룹 - 변경	4737
보안이 설정된 로컬 그룹	구성원 - 추가됨	4732
	구성원 - 제거됨	4733
	그룹 - 변경	4735
보안이 활성화된 유니버설 그룹	그룹 - 변경	4755
	구성원 - 추가됨	4756
	구성원 - 제거됨	4757
SID 기록	계정 추가 - 성공	4765
	계정 추가 - 실패	4766
Kerberos	Kerberos 정책이 변경되었습니다.	4713
	TGT 인증 티켓 요청	**4768**[62]
	서비스 티켓 요청	**4769**[63]
	사전 인증 실패	**4771**[64]
	서비스 티켓 거부됨	4821
	DES 또는 RC4를 사용한 사전 인증 실패	4824
사용자 계정 관리	ACL 설정 - 관리자 그룹	4780
	디렉터리 서비스 복원 모드 - 관리자 암호	4794
NTLM 인증[65]	실패	4822
OCSP 응답자 서비스	보안 설정 업데이트	5124
디렉터리 복제 에이전트(DRA)	사이트 간 복제	1102
디렉터리 서비스 개체	디렉터리 서비스 객체 - 수정됨	**5136**[66]
	디렉터리 서비스 객체 - 생성	5137
	디렉터리 서비스 개체 - 삭제됨	5141

61 자세한 내용은 WELF를 참조하십시오.
62 자세한 내용은 DMADC 표 6, 표 10, 표 14를 참조하십시오.
63 자세한 내용은 DMADC 표 1, 표 10을 참조하세요.
64 자세한 내용은 DMADC 표 3을 참조하세요.
65 자세한 내용은 WELF를 참조하십시오.
66 자세한 내용은 DMADC 표 1, 표 15를 참조하십시오.

AD(Active Directory) 및 도메인 서비스 보안 로그		
카테고리	**하위 카테고리**	**이벤트 ID**
사용자 계정[67]	사용자 계정 - 비활성화됨	4725
	사용자 계정 - 삭제됨	4726
	사용자 계정 - 변경됨[68]	**4738**[69]
	자격 증명 유효성 검사 시도	4776
인증서 서비스	서비스 실패	**39**[70]
	서비스가 시작되지 않음	**40**[71]
	호환되지 않는 SID	**41**[72]
	인증서 내보내기	**70**[73]
	CA 데이터베이스 백업	**4876**[74]
	인증서 요청	**4886**[75]
	인증서 발급	**4887**[76]
세라믹	템플릿 업데이트	**4899**[77]
	템플릿 보안 업데이트	**4900**[78]

5. Microsoft Windows 엔드포인트 로그

다음 이벤트 ID와 관련된 그룹 정책 변경 사항은 이 문서 끝에 있는 추가 참고자료를 참조하세요.

Microsoft Windows 엔드포인트 로그		
카테고리	**하위 카테고리**	**이벤트 ID**
Windows 애플리케이션 이벤트 로그	프로세스 생성	1 (**시스몬**[79])
	충돌(오류 메시지 포함)	1001
Windows 작업 스케줄러 이벤트 로그[80]	컴퓨터 시작 시 트리거되는 작업	118
	로그온 시 트리거되는 작업	119
	생성된 작업 프로세스	129
	작업 시작	200

67 자세한 내용은 WELF를 참조하세요.
68 자세한 내용은 HMWW를 참조하세요.
69 자세한 내용은 DMADC 표 1, 표 15를 참조하세요.
70 자세한 내용은 DMADC 표 6을 참조하세요. 자세한 내용은 DMADC 표 6을 참조하세요.
71 자세한 내용은 DMADC 표 6을 참조하세요.
72 자세한 내용은 DMADC 표 6을 참조하세요.
73 자세한 내용은 DMADC 표 7을 참조하세요.
74 자세한 내용은 DMADC 표 7을 참조하세요.
75 자세한 내용은 DMADC 표 6을 참조하세요.
76 자세한 내용은 DMADC 표 6을 참조하세요.
77 자세한 내용은 DMADC 표 6을 참조하세요.
78 자세한 내용은 DMADC 표 6을 참조하세요.
79 자세한 내용은 WELF를 참조하세요.
80 자세한 내용은 WELF를 참조하세요.

Microsoft Windows 엔드포인트 로그		
카테고리	**하위 카테고리**	**이벤트 ID**
윈도우 PowerShell 이벤트 로그[81]	모듈 이벤트	**4103**[82]
	스크립트 차단 이벤트	**4104**[83]
	엔진 수명 주기	400
Windows WMI 활동/운영 이벤트 로그[84]	ESS 시작	5859
	임시 ESS 시작	5860
	ESS 대 소비자 구속력	5861
	작업 시작	5857
	클라이언트 장애	5858
Windows 보안 이벤트 로그	감사 로그 지워짐	**1102**[85] [86]
	LSA(로컬 보안 권한) - 인증 패키지가 로드됨	4610
	LSA - 신뢰할 수 있는 로그온 프로세스 등록	4611
	보안 계정 관리자 - 알림 패키지 로드됨	4614
	LSA - 보안 패키지 로드됨	4622
	계정 로그온(87) - 성공	**4624**[88]
	계정 로그온(89) - 실패	**4625**[90]
	계정 로그온 - 명시적 자격 증명	4648
	개체 핸들 - 요청	**4656**[91]
	개체 액세스 - 실패	**4663**[92]
	특별 권한 - 새 로그온	**4672**[93]
	새 프로세스 - 생성됨	4688
	서비스 - 설치됨	**4697**[94], 7045
	예약된 작업 - 생성됨[95]	4698
	예약된 작업 - 업데이트됨[96]	4702

