설정 상황

Secure Email Threat Defense 를 설정하는 데 Microsoft 365 전역 관리자 권한이 필요한 이유는 무엇입니까 ?

Cisco 는 Microsoft 365 자격 증명을 물리적으로 수락하지 않으며 전역 관리자의 자격 증명을 캐시하거나 저장하지도 않습니다 . Secure Email Threat Defense Microsoft 의 API 에 대한 인증 토큰을 발급할 수 있도록 Microsoft 의 Azure 애플리케이션 등록 프로세스로 리디렉션합니다 . 전역 관리자만 이 토큰에 권한을 부여할 수 있습니다 .

자세한 내용은 애플리케이션의 관리자 권한에 대한 Microsoft 설명서를 참조하십시오 .
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent/

Malware Analytics/Threat Grid 에서 환영 이메일을 받은 이유는 무엇입니까 ?

최소 Cisco Secure Malware Analytics(이전 명칭 Threat Grid) 계정은 Secure Email Threat Defense 계정 생성 프로세스의 일부로 생성됩니다 . 새 Malware Analytics 계정이 보유하고 있을 수 있는 기존 Malware Analytics 계정에 연결되지 않았습니다 . Secure Email Threat Defense 설정을 위해 Malware Analytics 계정에 대해 어떤 작업도 수행할 필요가 없습니다 .

저널 주소를 찾으려면 어떻게 해야 합니까 ?

Secure Email Threat Defense 설정 페이지에 저널 주소가 표시됩니다 . 초기 설정 후 이를 찾아야 하는 경우 , Account Details(어카운트 세부 정보) 섹션의 **Settings(설정)**(톱니바퀴 아이콘) > **Administration(관리)** > **Business(비즈니스)** 페이지에서 찾을 수 있습니다 .

Microsoft 365 테넌트를 등록하려고 할 때 등록 오류가 표시되는 이유는 무엇입니까 ?

이전에 다른 Secure Email Threat Defense 계정에 등록한 테넌트를 등록하려고 하면 권한 부여가 실패합니다 . Secure Email Threat Defense 동일한 Microsoft 테넌트 ID 를 사용하는 여러 계정을 허용하지 않습니다 .

Cisco 는 저널 데이터를 얼마 동안 보존합니까 ?

각 저널 메시지는 거의 즉시 메타데이터 추출 및 콘텐츠 분석을 거친 후 삭제됩니다 . 저널 메시지에 포함된 모든 첨부 파일은 추가 분석 또는 샌드박싱을 위해 최소 24 시간 동안 보존됩니다 . 저널에서 추출된 메타데이터는 90 일 동안 저장됩니다 .

사용자를 둘 이상의 Secure Email Threat Defense 인스턴스에 추가할 수 있습니까 ?

동일한 SecureX 로그인 계정을 사용하여 여러 Secure Email Threat Defense 인스턴스에 액세스할 수 있습니다 . 이렇게 하면 로그아웃한 후 별도의 계정으로 다시 로그인할 필요 없이 각 인스턴스를 더 쉽게 추적할 수 있습니다 .

Settings(설정)(톱니바퀴 아이콘) > Administration(관리) > Users(사용자) 에서 새 사용자를 생성하여 추가 인스턴스에 사용자를 추가합니다 . Secure Email Threat Defense 동일한 SecureX 로그인을 사용하는 계정은 사용자 메뉴에서 사용할 수 있습니다 . 이 액세스는 동일한 지역 (북미 또는 유럽) 의 Secure Email Threat Defense 계정으로 제한됩니다 .