81 자세한 내용은 WELF를 참조하세요.
82 자세한 내용은 DMADC 표 5, 표 7, 표 8, 표 13, 표 14, 표 15, 표 16을 참조하세요.
83 자세한 내용은 DMADC 표 5, 표 7, 표 8, 표 13, 표 14, 표 15, 표 16을 참조하세요.
84 자세한 내용은 WELF를 참조하세요.
85 자세한 내용은 DMADC 표 6, 표 7, 표 8, 표 12, 표 13, 표 14, 표 15, 표 16을 참조하세요.
86 PRC state-sponsored actors compromise and maintain persistent access to U.S. critical infrastructure | Cyber.gov.au
87 자세한 내용은 WELF를 참조하세요.
88 자세한 내용은 DMADC 표 3, 표 4, 표 5, 표 11을 참조하세요.
89 자세한 내용은 WELF를 참조하세요.
90 자세한 내용은 DMADC 표 3, 표 4, 표 5, 표 11을 참조하세요.
91 자세한 내용은 DMADC 표 8을 참조하세요.
92 자세한 내용은 DMADC 표 8, 표 16을 참조하세요.
93 자세한 내용은 DMADC 표 8, 표 16을 참조하십시오.
94 자세한 내용은 DMADC 표 16을 참조하세요.
95 자세한 내용은 WELF를 참조하세요.
96 자세한 내용은 WELF를 참조하세요.

Microsoft Windows 엔드포인트 로그		
카테고리	**하위 카테고리**	**이벤트 ID**
Windows 보안 이벤트 로그	시스템 보안 액세스 - 허용됨	4717
	시스템 보안 액세스 - 삭제됨	4718
	시스템 감사 정책 - 변경됨	4719
	사용자 계정 - 생성됨	**4720**[97]
	사용자 계정 - 사용	**4722**[98]
	계정 비밀번호 변경(실패)	4723
	구성원 - 추가됨(보안이 설정된 로컬 그룹)	4732
	Kerberos Ticket-granting-ticket (TGT) 거부됨	4820
	새 로그온이 할당된 특수 그룹	4964
	개체 핸들 닫힘	4658
	프로세스 종료	4689
	예약된 작업 - 삭제됨[99]	4699
	예약된 작업 - 비활성화됨[100]	4701
AppLocker	정책이 잘못 적용됨	8000
	장애인	8008
	정책 변경/적용	8001
	모드 변경(시행에서 감사로)	
	EXE 또는 DLL 차단됨	8004
	스크립트 또는 Microsoft 소프트웨어 설치 관리자(MSI) 차단됨	8007
	파일을 실행할 수 없습니다.	8022, 8025
	패키지 앱 규칙 부족으로 인한 패키지 앱 실패	8027
	구성 CI 정책으로 인해 파일 또는 패키지가 실행 중	8029, 8036, 8040
	ManagedInstaller 스크립트 확인 성공/실패	8032, 8035
Windows 시스템 로그	청소된 처리	1017

97 자세한 내용은 DMADC 표 8, 표 16을 참조하십시오.
98 자세한 내용은 DMADC 표 8, 표 16을 참조하십시오.
99 자세한 내용은 WELF를 참조하세요.
100 자세한 내용은 WELF를 참조하세요.

Microsoft Windows 엔드포인트 로그		
카테고리	**하위 카테고리**	**이벤트 ID**
Windows ESENT (확장 가능 스토리지 엔진 기술) 애플리케이션	데이터베이스 위치 변경	**216**[101]
	새 데이터베이스	325
	NTDS.dit 파일 마운트	326
	데이터베이스 분리	327
	새로운 플러시 맵 파일	**637**[102]
Windows 터미널 서비스 로컬 세션 관리자	새로운 로컬 세션	21
	셸 시작 알림 수신	22
	세션 로그오프 성공	23
	세션 연결 끊기	24
	세션 다시 연결	25
Windows Defender 응용 프로그램 제어	파일이 차단되었습니다.	3077
	서명	3089

6. 가상화 시스템 로그

가상화 시스템 로그		
카테고리	**하위 카테고리**	**이벤트**
사용자 인증	로그온(성공 및 실패)	전체 대상
	권한 있는 액세스(성공 및 실패)	전체 대상
사용자 및 관리자/루트 액세스 및 작업	파일 및 개체 액세스	전체 대상
	감사 로그 액세스(성공 및 실패)	전체 대상
	시스템 액세스(실패)	전체 대상
시스템 성능 및 운영 특성	리소스 활용	전체 대상
	프로세스 상태	
	시스템 이벤트	전체 대상
	서비스 상태 변경	전체 대상
시스렘 구성	보안 구성 변경(성공/실패)	전체 대상
	하이퍼바이저 변경 사항	전체 대상
	VMS 변경 사항	전체 대상
	VMS 내 변경 사항	전체 대상
	감사 로그 지워짐	전체 대상

101 자세한 내용은 중국의 국가 지원 행위자들이 미국의 중요 인프라를 손상시키고 지속적인 접근을 유지하다를 .참조하세요

102 자세한 내용은 공동 지침을 참조하세요: 자취 생활 기법 식별 및 완화하기

가상화 시스템 로그		
카테고리	**하위 카테고리**	**이벤트**
VMS 생성	출처	전체 대상
	대상 시스템	전체 대상
	시간	전체 대상
	권한 부여	전체 대상
VMS 배포	출처	전체 대상
	대상 시스템	전체 대상
	시간	전체 대상
	권한 부여	전체 대상
VMS 마이그레이션	출처	전체 대상
	대상 시스템	전체 대상
	시간	전체 대상
	권한 부여	전체 대상
시스템 수준 개체	생성 및 삭제	전체 대상

7. 운영 기술 로깅

운영 기술(OT) 로깅을 SIEM에 통합하는 것은 종종 공급업체에 따라 다르고 일반적으로 SIEM이 위치한 환경과 분리되어 있는 OT 시스템의 특수한 특성으로 인해 어려울 수 있습니다. 또한 OT 디바이스에는 제한된 로깅이 제공되는 경우가 많습니다. 가능하면 OT 디바이스에서 로깅을 활성화한 다음 중앙 집중식 위치에 로그를 전송하고 저장하는 것이 좋습니다. OT 환경에 특화된 전용 SIEM을 구현하는 것이 가능할 수도 있지만, 직원들이 두 시스템과 이벤트 유형에 익숙해져야 합니다.

산업 제어 시스템(ICS) 모니터링은 SIEM으로 전달하거나 중앙 리포지토리에 저장하기 전에 OT 데이터를 안전하게 수집, 해석, 보강할 수 있는 솔루션을 제공합니다. 또한 이러한 제품은 OT 네트워크와 자산을 모니터링하고, OT 네이티브 프로토콜을 구문 분석하며, SIEM으로 전송되는 이벤트에 필요한 세부 정보와 상황별 메타데이터가 포함된 추가 로그를 생성할 수 있습니다.

보안이 다른 요구 사항보다 우선하는 경우, 조직은 단방향 게이트웨이 또는 데이터 다이오드를 구현하여 OT 환경의 로그 데이터를 외부 위협에 노출시키지 않고 IT SIEM으로 안전하게 전송할 수 있습니다.

OT 시스템으로부터 직접 로그를 수집하는 경우, 안전에 민감한 위험요소와 메시징의 고속성 및 결정적 통신 특성을 고려하여, 보수적인 접근 방식이 요구됩니다. 운영에 영향을 주지 않도록 모든 로깅 솔루션은 실제 배포 전에 철저한 테스트를 수행해야 합니다.

8. 클라우드 플랫폼 로깅[103], [104]

클라우드 서비스는 기본적으로 사용 설정되어 있지 않을 수 있습니다. 애플리케이션마다 고유한 로깅 형식이 있거나 로깅이 전혀 없을 수도 있습니다. 아래 권장 사항은 로깅할 수 있는 항목의 예시일 뿐이므로 조직의 보안 요구사항과 위험 프로필에 맞는 보안 로깅에 대해서는 클라우드 서비스 제공업체 및 클라우드 애플리케이션 제공업체에 조언을 구해야 합니다.

이에 대한 자세한 내용은 Best practices for event logging and threat detection 를 참조하세요.

클라우드 컴퓨팅의 로깅 우선 순위

작성 기관은 조직이 서비스형 인프라(IaaS), 서비스형 플랫폼(PaaS), 서비스형 소프트웨어(SaaS) 등 구현되는 클라우드 서비스에 따라 이벤트 로깅 관행을 조정할 것을 권장합니다. 예를 들어, IaaS는 테넌트에게 로깅 책임이 있는 반면, SaaS는 제공업체에게 로깅 책임이 있습니다. 따라서 조직은 로깅 우선순위에 영향을 미칠 수 있으므로 클라우드 서비스 제공업체와 긴밀히 협력하여 현재 시행 중인 공유 책임 모델을 이해해야 합니다. 로깅 우선순위는 다음에도 영향을 받을 수 있습니다.

다양한 클라우드 컴퓨팅 서비스 모델과 배포 모델(퍼블릭, 프라이빗, 하이브리드, 커뮤니티)에 따라 달라집니다. 개인정보 보호법 및 데이터 주권법이 적용되는 경우 로깅 우선 순위는 클라우드 서비스 제공업체의 인프라 위치에 따라 영향을 받을 수도 있습니다.

자세한 내용은 국가안보국의 효과적인 위협 헌팅을 위한 클라우드 로그 관리[105]지침을 참조하세요.

조직은 클라우드 컴퓨팅 서비스를 사용할 때 다음 로그 소스의 우선순위를 정해야 합니다:

- 표적이 될 가능성이 있는 중요 시스템 및 데이터 보유량
- 인터넷 연결 서비스(원격 액세스 포함) 및 해당되는 경우 기본 서버 운영 체제
- 클라우드 서비스에 액세스하고 관리하는 테넌트의 사용자 계정 사용
- 관리 구성 변경에 대한 로그
- 설정을 포함한 모든 보안 주체의 생성, 삭제 및 수정에 대한 로그를 기록
- 권한 변경
- 타사 서비스에 대한 인증 성공 및/또는 실패(예: 보안 어설션 마크업 언어(SAML)/오픈 권한 부여(OAuth))
- 클라우드 API(애플리케이션 프로그래밍 인터페이스) 로그, 모든 네트워크 관련 이벤트, 규정 준수 이벤트 및 청구 이벤트 등 클라우드 서비스에서 생성된 로그를 포함

103 자세한 내용은 CCSCSP를 참조하세요.
104 자세한 내용은 CCST를 참조하세요.
105 https://media.defense.gov/2024/Mar/07/2003407864/-1/-1/0/CSI_CloudTop10-Logs-for-Effective-Threat-Hunting.PDF

아마존 웹 서비스 로그

아마존 웹 서비스 로그		
카테고리	**하위 카테고리**	**이벤트**
아마존 웹 서비스	CloudTrail 로그	전체 대상
	서버 액세스 로그	전체 대상
	S3 버킷에 대한 웹 액세스	전체 대상
	로드 밸런서 로그	전체 대상
	프록시 웹 요청	전체 대상
	Breakglass 계정 사용	전체 대상
	VPC 네트워크 흐름 로그	전체 대상
비밀 관리자	ListSecrets	전체 대상
	GetSecretValue	전체 대상
S3	ListBuckets	오류 내역만 해당
	목록 개체	오류 내역만 해당
	GetObject	오류 내역만 해당
	CopyObject	오류 내역만 해당
	GetObjectAcl	전체 대상
	HeadBucket	전체 대상
	헤드 오브젝트	전체 대상
	PutPublicAccessBlock	전체 대상
EC2	CreateKeyPair	전체 대상
	ImportKeyPair	전체 대상
	스냅샷 생성	전체 대상
	Run 인스턴스	전체 대상
	보안 그룹 설명	전체 대상
	보안 그룹 규칙 수정	전체 대상
	비밀번호 데이터 가져오기	전체 대상
	콘솔 스크린샷 가져오기	전체 대상
	설명 인스턴스 데이터	속성='사용자 데이터' 항목만 해당
VPC	CreateNatGateway	전체 대상
	인터넷 게이트웨이 연결	전체 대상
	인터넷 게이트웨이 생성	전체 대상
	CreateEgressOnlyInternetGateway	전체 대상
	CreateVpc피어링 연결	전체 대상
	수락Vpc피어링 연결	전체 대상

아마존 웹 서비스 로그		
카테고리	**하위 카테고리**	**이벤트**
EBS 다이렉트 API	스냅샷 차단	전체 대상
IAM	계정 승인 세부 정보 가져오기	전체 대상
	ListUsers	전체 대상
	사용자 만들기	전체 대상
	CreateOpenIDConnectProvider	전체 대상
STS	발신자 신원 확인	전체 대상
SSM	설명 매개변수	오류 내역만 해당
	GetParameter	오류 내역만 해당
RDS	DB 인스턴스 설명	전체 대상
	디비클러스터 설명	전체 대상
DynamoDB	쿼리	오류 내역만 해당
	스캔	오류 내역만 해당
	목록 테이블	전체 대상
	테이블 설명	오류 내역만 해당
Lambda	GetFunction	전체 대상

중요한 Azure 서비스 및 앱 로그

중요한 Azure 서비스 및 앱 로그		
카테고리	**하위 카테고리**	**이벤트**
엔트라 & *엔트라 커넥트 서버*[106]	통합 감사 로그	전체 대상
	PHS 실패	**611**[107]
	AD 암호 동기화 - 시작	**650**[108]
	AD 비밀번호 동기화 - 완료	**651**[109]
	비밀번호 동기화	**656**[110]
	비밀번호 변경 요청	**657**[111]
	감사 로그 지워짐	**1102**[112]
	PowerShell - 파이프라인 실행 및 로그	**4103**[113]
	PowerShell - 스크립트 및 명령	**4104**[114]

106 자세한 내용은 DMADC 표 13을 참조하세요.
107 자세한 내용은 DMADC 표 13을 참조하세요.
108 자세한 내용은 DMADC 표 13을 참조하세요.
109 자세한 내용은 DMADC 표 13을 참조하세요.
110 자세한 내용은 DMADC 표 13을 참조하세요.
111 자세한 내용은 DMADC 표 13을 참조하세요.
112 자세한 내용은 DMADC 표 13을 참조하세요.
113 자세한 내용은 DMADC 표 13을 참조하세요.
114 자세한 내용은 DMADC 표 13을 참조하세요.

중요한 Azure 서비스 및 앱 로그		
카테고리	**하위 카테고리**	**이벤트**
엔트라 & *엔트라 커넥트 서버*[106]	로그인 로그	전체 대상
	관리되는 ID 로그인 로그	전체 대상
	비대화형 사용자 로그인 로그	전체 대상
	서비스 담당자 로그인 로그	전체 대상
	ADFS 로그인 로그	전체 대상
Azure 감사 로그	읽기 및 쓰기	전체 대상
Azure 스토리지 컨테이너 로그	읽기 및 쓰기	전체 대상
Breakglass 계정 사용	모든	전체 대상
마이크로소프트 오피스 365	통합 감사 로그	전체 대상
가상 머신	Linux 운영 체제 로그(VM에 구성된 OS)	전체 대상
	Windows 운영 체제 로그(VM에 구성된 OS)	전체 대상

Google 클라우드 플랫폼(GCP) 로그

Google 클라우드 플랫폼(GCP) 로그		
카테고리	**하위 카테고리**	**이벤트**
Google 클라우드 플랫폼	투명성 로그에 액세스	전체 대상
	관리자 활동 로그	전체 대상
	엔터프라이즈 그룹 감사 로그	전체 대상
	로그인 감사 로그	전체 대상
	시스템 이벤트 로그	전체 대상
	정책 거부 감사 로그	전체 대상
	스토리지 버킷 로그	전체 대상
	호스트 VM 로그	전체 대상
	플랫폼 감사 로그	전체 대상
	브레이크글래스 계정 사용	전체 대상
	VPC 방화벽 로그	전체 대상
	VPC 네트워크 흐름 로그	전체 대상

Google 워크스페이스(GWS) 로그

Google 워크스페이스(GWS) 로깅		
카테고리	**하위 카테고리**	**이벤트**
Google 워크스페이스	투명성 로그에 액세스	전체 대상
	관리자 활동 로그	전체 대상
	컨텍스트 인식 액세스	전체 대상
	디바이스 이벤트	전체 대상
	디렉터리 동기화 이벤트	전체 대상
	OAuth 이벤트	전체 대상
	비밀번호 보관 앱 이벤트	전체 대상
	규칙 이벤트	전체 대상
	SAML 이벤트	전체 대상
	보안 LDAP 이벤트	전체 대상
	사용자 감사 이벤트	전체 대상
	Chrome 이벤트	전체 대상
	드라이브 이벤트	전체 대상
	Gmail 이벤트	전체 대상
	졸업 이벤트	전체 대상
	테이크아웃 이벤트	전체 대상

9. 컨테이너 로그

컨테이너 로그		
카테고리	**하위 카테고리**	**이벤트**
컨테이너 사용자 로그	로그온(성공 및 실패)	전체 대상
	권한 있는 액세스(성공 및 실패)	전체 대상
컨테이너 서비스 로그	감사 로그 변경 사항	전체 대상
	감사 로그 지워짐	전체 대상
컨테이너 및 애플리케이션 API 감사 로그	파일 및 개체 액세스	전체 대상
	로그 액세스 감사(성공 및 실패)	전체 대상
	시스템 액세스(실패)	전체 대상
컨테이너 관리 액세스 로그	로그온(성공 및 실패)	전체 대상
	컨테이너 RBAC 변경 사항	전체 대상
	서비스 상태 변경	전체 대상

컨테이너 로그		
카테고리	**하위 카테고리**	**이벤트**
컨테이너 리소스	보안 구성 변경	전체 대상
	컨테이너 변경 사항	전체 대상
	감사 로그 변경 사항	전체 대상
	감사 로그 지워짐	전체 대상
컨테이너 관리 환경	로그온(성공 및 실패)	전체 대상
	권한 있는 액세스(성공 및 실패)	전체 대상

10. 데이터베이스 로그

데이터베이스 로그		
카테고리	**하위 카테고리**	**이벤트**
사용자 인증	로그온(성공 및 실패)	전체 대상
	권한 있는 액세스(성공 및 실패)	전체 대상
	사용자 역할(변경 사항)	전체 대상
사용자 및 관리자 액세스 및 작업	테이블 및 개체 액세스	전체 대상
	신규 사용자/권한 있는 사용자	전체 대상
	권한 승격(성공 및 실패)	전체 대상
	로그 액세스 감사(성공 및 실패)	전체 대상
	실행 명령	전체 대상
	비밀번호	전체 대상
	데이터베이스 권한	전체 대상
	CLI 명령	전체 대상
쿼리, 응답 및 트레이스백 특성	쿼리 실행	전체 대상
	방법	전체 대상
	주석 또는 변수	전체 대상
	여러 임베디드 쿼리	전체 대상
	알림 또는 실패	전체 대상
	쿼리 실행 시간	전체 대상
시스템 구성	데이터베이스 구조 변경	전체 대상
	버전 업데이트/롤백	전체 대상
	키(액세스 포함)	전체 대상
	사용자 역할 또는 데이터베이스 권한 변경	전체 대상

11. 모바일 디바이스 관리

모바일 디바이스 관리		
카테고리	**하위 카테고리**	**이벤트**
디바이스 데이터	장치 이름 변경	전체 대상
	전화번호 변경	전체 대상
	OS 버전 변경	전체 대상
	펌웨어 버전 변경	전체 대상
	개발자 모드 사용	전체 대상
	엔터프라이즈와 동기화된 디바이스	전체 대상
애플리케이션 데이터	애플리케이션 설치	전체 대상
	애플리케이션 업데이트	전체 대상
	제거한 애플리케이션	전체 대상
	데이터 저장 위치	전체 대상
	애플리케이션 권한 변경	전체 대상
디바이스 정책 설정	등록 정책(변경 사항)	전체 대상
	적용된 정책(성공/실패)	전체 대상
	인증 정책 변경	전체 대상
장치 구성	인증서 변경	전체 대상
	장치 암호화 구성 변경	전체 대상
	Android Enterprise 설정 변경 사항	전체 대상
	시스템 무결성 상태(장애)	전체 대상
네트워크 구성	네트워크(허용/불허)	전체 대상
	프록시/터널	전체 대상
	앱별 VPN 세부 정보	전체 대상
	연결된 네트워크	전체 대상
	캡티브 포털 연결	전체 대상
	네트워크 MAC 주소	전체 대상
	블루투스 연결	전체 대상
	Wi-Fi SSID 연결	전체 대상
이벤트/감사/크래시 로그	이벤트 타임스탬프	전체 대상
	이벤트 유형	전체 대상
	사용자 인증(성공/실패)	전체 대상
	다양한 서비스(성공/실패)	전체 대상
	이벤트 Actor	전체 대상
	이벤트 ID	전체 대상
	이벤트 변경 유형(CRUD)	전체 대상

모바일 디바이스 관리		
카테고리	**하위 카테고리**	**이벤트**
MTD 에이전트 정보	상담원 상태	전체 대상
	상담원 구성 변경 사항	전체 대상
	위협 탐지	전체 대상
	MITM 활동	전체 대상
	해결 조치	전체 대상
	권한 에스컬레이션	전체 대상
	피싱 보호 상태	전체 대상
	마지막으로 디바이스가 엔터프라이즈와 동기화된 시간	전체 대상

12. Windows DNS 서버 분석 이벤트 로그

Windows DNS 서버 분석 이벤트 로그		
카테고리	**하위 카테고리**	**이벤트 ID**
DNS 서버 분석	응답 성공	257
	응답 실패	258
	무시된 쿼리	259
	쿼리 아웃	260
	응답	261
	재귀 쿼리 시간 초과	262
	에서 업데이트	263
	응답 업데이트	264
	앞으로 업데이트	277
	응답 업데이트	278
DNS 서버 영역 이전	DNS 서버 영역 전송이 성공적으로 완료되었습니다.	6001

13. Linux 엔드포인트 감사 로그

Linux 엔드포인트 감사 로그		
카테고리	**하위 카테고리**	**이벤트**
감사	구성	수정
	로그 파일	수정

Linux 엔드포인트 감사 로그		
카테고리	**하위 카테고리**	**이벤트**
감사 도구	구성	수정 내역만 해당
	읽기	액세스 내역만 해당
	모니터링	액세스 내역만 해당
사용자 액세스	민감한 디렉토리 및 바이너리(예: /sbin)	전체 대상
	인증 메커니즘(예: SSH).	수정 내역만 해당
	인증/승인 구성 변경	전체 대상
	로그인 및 로그아웃 이벤트(/var/log/wtmp).	전체 대상
	세션 녹화	수정 내역만 해당
	사용자(+연결), 그룹(+연결) 및 비밀번호	수정 내역만 해당
	SSH 세션 시작	전체 대상
권한 있는 이벤트	권한 있는 시스템 호출	전체 대상
	Sudo/Root 권한	수정 내역만 해당
	로그인 정보	수정 내역만 해당
	민감한 액세스 제어 수준(예: chmod >= 500)	수정 내역만 해당
	공개/개인 키 위치(.ssh 디렉터리)	전체 대상
	셸 기록	수정 내역만 해당
	auditctl을 사용하여 /etc/passwd	전체 대상
	모든 권한 있는 기능에 대한 감사	전체 대상
시스템 이벤트	신뢰할 수 있는 데이터베이스(예: /etc/passwd).	수정 내역만 해당
	프로세스 ID	수정 내역만 해당
	시스템 파일 삭제	전체 대상
	드라이브 및 파일 마운트 작업	전체 대상
	시작 스크립트 및 변경 사항	수정 내역만 해당
	검색 경로	수정 내역만 해당
	특수 파일(예: 첨부된 블록 장치)	전체 대상
	마운트 작업	전체 대상
	스왑 작업	전체 대상
	표준 커널 매개변수	전체 대상
	모듈 로드 및 언로드	전체 대상
	패키지(소스 포함) 설치 제거 재구성	전체 대상

Linux 엔드포인트 감사 로그		
카테고리	**하위 카테고리**	**이벤트**
시스템 이벤트	부팅 매개변수 수정	전체 대상
	마운트 옵션 수정	전체 대상
	SSSD 로그 파일	전체 대상
	KEXEC 사용법	전체 대상
	Cron 구성 및 로그(/etc/cron 및 /.var/log/cron).	수정 내역만 해당
	서비스 및 시스템 구성	수정 내역만 해당
파일 이벤트	무단 파일 액세스 시도가 실패한 경우	전체 대상
보안 이벤트	일반적인 정찰 도구(예: 넷캣)	전체 대상
	의심스러운 바이너리(예: 코드/데이터/프로세스 인젝션)	전체 대상
네트워크 이벤트	호스트 이름 변경 및 연결 등	전체 대상

14. Apple MacOS 엔드포인트 로그

Apple MacOS 엔드포인트 로그		
카테고리	**하위 카테고리**	**이벤트**
콘텐츠 캐싱	com.apple.AssetCache(하위 시스템)	전체 대상/기본값
게이트키퍼	시스폴리드(정책)	전체 대상/기본값
	com.apple.syspolicy.exec(하위 시스템)	전체 대상/기본값
macOS 설치 관리자 및 소프트웨어 업데이트	소프트웨어 업데이트(정책)	전체 대상/기본값
	com.apple.mac.install(하위 시스템)	전체 대상/기본값
	com.apple.SoftwareUpdate(하위 시스템)	전체 대상/기본값
	com.apple.SoftwareUpdateMacController(하위 시스템)	전체 대상/기본값
	com.apple.mobileassetd(하위 시스템)	전체 대상/기본값
모바일 디바이스 관리(MDM)	Mdmclient(정책)또는	전체 대상
	com.apple.ManagedClient(하위 시스템)	전체 대상
네트워킹	com.apple.network(하위 시스템)	전체 대상
	연결(카테고리)	전체 대상
	보링슬 (카테고리)	전체 대상
OCSP(인증서 밸리디리)	com.apple.securityd(하위 시스템)	전체 대상
	OCSP(카테고리)	전체 대상

Apple MacOS 엔드포인트 로그		
카테고리	**하위 카테고리**	**이벤트**
OS 구성 요소 및 애플리케이션에 대한 사용자 및 관리자 액세스	파일 및 개체 액세스	전체 대상
	로그 액세스 감사	성공/실패
	시스템 액세스 및 로그오프	성공/실패
	권한 액세스 및 로그오프	성공/실패
	민감한 권한 사용(sudo)	성공/실패
	원격 터미널 또는 이에 상응하는 액세스 및 로그 꺼짐	성공/실패
	Samba/NFS/(S)FTP 또는 이에 상응하는 액세스	전체 대상
	Mac OS X utmpx / wmtp	전체 대상
	감사 데몬	전체 대상
	권한/접근 위반	전체 대상
	터미널 명령 세션	전체 대상
	SSH 세션 시작	전체 대상
	디렉터리 열기	
	터미널 명령 기록	전체 대상
	애플리케이션 설치 또는 제거	전체 대상
	스토리지 볼륨 또는 이동식 미디어의 설치 또는 제거	전체 대상
시스템 성능 및 운영 특성	리소스 사용률, 프로세스 상태	전체 대상
	시스템 이벤트	전체 대상
	서비스 상태 변경	시작, 중지, 실패, 다시 시작 등 상태만
	서비스 장애 및 재시작	전체 대상
	서비스 데몬 실행	전체 대상
	Jamf	전체 대상
	프로세스 생성 및 종료	전체 대상
시스렘 구성	보안 구성 변경	성공/실패
	감사 로그 지워짐	전체 대상
	계정 변경	전체 대상
	사용자 또는 그룹 관리 변경 사항	전체 대상
	Apple 푸시 알림 서비스(APN)	전체 대상
	스냅샷 DB	성공/실패
	Syslog 형식 파일	전체 대상
	예약된 작업 변경	전체 대상

Apple MacOS 엔드포인트 로그		
카테고리	**하위 카테고리**	**이벤트**
파일 액세스	외부 미디어로 전송	전체 대상
	원격 호스트로 전송	전체 대상
파일 공유	ALL	전체 대상
호스트 네트워크 통신	포트	전체 대상
	IP 주소	전체 대상
	활성 네트워크 통신	전체 대상
명령줄 인터페이스(CLI)	시스템 로그 폴더: /Var/Log/*	전체 대상
	시스템 로그: /Var/Log/System.Log	전체 대상
	Mac 분석 데이터: /Var/Log/ 진단 메시지: /*	전체 대상
	Wi-Fi 로그: /Var/Log/Wifi.Log	전체 대상
	시스템 애플리케이션 로그: /Library/Logs/* 및 /Private/Var/Log/*	전체 대상
	시스템 보고서: /Library/Logs/ 진단 보고서/ *	전체 대상
	사용자 애플리케이션 로그: /Users/Name/Library/Logs/*	전체 대상
	사용자 보고서: /Users/Name/Library/Logs/Diagnosticreports/*	전체 대상
	감사 로그: /Var/Audit/*	전체 대상
BIOS(기본 입력 출력 시스템), UEFI(통합확장 펌웨어 인터페이스) 및 기타 펌웨어	버전	전체 대상
	생성된 날짜	전체 대상
	설치 날짜	전체 대상
	제조업체	전체 대상
키체인 이벤트	공개/개인 키 위치(.ssh 디렉터리)	전체 대상
XProtect	탐지 이벤트 및 알림	전체 대상
기타 로그	필요에 따라 또는 위험을 통해 결정 / 평가	전체 대상

참조 부록

액티브 디렉터리 그룹 정책 변경

다음 표는 특정 이벤트 ID를 로그 소스에서 생성하는 데 필요한 그룹 정책 변경 사항을 정리한 것입니다.

이벤트 ID	그룹 정책 개체
4618	시스템 무결성 감사
4649	기타 로그온/로그오프 이벤트 감사
4964	특별 로그온 감사
4662	디렉터리 서비스 액세스 감사
4670	기타 정책 변경 이벤트 감사
4897	감사 인증 서비스
4673	민감한 권한 사용 감사
4694	DPAPI 활동 감사
4703, 4704, 4705, 4706, 4707	감사 권한 정책 변경
4724, 4739	감사 계정 관리
4728, 4729, 4732, 4733, 4735, 4737, 4755, 4756, 4757	보안 그룹 관리 감사
4765 4766	사용자 계정 관리 감사
4713	감사 인증 정책 변경
4768	Kerberos 인증 서비스 감사
4769	Kerberos 서비스 티켓 운영 감사
4771	Kerberos 사전 인증에 실패했습니다.
4821	Kerberos 서비스 티켓 운영 감사
4780, 4794, 4725, 4726, 4738	사용자 계정 관리 감사
5141	디렉터리 서비스 변경 사항 감사
5124	보호된 사용자
5136	OCSP 응답자 서비스
70	그룹 정책 설정과 직접 관련이 없음
4876, 4886, 4887	감사 인증 서비스
39, 40, 41, 4776, 4824, 4899 4900, 5137	Windows 기본값

Windows 엔드포인트 그룹 정책 변경

다음 표는 특정 이벤트 ID를 로그 소스에서 생성하는 데 필요한 그룹 정책 변경 사항을 정리한 것입니다.

이벤트 ID	그룹 정책 개체
4103	모듈 로깅 켜기
4104	PowerShell 스크립트 블록 로깅 사용
4610, 4611, 4614, 4622	보안 시스템 확장 감사
4624, 4625, 4648	로그온 이벤트 감사
4656, 4663	개체 액세스 감사
4688	감사 프로세스 생성
4697	보안 시스템 확장 감사
4698, 4699, 4701, 4702	기타 개체 액세스 이벤트 감사
4717, 4718, 4719	감사 인증 정책 변경
4720, 4722, 4723	사용자 계정 관리 그룹 정책 감사
4732	보안 그룹 관리 감사
4820	디바이스 기반 액세스 제어 정책
4964	특별 로그온 감사
4658	Handle 조작 감사
4689	감사 프로세스 종료
8000, 8004	NTLM 감사 설정
8007, 8022, 8025, 8027, 8029, 8032, 8036, 8040, 8035	AppLocker 정책
3077, 3089	Windows Defender 응용 프로그램 제어
1, 118, 119, 129, 200, 1001, 1102, 5857, 5858, 5859, 5860, 5861, 7045	Windows 기본값

도메인 컨트롤러 그룹 정책 변경

다음 표는 특정 이벤트 ID를 로그 소스에서 생성하는 데 필요한 그룹 정책 변경 사항을 정리한 것입니다.

이벤트 ID	그룹 정책 개체
4768, 4769	Kerberos 인증 서비스 감사
4741, 4742, 4743	컴퓨터 계정 관리 감사
4739	모든 보안 설정 / 계정 정책 GPO
4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, 4754, 4755, 4756, 4757, 4758, 4764, 4928, 4929	상세 디렉토리 서비스 복제 감사
4675, 4720, 4722	감사 로그온
4723, 4724, 4725, 4726, 4738, 4767, 4780, 4781, 4794, 5376, 5377	사용자 계정 관리 감사
4876, 4886, 4887	감사 인증 서비스
4688, 4696	감사 프로세스 생성
4689	감사 프로세스 종료
4661, 4662	디렉터리 서비스 액세스 감사
5136, 5137, 5138, 5139, 5141	디렉터리 서비스 변경 사항 감사
8222	보안
307	관리 템플릿 / 프린터
4679	감사 정책
4770	Kerberos 서비스 티켓 운영 감사
2889	네트워크 보안: LDAP 클라이언트 서명 요구 사항
4634	감사 로그오프
4625, 4647	로그온 이벤트 감사
4624, 4634, 4648	고급 감사 정책 구성
4627	감사 그룹 멤버십
4779	기타 로그온/로그오프 이벤트 감사
4964	특별 로그온 감사
4672	새 로그온에 할당된 특별 권한
4663	개체 액세스 감사
4671, 4691, 4698, 4699, 4700, 4701, 4702, 5148, 5149, 5888, 5889, 5890	기타 개체 액세스 이벤트 감사
4673, 4674	민감한 권한 사용 감사
4985	파일 시스템 감사

이벤트 ID	그룹 정책 개체
4670, 4707, 4739, 4864	개체 액세스 감사
4706, 4707, 4713, 4717, 4718, 4865, 4866, 4867	감사 인증 정책 변경
4703	감사 권한 정책 변경
4719	감사 정책 변경
4960, 4961, 4962, 4963, 4965, 5478, 5479, 5480, 5483, 5484, 5485	IPsec 드라이버 감사
4608, 4616, 4621	보안 상태 변경 감사
4610, 4611, 4614, 4622, 4697	보안 시스템 확장 감사
4612, 4615, 4618, 5038, 5056, 5061, 6281, 6410	시스템 무결성 감사
5890	기타 개체 액세스 이벤트 감사
6410	코드 무결성
3033, 3063	코드 무결성 정책
39, 40, 41, 70, 510, 1007, 1102, 1200, 1202, 4678, 4695, 4740, 4776, 4899, 4900	Windows 기본값

면책 조항

이 가이드의 자료는 일반적인 성격의 것으로, 법적 조언으로 간주되거나 혹은 특정 상황이나 긴급 상황에서 의존해서는 안 됩니다. 중요한 사안에 대해서는 자신의 상황에 맞는 적절한 독립적인 보안전문가의 조언을 구해야 합니다.

호주 연방은 본 가이드에 포함된 정보에 의존한 결과로 발생한 어떠한 손해, 손실 또는 비용에 대해서도 책임을 지지 않습니다.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre