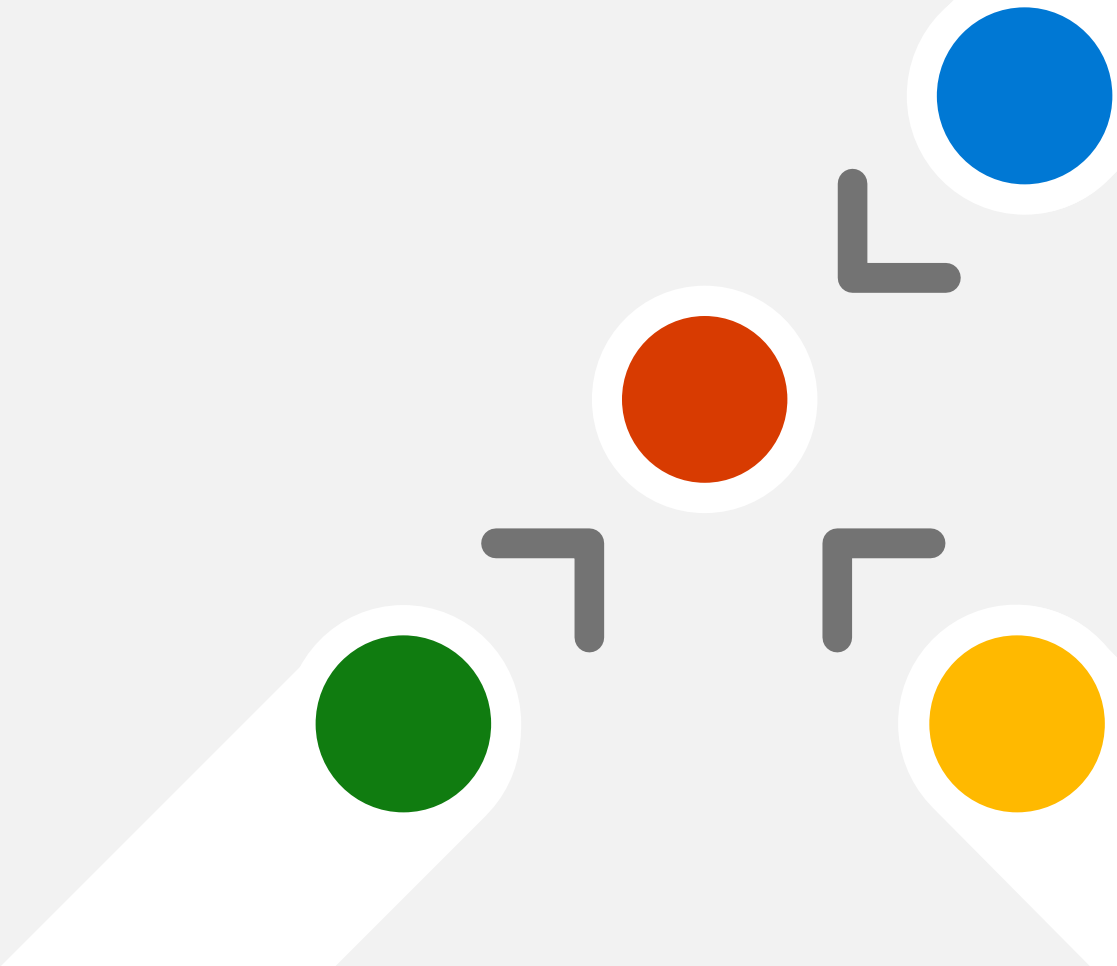
Microsoft Security

최신 보안 운영:

Microsoft 사이버 방어 운영 센터에서 배운 모범 사례 및 교훈



목차

보안 운영 개요

여러분은 보안 전문가로서 환경에 대한 위협이 진화하고 가속화되고 있음을 알고 있습니다.

오늘날의 사이버 공격은 조직적인 범죄 행위입니다. 사이버 범죄자들은 범죄 방식과 취약점에 대한 정보를 서로 공유합니다. 이들은 기술이 발전함에 따라 범죄 기술을 발전시키기 위해 노력합니다.

사이버 공격은 단순히 진화하는 기술적 위협 그 이상입니다. RaaS(서비스로서의 랜섬웨어)와 같은 트렌드는 점점 더 산업화되고 정교한 경제의 일부로, 자체 도구를 개발할 역량이나 기술이 없는 공격자는 이제 기성 침투 테스트 및 시스템 관리 도구를 관리하여 공격을 수행할 수 있습니다. 이러한 하위 수준의 사이버 범죄자들은 이미 경계를 위반하여 보다 정교한 범죄 그룹으로부터 네트워크 액세스를 구입할 수 있으며 성공적인 랜섬웨어 및 강탈 공격으로 범죄자들과 범죄 그룹 모두 이익을 얻습니다.

사이버 범죄자들이 계속해서 혁신함에 따라, 보안 팀은 공격에 대비할 수 있도록 보안 운영을 지속적으로 현대화해야 합니다.

즉, 모든 공격 벡터에서 보호 및 가시성을 확보하기 위해 기술 스택을 해결해야 합니다. 이는 팀의 프로세스를 평가하는 것을 의미하기도 합니다. 보안 운영 팀이 신속하고 정확하게 실제 위협을 방지하고, 탐지하며, 대응할 수 있나요? 아니면 팀원들이 너무 많은 신호와 거짓 긍정을 쫓는 것에 압도되어 있나요?

이 가이드의 세부 정보는 보안 운영을 현대화하고 진화하는 위협 환경에서 조직을 보호할 수 있도록 돕습니다.

Microsoft SOC에서 배운 교훈

여기에서 제시된 학습과 모범 사례는 Microsoft 고객과의 대화와 보안 운영 관행을 개발하고 발전시킨 Microsoft의 경험에서 비롯되었습니다.

어떤 사람들에게 놀랍게 들릴 수 있지만, Microsoft Corporate IT SOC는 Microsoft 및 서드파티 소프트웨어를 실행하는 Windows, Linux 및 Mac의 많은 사용자를 통해 크로스 플랫폼 환경을 보호합니다. 과거에 이 SOC는 대부분의 조직에서 보이는 것과 비슷한 전통적인 SOC 모델을 운영했으며, 사람들은 이러한 모델과 마찬가지로 당연한 과제에 직면했습니다.

- **이벤트 볼륨**—대용량 및 성장(현재 하루 200억 이벤트 규모)이 이를 처리하는 온-프레미스 SIEM의 용량을 초과했습니다.
- **분석가 과부하**—정적 규칙 집합은 경고에 대한 피로를 유발하는 과도한 양의 거짓 긍정을 만들었습니다.
- **열악한 조사 워크플로**—전통적인 온-프레미스 SIEM을 활용한 이벤트 조사는 투박했고, 수동 쿼리 및 수동 도구 전환이 필요했습니다.

과거에 경험했던 것이기 때문에 Microsoft는 귀하가 무엇을 다루고 있는지 알고 있습니다. 이 가이드를 통해 Microsoft와 고객 모두를 위해 Microsoft가 자체 보안 운영을 현대화하기 위해 노력하면서 배운 모범 사례 및 주요 교훈을 공유합니다.

Microsoft Corporate IT SOC는 Microsoft 및 서드파티 소프트웨어를 실행하는 Windows, Linux 및 Mac의 많은 사용자를 통해 크로스 플랫폼 환경을 보호합니다.

보안 운영의 역할

보안 운영은 범죄자들이 실시간으로 공격하고 있는 동안에도 시스템의 보안 보증을 유지하고 복원합니다. 주요 기능은 NIST 사이버 보안 프레임워크에 설명되어 있으며 다음과 같습니다.

- **탐지**
- **대응**
- **복구**

- **탐지**—보안 운영은 시스템 내부에 있는 적의 존재를 탐지해야 합니다. 사이버 범죄자들은 방해받지 않고 목표를 달성하기 위해 대부분의 경우 숨어있습니다. 탐지를 통해 의심스러운 활동에 대한 경고에 대응하거나 기업 활동 로그에서 비정상적인 이벤트를 사전 예방적으로 추적할 수 있습니다.

- **대응**—잠재적인 범죄 행동 또는 캠페인을 탐지하면, 보안 운영은 신속하게 조사하여 실제 공격(정탐) 또는 거짓 경보(오탐)인지 여부를 확인한 다음 공격의 범위와 목표를 열거해야 합니다.

- **복구**—보안 운영의 목표는 공격 중 또는 공격 후에 비즈니스 서비스의 보안 보증(기밀성, 무결성, 가용성)을 보존하거나 복구하는 것입니다.

이러한 영역에서의 효율성은 공격자가 조직에서 얼마나 많은 시간과 액세스 권한을 가지고 있는지를 제한하여 위험을 줄입니다. 따라서 궁극적으로는 사이버 공격자의 비용이 증가하고, 이익이 감소하여, 공격자는 ROI(투자 수익률)와 조직 공격에 대한 동기가 줄어듭니다. 또한 보안 운영 팀은 전반적인 보안 성숙도를 높입니다.

보안 운영의 모든 작업은 공격 시 사이버 공격자가 조직의 자산에서 얻을 수 있는 시간과 액세스를 제한하여 비즈니스 위험을 완화하는 방향으로 추진되어야 합니다.

보안 운영의 약점이 보안 운영으로 처리해야 하는 사고로 이어질 수 있으므로 조직 전체의 보안 성숙도를 높이는 것을 지지하는 경우가 많습니다.

비즈니스 관계

조직의 비즈니스 측면과 관계를 구축하고 유지 관리하면 보안 팀의 효율성이 향상됩니다. 비즈니스 전략을 이해하려는 노력과 팀이 공격을 예방하고 완화하기 위해 수행하는 작업을 이해하는 데 도움이 되는 방식으로 리더를 참여시키는 것이 이에 포함됩니다.

Microsoft에서는 비즈니스와 네 가지 주요 기능 통합 지점에 중점을 둡니다.

- **비즈니스 컨텍스트**
- **합동 연습**
- **주요 사건 업데이트**
- **비즈니스 인텔리전스**

- **비즈니스 컨텍스트**—해당 컨텍스트를 유동적인 실시간 보안 상황에 적용할 수 있도록 보안 운영에서 조직에 가장 중요한 사항을 이해합니다. 비즈니스에 가장 부정적인 영향을 미치는 것이 무엇인가요? 중요한 시스템의 가동 중지 시간일까요? 평판과 고객의 신뢰를 잃어버리는 걸까요? 중요한 데이터의 유출일까요? 중요한 데이터 또는 시스템의 무단 변경일까요? Microsoft 는 주요 보안 운영 리더와 직원들이 지속적인 정보 및 분류 사건을 헤쳐 나간 다음 이러한 맥락을 이해하고 시간, 주의 및 노력을 우선시하는 것이 중요하다는 것을 배웠습니다.

- **합동 연습**—주요 사건에 대해 함께 대응하는 연습을 하면 실제 사건의 높은 압박 속에서 신속하고 효과적인 의사 결정을 내리는 데 중요한 근육 기억과 관계를 구축하여 조직 위험을 줄입니다. 또한 사건이 실제로 발생하기 전에 해결할 수 있는 프로세스의 격차와 가정을 노출하여 위험을 줄입니다.

- **주요 사건 업데이트**—비즈니스 이해 관계자에게 주요 사건이 발생할 때 업데이트를 제공하면 비즈니스 리더가 위험을 이해하고 해당 위험을 관리하기 위해 사전 대응 및 대응 조치를 취할 수 있습니다.

- **비즈니스 인텔리전스**—예기치 않은 대상에 대한 발견을 비즈니스 리더와 공유하면 비밀 비즈니스 이니셔티브에 대한 외부 인식 또는 간과된 데이터 집합의 상대적 가치와 같은 인사이트가 트리거될 수 있습니다.

보안 운영이 조직의 다른 팀, 특히 비즈니스 부서와 어떻게 협업하나요?

팀은 중요한 자산을 식별하고 그에 따라 보안 우선순위를 설정할 수 있도록 주요 비즈니스 우선순위를 알고 있어야 합니다. 이를 통해 가장 중요한 자산에 노력을 집중하고 필수적인 방어 시스템, 정책 및 자동화된 조사를 비즈니스 팀에 맞출 수 있습니다.

주요 이해 관계자가 누구인지 알고 이들에게 즉시 알리면 다음을 포함하여 전체 비즈니스가 대응할 수 있습니다.

비즈니스와 필수적인 관계를 구축하는 가장 좋은 방법 중 하나는 사건 대응을 연습하기 위한 모의 훈련입니다. 모의 훈련 중에는 리더십 팀과 사건 대응 이해관계자가 모두 참여합니다. 이를 통해 보안 및 비즈니스 이해관계자가 관계를 구축할 수 있습니다. 두 가지 기능이 협업하는 방법을 배우게 되므로 사건이 발생했을 때 다른 당사자가 누구이고, 어떻게 참여하며, 비상사태를 해결하기 위해 무엇을 해야 하는지 모든 사람이 알게 됩니다.

- **보안 운영**
- **운영**
- **물류**
- **홍보/커뮤니케이션**
- **비즈니스 리더십**

일반적인 보안 운영 기능

보안 운영의 가장 일반적인 구성 요소는 사건 조사 및 대응이며, 대부분의 보안 운영 팀이 이를 위해 개발을 시작합니다. 일반적인 기능으로는 다음이 있습니다.

- **사건 조사 및 대응**—보안 도구(예: SIEM, XDR 및 EDR)의 경고 조사 및 수정에 대해 살펴보는 것이 이에 해당합니다. 대규모 조직에서는 모든 사건 대응이 기업 내부에서 처리될 가능성이 높습니다. 그러나 더 작은 소규모 조직이나 보안 기능의 개발이 더딘 조직에서는 이러한 업무가 MSSP(관리형 보안 서비스 공급자)에 전적으로 아웃소싱되는 경우가 있습니다. 다른 경우에는 고급 조사가 기업 내부에서 유지되는 동안 MSSP에 아웃소싱된 분류 및 고속 교정을 통해 하이브리드 모델이 개발됩니다.

- **전술적 위협 인텔리전스**—대규모 조직에서 가장 일반적으로 활용하는 전술적 위협 인텔리전스는 IOC(손상 표시기), 악성 IP 주소, 잘못된 DNS 이름 및 파일 해시와 같은 기술적인 사항에 중점을 둡니다. 경우에 따라 위협 인텔리전스 서비스의 정보를 이용하여 이 기능을 처리하는 조직도 있지만 다른 조직에서는 자체적인 기능을 만들고 연구를 수행합니다. 전술적 위협 인텔리전스는 조사 대응 기능을 지원하는 기능이며 진행 중인 경고 및 조사를 다룹니다.

- **사건/위기 관리**—중대한 사건 또는 큰 위기가 비즈니스를 위험에 빠뜨릴 때 조직은 전문적인 역할을 수행하는 사건 관리자 또는 위기 관리자를 고용할 수 있습니다. 이러한 관리자는 위기 대응을 관리하고, 사건의 규제 또는 규정 준수 효과를 평가하며, 사건 전반에 대해 비즈니스 리더와 의사 소통을 유지하는 데 능숙한 전문가입니다. 대규모 조직은 정규직 사건 관리자를 고용했을 수 있으며, 소규모 조직에서는 필요에 따라 임시직으로 고용할 수 있습니다. 이 역할에는 다른 분석가의 기술적인 조사 기술과는 다른 전문 기술이 필요합니다.

- **전용 SIEM 인프라 관리**—온-프레미스 인프라 집약적인 SIEM에 의존하는 조직은 SIEM 인프라를 유지 관리하기 위한 사내 팀을 보유했을 수도 있습니다. 레거시 온-프레미스 SIEM의 인프라는 매우 크고 복잡성이 높을 수 있습니다. 이러한 경우 고급 쿼리 및 사이버 공격자를 추적하는 분석가 팀을 지원하려면 추가적인 인력이 필요할 수 있습니다. 조직이 Microsoft Sentinel과 같은 클라우드 기반 SIEM으로 마이그레이션할 때 클라우드 기반 SIEM은 인프라 관리가 필요하지 않기 때문에 이 기능이 단계적으로 폐지되거나 다른 인프라 요구 사항으로 리디렉션될 것으로 예상됩니다.

전술적 위협 인텔리전스는 조사 대응 기능을 지원하는 기능이며 진행 중인 경고 및 조사를 다룹니다.

고급 보안 운영 팀의 경우:

- **사전 예방적 추적**—재능 있고 결단력 있는 사이버 공격자는 탐지를 피할 방법을 찾을 수도 있습니다. 공격자가 내부에 침입하면 노이즈 속에 숨어 더 낮은 우선 순위처럼 보이게 됩니다. 공격자들은 숨어 다니기 때문에 정상적인 프로세스로는 놓칠 수 있습니다. 업계는 1차 방어 방법을 파악한 적을 찾고 제거할 사전 예방적인 추적자가 필요하다는 사실을 인식하고 있습니다. 모범 사례에 대한 섹션에서 사전 예방적 사냥에 대해 더 많이 이야기하겠습니다.

- **전략적 위협 인텔리전스**—이 전략적 위협 인텔리전스 기능은 앞에서 설명한 전술 위협 인텔리전스 기능과는 다른 기능이며, 손상의 기술적 지표를 제공합니다. 전략적 위협 인텔리전스는 미래 지향적이며 비즈니스가 직면할 수 있는 위협과 공격의 종류에 대한 전략적 지침, 인텔리전스 및 연구, 이러한 공격이 발생했을 때 비즈니스에 위험 및 결과에 대한 고려 사항을 제공합니다. 전략적 위협 인텔리전스 담당자는 CISO 또는 비즈니스 리더가 현재의 위협 환경, 사이버 보안 관점에서 보는 뉴스를 해석하는 방법을 이해한 다음에 이러한 해석을 전략 계획에 추가하도록 조언합니다.

현실적으로 말하자면, 현재 보안 분석가에게는 인재가 부족합니다. 사내 보안 운영 팀을 보유한 모든 기업의 경우, 보안 운영 팀은 주로 사건 조사 및 대응에 집중해야 합니다. 이러한 기준이 충족되고 보안 운영 팀이 성숙하고 확장됨에 따라, 팀의 기능도 사전 예방적 추적 및 전략적 위협 인텔리전스를 추구하는 방향으로 확장되고 이동할 수 있습니다. 그러나 소규모 팀만 있는 경우 사건을 식별하고 대응하는 데 집중해야 합니다.

보안 운영 현대화

보안 운영을 현대화하기 위해 사후 대응에서 사전 예방적 대응으로, 네트워크 경계 모델에서 보안을 위한 기본 제어 평면으로 ID를 이용하는 보안 모델로의 진화를 지원하는 도구 및 프로세스를 발전시켜야 합니다.

사후 대응에서 사전 예방으로

가시성 향상

심층 툴링과 자동화는 분석가가 순수 사후 대응에서 적에 대비해 사전 예방적으로 준비하고 검색하도록 전환하는 데 필요한 가시성을 제공하고 시간을 절약할 수 있도록 돕습니다. 이러한 툴링 유형은 XDR(Extended Detection and Response)이라고도 하며, 엔드포인트, ID, 클라우드 스토리지 계정 등과 같은 특정 리소스에 대한 고품질 탐지 및 기타 기능을 제공하는 데 중점을 둡니다.

많은 조직이 레거시, 온-프레미스 SIEM 및 로그 중심 분석 프로세스에 계속 의존하고 있습니다. 그러나 "수집은 탐지가 아니다"라는 사실을 기억하는 것이 중요합니다. 분석가가 면밀히 조사하기에 데이터가 너무 많다면 단순히 로그를 수집하는 것은 도움이 되지 않습니다. 노이즈 내부의 신호를 놓치고, 실제 위협이 파악되지 않는 동안 분석가가 거짓 긍정을 쫓으면서 귀중한 시간을 낭비하는 가능성이 높아질 것입니다. 레거시 SIEM 및 로그 중심 접근 방식에서 조직은 Microsoft Sentinel과 같은 클라우드 기반 SIEM 및 EDR(Endpoint Detection and Response)과 같은 심층 툴링을 활용하여 모델을 발전시키기 위해 노력해야 합니다. 이러한 탐지 도구가 머신 러닝, 동작 분석 및 SOAR(보안 오케스트레이션 자동 응답) 기술을 유입되는 경고에 적용할 수 있는 클라우드 기반 SIEM과 통합되면 다음과 같은 세 가지 상황이 발생합니다.

1. 많은 경고가 분석가의 시간을 필요로 하지 않고 자동화를 통해 처리됩니다.

2. 분석가가 실제로 일어나고 있는 일과 성공하기 위해 위치해야 하는 장소에 대한 정확한 가시성을 확보함에 따라 분석가의 대기열에 전달되는 경고의 품질이 크게 향상됩니다.

3. 기술이 점점 더 보안 운영의 사후 기능을 더욱 자동화함에 따라 분석가들은 보안의 사전 예방적인 추적 측면에 더 집중하며, 운영 환경에서 이상 징후를 검색하고 적을 추적하는 작업을 시작할 수 있습니다.

사후 대응에서 사전 예방으로, 온-프레미스 SIEM 및 툴링에서 클라우드 기반으로의 발전이 항상 직선적인 것은 아닙니다. 그러나 역사적으로 확인할 수 있는 일반적인 성숙도입니다. 이러한 보안 운영은 미래에 증가할 것으로 예상되고, 보안 운영을 현대화하기 위해 생산적인 단계를 밟아 나가는 데 관심 있는 조직을 위한 모델로 삼는 것이 좋습니다.

공격 노출 영역을 줄이는 것은 취할 수 있는 또 다른 사전 예방적 단계입니다. 조직에 대한 대부분의 공격은 사이버 킬 체인으로 알려진 구조에 따라 진행됩니다. 킬 체인은 일반적인 공격이 어떻게 작동하는지, 어떤 기술이 체인의 각 섹션의 위협을 완화하는 데 도움이 되는지를 이해하는 데 도움이 됩니다. 조직에서는 이러한 킬 체인을 이해함으로써 공격을 중지하거나 확산을 막기 위해 체인의 각 링크에 '방어점(break)'을을 배치할 수 있습니다.

다음은 일반적인 킬 체인의 단계입니다.

1. 정찰—범죄자는 조직이나 조직 내 사용자를 악용하는 방법을 고안합니다. 이 활동에는 스피어 피싱 캠페인에 이용될 수 있는 정보를 밝히기 위한 연구, 범죄자가 조직 내 취약성에 대한 정보를 구매하는 다크 웹 활동 또는 조직의 IT 인프라 또는 사용자 기반의 약점을 밝히기 위한 정찰이 포함될 수 있습니다.

2. 취약성 악용—그런 다음 사이버 범죄자는 공격을 시작합니다. 이러한 공격은 일반적인 피싱 캠페인이거나 조직의 시스템에 악성 코드를 제공하도록 설계된 보다 정교한 기술을 통해 진행될 수 있습니다.

3. 횡적 이동—일단 조직 내부로 침입하면, 범죄자들은 탐지되지 않도록 조직의 시스템을 통해 사용자의 액세스를 활용하여 주요 데이터를 찾습니다. 침입이 발각된 경우, 사이버 범죄자들은 침입 경로를 숨기거나 다른 진입점을 추가하는 조치를 취할 수 있습니다.

4. 데이터 유출—개인, 금융, 지적 재산권 또는 기타 중요한 정보 등 원하는 데이터를 찾으면 범죄자들은 이를 훔치거나 랜섬웨어 공격의 일환으로 암호화할 수 있습니다.

보안 도구 전반의 오케스트레이션이 부족하면 보안 분석가가 위협을 수동으로 해독할 수밖에 없어 시간이 중요한 보안 조치 측면에서 대응 속도가 느려질 수 있습니다.

전통적인 경계 방어 전략은 더 이상 조직에 대한 공격을 완화하기에 충분하지 않습니다. 피싱 및 암호 스프레이와 같은 최신 공격 기술은 경계 방어를 물리칠 수 있도록 설계되었습니다. 또한 클라우드와 회사 네트워크 외부의 모바일 디바이스에 점점 더 많은 양의 데이터가 존재하게 됩니다. 이에 대응하여 보안 팀 리더는 단순히 사이버 범죄자들을 막기 위해 설계된 경계 기반의 보호에서 벗어나 오늘날의 '침해 가정'에 대해 설계된 보호/탐지/대응 접근 방식으로 전환해야 합니다.

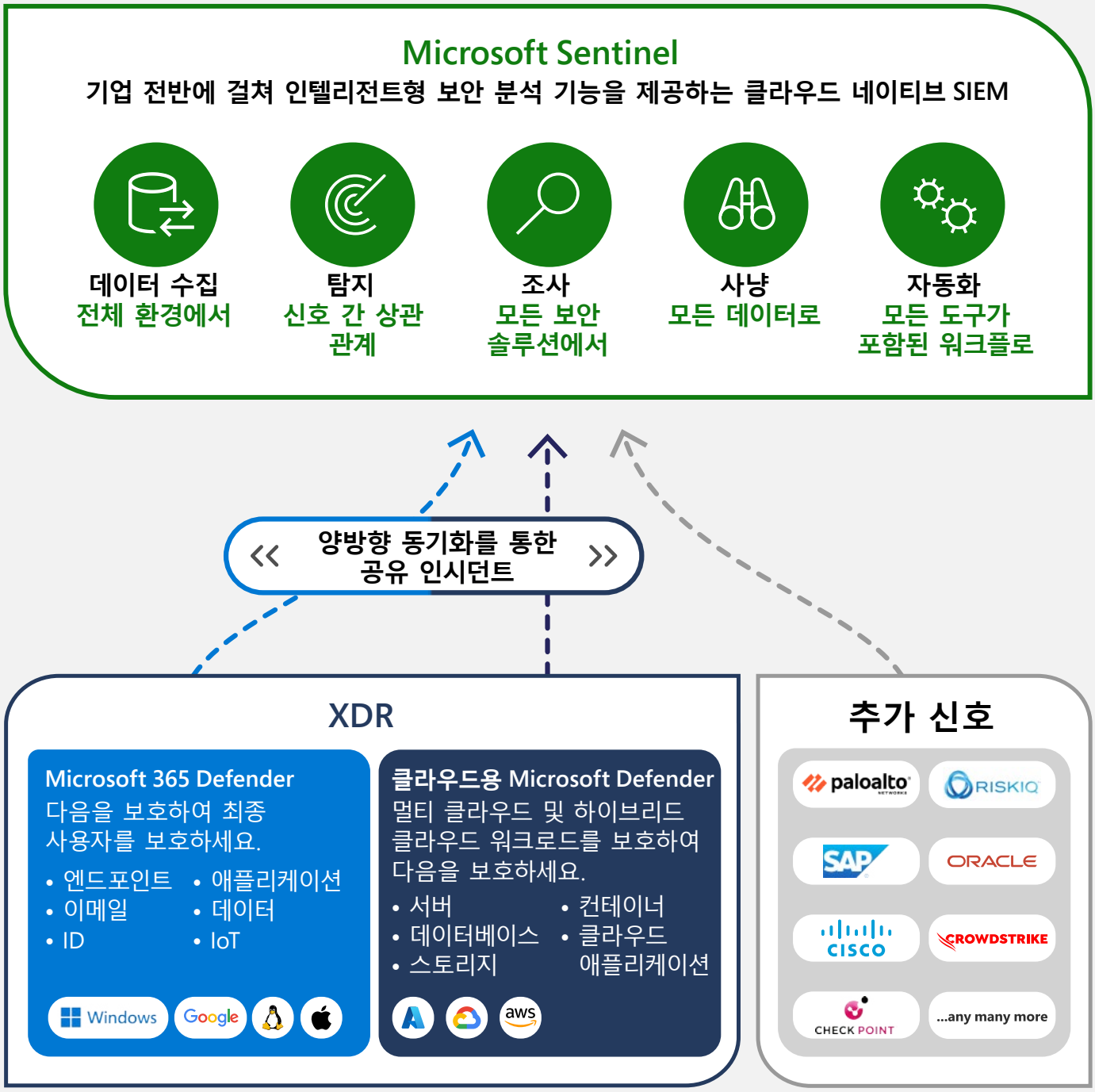
그러나 다층 접근 방식은 킬 체인의 특정 섹션을 해결하기 위해 단편적으로 배포된 포인트 솔루션을 통해 구현되는 경우가 많으며, 도구가 격리되어 별도로 관리해야 하는 경우가 있기 때문에 조직을 취약하게 만듭니다. 이를 통해 사이버 공격자는 가시성과 커버리지 측면에서 그들이 악용할 수 있는 공간을 확보할 수 있습니다.

오늘날의 진화하는 위협 환경에서 사이버 위협을 완화할 수 있는 전체적인 접근 방식을 위해서는 CIO와 조직 전반에 걸쳐 통합성과 가시성을 제공할 수 있는 플랫폼이 필요합니다. 통합형 접근 방식은 격차를 줄여 공격 노출을 줄입니다. 이 접근 방식은 클라우드 네이티브 SIEM 시스템을 통합하여 활성화되며, 이는 XDR(확장 탐지 및 대응) 솔루션으로 플랫폼 전반에 걸쳐 광범위한 기능을 제공합니다. 이러한 솔루션은 도메인 전반에 걸쳐 심층적인 위협 보호를 제공하여 방어자가 서로 다른 경고를 연결하고 공격자보다 앞서 나갈 수 있도록 지원합니다.

피싱 및 패스워드 스프레이와 같은 최신 공격 기술은 경계 주변을 돌아다니며, 점점 더 많은 리소스가 기업 네트워크 외부의 클라우드와 모바일 디바이스로 유입됩니다.

Microsoft의 접근 방식

Microsoft SOC에서는 Microsoft Sentinel, Microsoft 365 Defender 및 클라우드용 Microsoft Defender의 통합형 SIEM + XDR 기능으로 폭넓고 깊이 있는 가시성을 구현합니다.



- **Microsoft Sentinel**은 업계를 선도하는 클라우드 네이티브 SIEM으로서 모든 소스, 데이터 및 엔터티에서 수집합니다. Sentinel은 내장 SOAR 기술로 경고 탐지, 위협 가시성, 사전 예방적 추적 및 오케스트레이션된 위협 대응을 지원하여 기업 전반에서 인텔리전트 보안 분석 및 위협 인텔리전스를 제공합니다.

- **Microsoft 365 Defender**는 ID, 엔드포인트, 애플리케이션 및 이메일 전반에서 XDR(Extended Detection and Response)을 제공합니다.

- **클라우드용 Microsoft Defender**는 IoT, 인프라, 클라우드 리소스 및 워크로드에 대한 포괄적인 다중 클라우드 보호를 제공합니다.

보안 운영

Microsoft 참조 아키텍처

보안 운영에 대한 Microsoft의 기술 비전의 중심에는 분석가와 추적자와 같은 인력이 있습니다. Microsoft의 통합 SIEM + XDR 보안 기술은 분석가와 추적자에게 XDR을 통한 신호의 깊이와, 클라우드 네이티브 SIEM인 Microsoft Sentinel을 통한 신호의 폭을 모두 통합하는 고품질 경고에 대한 깊이 있는 인사이트를 제공함으로써 성공할 수 있도록 지원합니다. Microsoft의 XDR 보호는 Microsoft 제품 및 서비스에서 환경의 다른 모든 제품으로 확장되며, 조정된 탐지 및 대응으로 정교한 공격 체인도 찾고 제거하여 적들이 환경 전반에 침입했을 때 돌아다니지 못하도록 막을 수 있습니다.

SIEM 및 XDR을 통한 Microsoft 통합 위협 방지에 대해 자세히 알아보세요.

Microsoft의 통합 SIEM + XDR 보안 기술은 분석가와 추적자에게 고품질 경고에 대한 심도 있는 인사이트를 제공하여 성공할 수 있도록 지원합니다.

제로 트러스트 및 최신 보안 운영

지금까지 대부분의 조직은 네트워크 기반 공격에 대한 적절한 방어 시스템을 보유했습니다. 사이버 공격자는 이를 인식하여 방어가 약한 ID 기반 및 애플리케이션 기반을 공격하는 것으로 전술을 전환했습니다. 또한 디바이스와 앱은 이제 네트워크를 떠나 경계선을 제어 지점으로 제거합니다.

현대화는 적의 전술에 맞춰 방어 전술을 진화시키는 것을 의미합니다. 제로 트러스트 모델이 ID 우선 모델이므로 제로 트러스트 보안 모델을 채택하는 것이 좋습니다. 이제 네트워크를 무시해야 한다고 말하는 것이 아닌, ID 기반 공격 기술에 먼저 집중해야 하며 ID 보안 기술과 기능을 구축할 수 있도록 최우선 순위로 설정하는 것이 좋습니다.

네트워크에 강력한 방어를 구축하고 기업 방화벽 뒤에 있는 모든 것이 안전하다고 믿는 대신, 제로 트러스트 모델은 보안 침해를 가정하고 마치 각 요청이 통제되지 않은 네트워크에서 비롯된 것처럼 검증합니다. 제로 트러스트 모델에는 신뢰할 수 있는 네트워크가 없으며 모든 네트워크는 적대적입니다.

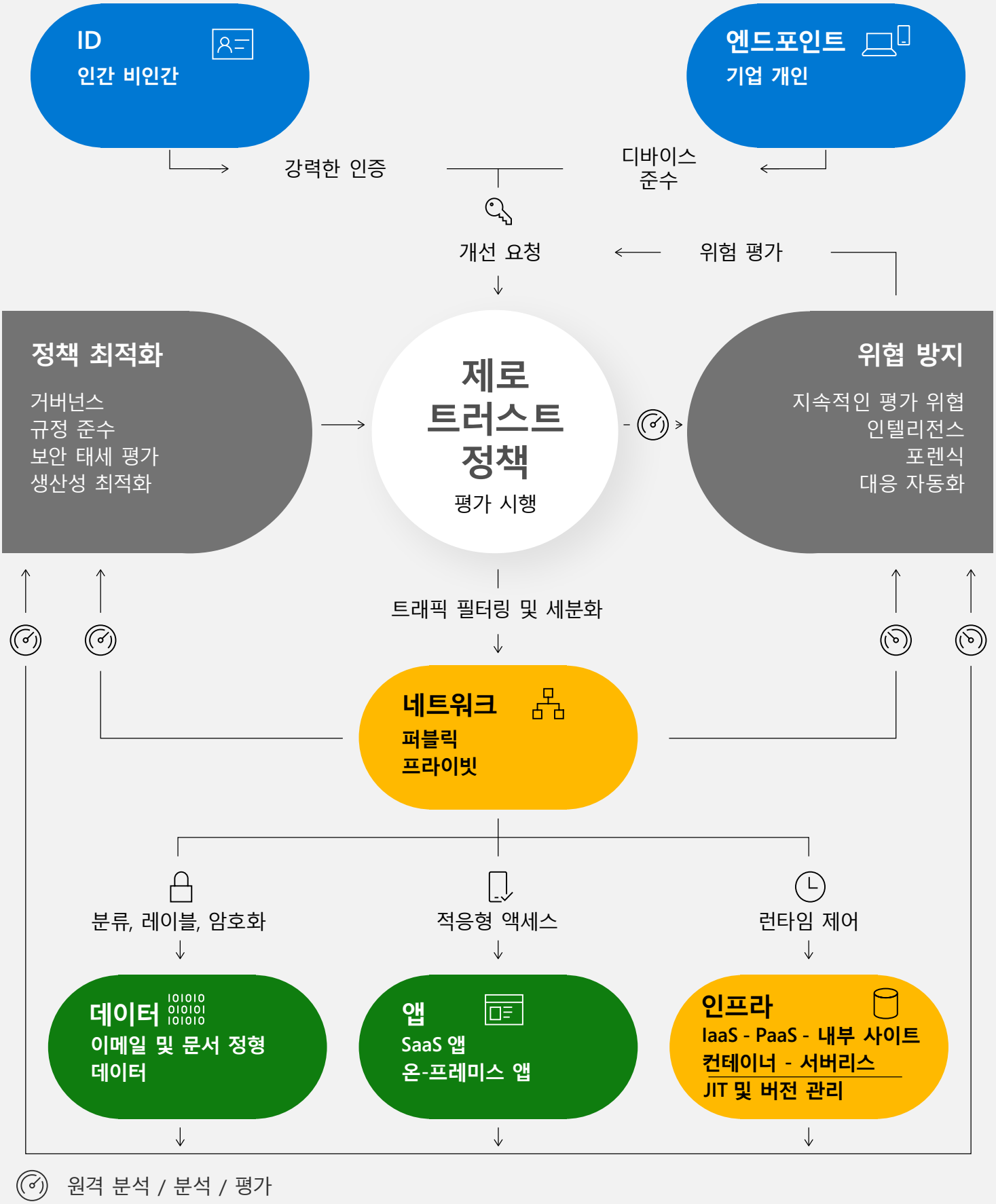
1. 명시적으로 검증 – 항상 사용자 ID, 위치, 디바이스 상태, 서비스 또는 워크로드, 데이터 분류 및 이상 징후를 포함하여 이용 가능한 모든 데이터 요소를 기반으로 인증하고 승인합니다.

2. 최소 권한 액세스 이용 – 위험 기반 적응형 정책, Just-In-Time 및 Just-Enough Access(JIT/JEA), 그리고 데이터 보호를 통해 사용자 액세스를 제한하여 데이터와 생산성을 모두 보호합니다.

3. 침해 가정 – 네트워크, 사용자, 디바이스 및 애플리케이션 인식에 따라 액세스를 세분화하여 침해에 대한 피해 반경을 최소화하고 측면 이동을 방지합니다. 모든 세션이 엔드 투 엔드 암호화 처리되었는지 확인합니다. 분석 기능을 사용하여 가시성을 확보하고 위협을 탐지하며 방어를 개선합니다.

제로 트러스트 접근 방식은 전체 디지털 부동산 전반에 걸쳐 확장되어야 하며 통합 보안 철학과 엔드 투 엔드 전략 역할을 수행해야 합니다. ID 엔드포인트, 디바이스, 애플리케이션, 데이터, 인프라 및 네트워크 등 6가지 기본 요소에서 제로 트러스트 제어와 기술을 구현함으로써 가능합니다. 이러한 6가지 기본 요소는 신호원이고, 적용을 위한 제어 평면이자, 방어해야 할 중요한 리소스입니다. 이를 통해 ID부터 시작하여 각 요소는 중요한 집중 투자 영역이 됩니다.

이러한 6가지 기본 요소는 신호원이고, 적용을 위한 제어 평면이자, 방어해야 할 중요한 리소스입니다.


ID
인간 비인간
엔드포인트
기업 개인
강력한 인증
디바이스
준수
개선 요청
위험 평가
정책 최적화
거버넌스
규정 준수
보안 태세 평가
생산성 최적화
제로
트러스트
정책
평가 시행
위협 방지
지속적인 평가 위협
인텔리전스
포렌식
대응 자동화
트래픽 필터링 및 세분화
네트워크
퍼블릭
프라이빗
분류, 레이블, 암호화
적응형 액세스
런타임 제어
데이터
이메일 및 문서 정형
데이터
앱
SaaS 앱
온-프레미스 앱
인프라
IaaS - PaaS - 내부 사이트
컨테이너 - 서버리스
JIT 및 버전 관리
원격 분석 / 분석 / 평가

제로 트러스트에서 오케스트레이션의 역할

오케스트레이션은 애플리케이션을 통합하고 워크플로를 자동화하는 프로세스입니다. 이미 언급한 바와 같이, 제로 트러스트는 엔드 투 엔드 전략에 완전히 통합될 때 가장 효과적입니다. 그러나 규정 준수 및 운영 효율성을 지원하는 방식으로 이러한 통합을 달성하려면 신중한 오케스트레이션이 필요합니다.

이는 명확한 제로 트러스트 정책을 시행하고 이러한 정책의 효과에 대한 지속적인 평가를 실시하여 필요에 따라 조정할 수 있음을 의미합니다. 지속적인 평가는 강력한 보안 태세를 유지하면서 거버넌스, 규정 준수 및 생산성을 최적화하는 데 필수적입니다. 위협 인텔리전스 피드를 통합하면 최신 위협에 따라 정책을 쉽게 조정할 수 있으며, 대응 자동화를 통해 공격에 실시간으로 대응하고 효율성을 높일 수 있습니다.

제로 트러스트로의 전환을 계획하고 구현할 수 있도록 제로 트러스트 현대화 전략을 추진하기 위한 권장 로드맵입니다.

세분화 전략 및 팀 조정

- ID, 디바이스, 애플리케이션, 데이터, 인프라 및 네트워크를 단일 기업 세분화 전략으로 통합하세요. 모든 사람이 같은 곳에서, 같은 전략을 추구하고, 같은 우선 순위로, 같은 언어를 말해야 합니다.

최신 ID 기반 경계 구축

- 사용자 및 디바이스 보증을 활용하여 **주요 경로**를 설정하세요.

  사용자 – 최신 애플리케이션에 액세스하려면 암호가 필요하지 않거나 다중 인증이 필요합니다.

  디바이스 – 액세스하려면 디바이스 무결성이 필요합니다.

먼저 IT 관리자에게 주요 경로를 롤아웃하는 것이 좋습니다.

IT 관리자는 광범위한 롤아웃 전에 개선 작업을 수행하도록 기술 피드백을 제공할 수 있으며, IT 관리자가 사이버 공격자의 표적이 되므로 관리자 계정 침해는 큰 영향을 미칠 수 있습니다. IT 관리자를 먼저 보호한 다음 일반 사용자를 보호하세요.

완료 전략

- 앱을 현대화하고 App Proxy를 통해 레거시 온-프레미스 자산에 대한 강력한 보증을 제공하세요.
- 중요한 데이터(CASB, CA 액세스 제어, AIP)에 대한 보호 수준을 높이세요.
- 레거시 인증 프로토콜을 폐기하세요.

세분화 및 네트워크 경계 개선

- 비즈니스 크리티컬, 생명/안전 및 운영/물리적 영향으로 자산을 세분화하세요.
- 미세 세분화를 추가하여 위험을 더욱 줄이세요.
- 지원되지 않는 운영 체제 및 애플리케이션과 같은 레거시 컴퓨팅 플랫폼을 폐기하고 분리하세요.

제로 트러스트로 시작하기

제로 트러스트는 특정 기술이 아닌 보안 모델이며, 제로 트러스트를 달성은 끄고 켤 수 있는 스위치가 아닌 하나의 여정입니다. 오늘날의 모바일, 원격 및 하이브리드 업무 환경에서 더 이상 보안을 위해 네트워크 경계에 의존할 수 없으며 네트워크 경계는 사라지고 있습니다. ID 기반 보호를 통해 보안 운영을 조정하고 제로 트러스트 모델의 토대를 마련해야 합니다. 사용자는 여러 디바이스를 이용해 다양한 네트워크 및 앱을 통해 엔터프라이즈 리소스에 액세스할 수 있습니다. 거의 모든 리소스는 액세스를 위한 인증이 필요하고, 공용 Wi-Fi 네트워크의 개인 디바이스나 네트워크 경계 내부에 있는 기업 디바이스의 모든 액세스 요청에서 ID가 공통적 요소입니다. ID를 제어 평면으로 활용하여 사용자, 디바이스 및 기타 요소가 완전히 검사될 때까지 모든 단일 액세스 요청을 신뢰할 수 없는 것으로 처리합니다.

제로 트러스트 보안 모델을 구현하는 첫 번째 단계는 모든 앱을 Microsoft Entra ID와 같은 단일 클라우드 ID 솔루션에 연결하는 것입니다. 이를 통해 ID 기반 보안을 구축하고 전체 환경에 사용자 맞춤형 정책을 적용하여 모든 앱에 대한 액세스를 제어할 수 있습니다. 이 단계가 완료되면 모든 앱에 대한 다중 인증을 구현할 수 있습니다. 다중 인증은 계정 손상 공격을 최대 99.9%까지 차단할 수 있는 일관되고 강력한 보안 정책입니다.

조직의 제로 트러스트 보안 상태를 평가하려면 제로 트러스트 성숙도 평가를 수행합니다.

제로 트러스트에 대한 Microsoft의 권장 ID 솔루션은 Microsoft Entra ID입니다. ID 및 액세스 관리를 사용하여 제로 트러스트 여정을 시작하는 방법을 알아보려면 제로 트러스트를 사용하여 ID 보안을 참조하세요.

내부자 위협 방지

제로 트러스트 보안 모델과 통합 보안 제품군으로 활용한 보안 운영을 통해 외부 위협으로부터 조직을 더 안전하게 보호할 수 있습니다. 하지만 정보, 사용자 및 디바이스를 보호하는 도구와 프로세스로 내부자 위협을 방지해야 합니다.

이제 데이터는 온-프레미스 인프라를 넘어 멀티 클라우드 및 하이브리드 클라우드 환경으로 확장되어 데이터가 생성되는 시점부터 사용 중지되거나 삭제되는 시점까지 전체 데이터 수명 주기에 걸쳐 책임을 확장합니다.

보유하고 있는 데이터, 액세스하는 사람, 데이터를 사용하여 수행하는 작업을 아는 것은 조직의 보안에 필수적입니다. 그러나 ID 보안을 간소화하는 것과 마찬가지로 이러한 노력의 핵심은 확장된 IT 환경에서 사용자 생산성을 저하시키지 않으면서 위험을 줄이는 것입니다.

조직은 수명 주기의 여러 단계에서 데이터를 관리하고 보호하기 위한 다양한 기술과 도구를 보유하고 있습니다. 이러한 도구는 유연성을 제공하지만 많은 복잡성도 추가시킵니다. IDG의 최근 연구에 따르면 조직은 분류, 전자 검색 및 기록 관리와 같은 활동에 평균 5개의 서로 다른 데이터 관리 시스템을 이용하는 것으로 나타났습니다. 또한 통합형 보안 솔루션은 데이터 유출로 이어지는 중대한 격차를 해소하고 데이터 수명 주기 전반에서 엔드 투 엔드 가시성을 제공함으로써 내부자 위협을 방지할 수 있습니다.

다음 세 가지 주요 단계에 대해 엔드 투 엔드 내부자 위협 방지 노력에 집중하는 것이 좋습니다.

- **데이터 식별**
- **데이터 분류**
- **데이터 보호를 위한 도구 및 정책 배포**

목표는 정보가 어디서 어떻게 이용되든 모든 정보를 보호하도록 지원하는 것입니다.

보유하고 있는 데이터, 액세스하는 사람, 데이터를 사용하여 수행하는 작업을 아는 것은 조직의 보안에 필수적입니다.

의도적인 위험과 의도하지 않은 위험 구분

내부 위협은 모든 비즈니스에서 불가피한 부분이며, 합법적인 업무의 정상적인 과정 중에서도 데이터가 위험에 처하게 되는 경우도 있습니다. 리소스에 액세스하는 사람들의 수, 회사를 오고 가는 사람들의 자연스러운 주기에 대해 생각해 보세요. 작동 중인 올바른 프로세스, 기능 및 제어를 통해 생산성을 저하시키지 않으면서 데이터를 감독하고 사용자와의 신뢰를 유지할 수 있습니다.

갖춰야 할 중요 기능 중 하나는 사용자의 의도적인 위험과 의도하지 않은 위험을 구분하는 것입니다. 진정한 악성 사용자는 보안 제어를 끄거나 악성 소프트웨어를 설치하는 등 기업 정책에 위배되는 작업을 시도할 수 있습니다.

개인적인 이득 또는 악의적인 이유로 데이터를 유출하거나 훔치려는 의도도 있습니다.

보안 운영은 이러한 이벤트에 대비해야 하며 이러한 위협을 방지, 탐지 및 억제하는 방법이 필요합니다.

그러나 사용자가 기업 정책을 위반하고 있다는 사실을 인식하지 못한다는 위협 유형도 있습니다. 예를 들어, 사용자는 프로젝트에 대해 흥미를 느끼고 그룹 외부에서 프로젝트에 대한 정보를 공유할 수 있으며, 그 과정에서 중요한 정보를 전송하고 있다는 사실을 깨닫지 못하고 데이터 유출을 저지를 수 있습니다. 의도하지 않은 데이터 유출이 발생하기 전에 이를 중단시키고, 실시간으로 조사하고 확인할 수 있는 도구가 필요합니다. 따라서 보안 운영팀이 의도와 영향을 판단하고 데이터 유출이 부주의한 한 번의 행동인지, 잠재적으로 악의적인 대규모 공격의 일부인지를 판단할 수 있습니다.

위험을 표면화할 때는 의심스러운 활동에만 초점을 유지하여 사용자와 문제를 일으키지 않거나 거짓 긍정 경고를 통해 분석가를 압도되지 않도록 해야 합니다.

Microsoft Purview에서 내부자 위험 관리에 대해 알아보세요.

보안 운영 모범 사례

앞서 언급한 바와 같이, 보안 운영의 중심에는 사람, 특히 보안 분석가가 있습니다.

분석가는 작업을 수행할 때 OODA 루프를 통해 공식적으로 또는 비공식적으로 작업을 진행합니다.

- **관찰**
- **지향**
- **결정**
- **행동**

목표는 이용할 수 있는 최선의 정보를 활용해 가능한 한 빨리 OODA 루프를 통해 보안 운영 팀에게 권한을 부여하여, 보안 운영 팀이 최선의 결정을 내리고 가능한 가장 효과적인 조치를 취할 수 있도록 지원하는 것입니다.

더 나은 의사 결정을 더 신속하게 내리기 위해 가시성을 극대화하고, 수동 단계를 줄이며, 인적 영향을 극대화하는 데 집중해야 합니다.

가시성 극대화

- **내부**—우수한 커버리지(관리할 수 있는 100%에 가까운)뿐만 아니라 자산 유형 커버리지(ID, 엔드포인트, 이메일, 클라우드 애플리케이션, 온-프레미스 데이터센터, 클라우드 데이터센터 및 클라우드 SaaS/PaaS 애플리케이션의 데이터 포함)를 확보하여 내부 사각지대를 최소화합니다.

- **외부**—맬웨어, 이메일 공격, 웹사이트 공격, 손상된 암호/ID 등의 외부 환경으로부터 인사이트와 컨텍스트를 제공하는 외부 소스에서 위협 피드의 다양성을 확보해야 확인합니다. 이용하는 외부 위협 소스의 신선도 및 충실도(관련 세부 정보)를 극대화하세요.

수동 단계 (및 오류) 줄이기

불필요한 사람의 행동을 제거하기 위해 가능한 한 많은 수동 프로세스를 자동화하고 통합하면, 속도가 저하되고 잠재적인 인적 오류로 이어질 수 있습니다.

노이즈(거짓 긍정)에서 신호(실제 탐지)를 신속하게 분류하려면 사람과 자동화에 모두 투자해야 합니다.

Microsoft는 사람의 수고를 줄이는 자동화와 기술의 힘을 굳게 믿습니다. 그러나 궁극적으로, 상대해야 하는 사이버 공격자는 인간 운영자이기 때문에 사람의 판단이 위협에 대한 방어 프로세스에 매우 중요합니다.

자동화는 효율성을 활용하여 사람을 프로세스에서 제거하는 것이 아닌, 사람에게 권한을 부여하는 것입니다. 분석가의 업무에서 반복 작업을 자동화하여 분석가가 사람만이 유일하게 해결할 수 있는 복잡성 높은 문제에 집중할 수 있는 방법에 대해 생각해 보세요.

자동화는 대응 속도를 높이고 인적 전문 지식을 확보하여 사람이 더 많은 업무를 할 수 있도록 지원합니다. 반복적인 작업의 부담과 지루함을 줄여 분석가가 새로운 도전과 위협에 시간과 창의력을 집중할 수 있도록 지원합니다.

인적 영향 극대화

프로세스에서 인적 상호 작용(어려운 선택, 새로운 결정 등)이 합리적으로 요구되는 경우 분석가가 더 나은 이러한 결정을 하기 위해 심층적인 전문 지식과 인텔리전스에 액세스할 수 있어야 합니다.

또한 공격의 목표(장기적 가치)와 공격 차단(단기적 가치)을 학습하기 위해 공격 전개를 확인하는 시점을 고려하여 프로세스 전반에 학습이 통합되도록 보장해야 합니다.

신속하게 더 나은 의사 결정

가시성 극대화

내부 – 센서 커버리지 완전성 및 다양성

외부 – 위협 피드 다양성 및 충실도

수동 단계 (및 오류) 줄이기

자동화 – 탐지 및 대응 작업

통합 – 조사 도구

인적 영향 극대화

분석가에게 **심층적인 전문 지식 및 인텔리전스 연속 학습**에 대한 액세스 제공—공격을 관찰하고 방어에 학습을 통합

보안 운영 문화

문화는 모호한 상황이 많은 보안 운영에서 올바른 답이 어떤 것이고, 어떻게 느껴지는지 확립함으로써 매일 수많은 결정을 이끌어 냅니다.

문화적 요소를 사람, 팀워크 및 지속적인 학습에 집중시키면 팀이 다음과 같은 위협에 뒤처지지 않기 위해 지속적으로 진화하도록 지원할 수 있습니다.

- **현명한 인재 활용**—사람이 가장 가치 있는 자산이며, 자동화할 수 있는 반복적이고 고민하지 않아도 되는 작업에 시간을 낭비할 여유가 없습니다. 직면한 인적 위협에 대처하기 위해 전문 지식, 판단 및 창의적인 사고를 활용할 수 있는 풍부한 지식을 갖춘, 준비된 인력이 필요합니다. 이러한 인적 요인은 사람을 대체하는 것이 아닌 사람에게 더 많은 업무를 하도록 권한을 부여하는 도구 및 자동화의 역할과 분석가의 수고를 줄이는 것을 포함하여 보안 운영의 거의 모든 측면에 영향을 미칩니다.
- **팀워크**—팀에서 '외로운 영웅' 사고 방식을 용납해서는 안 됩니다. 팀 전체만큼 똑똑한 사람은 없습니다. 팀워크는 모두가 한 팀의 소속이고 모두가 서로를 지원하고 있다는 사실을 인식할 때 압박이 많은 근무 환경을 훨씬 더 재미있고, 즐겁고, 생산적인 환경으로 만듭니다. Microsoft SOC(Security Operations Center : 보안 운영 센터)는 작업을 전문 분야로 나누고, 사람들이 인사이트를 공유하고, 서로의 업무를 조정하고 확인하며, 서로에게서 지속적으로 배울 수 있도록 프로세스와 도구를 설계합니다.
- **'왼쪽으로 이동' 사고 방식**—기술을 지속적으로 진화시키는 사이버 범죄자와 해커보다 앞서 나가기 위해 팀은 활동을 지속적으로 개선하고 공격 타임 라인에서 팀의 활동을 '왼쪽으로 이동'해야 합니다. 속도와 효율성에 초점을 두면 공격을 조기에 탐지하고 더욱 신속하게 대응할 수 있는 방법을 찾음으로써 팀이 '공격 속도보다 더 빠르게' 행동할 수 있습니다. 이 원칙은 팀이 조직과 고객에 대한 위험을 줄이는 데 완전히 집중하는 지속적인 학습 성장 사고 방식을 효과적으로 적용한 것입니다.

높은 권한 계정 분리

모든 공격이 성공할 경우 비즈니스에 미칠 수 있는 피해의 관점에서 동일하게 생성되는 것은 아닙니다. 예를 들어, 이사회 구성원, CEO, CFO 등 높은 권한이 있는 계정과 관리자 계정이 손상될 경우 가장 큰 위험이 발생합니다. 따라서, 인터넷 공격 및 기타 위협 벡터로부터 중요한 계정을 보호하는 PAW(Privileged Access Workstations)로 전용 컴퓨팅 환경에서 계정을 분리하여 이러한 계정을 사전에 먼저 보호하기 위해 각별한 주의를 기울여야 합니다.

지표 – 성공 측정

지표(metric)는 문화를 명확하고 측정 가능한 목표로 바꾸고 사람들의 행동을 형성하는 데 강력한 영향을 미칩니다. 측정 내용과 지표에 집중하고 적용하는 방법을 모두 고려하는 것이 중요합니다. Microsoft는 SOC에서 몇 가지 성공 지표를 측정하지만 SOC의 업무가 직접 제어(공격, 공격자 등)에서 벗어난 중요한 변수를 관리하는 것이라고 항상 인식하고 있습니다. Microsoft는 편차를 목표 달성을 위한 SOC 실패의 일부가 아닌 프로세스 또는 도구를 개선하기 위한 학습 기회로 간주합니다.

다음은 추적, 동향 및 보고서 지표입니다.

- **MTTA(전체 평균 승인 시간)**—대응성은 SOC가 직접 제어하는 몇 가지 요소 중 하나입니다. 경고가 제기되는 순간부터 분석가가 경고를 확인하고 조사를 시작할 때까지의 시간을 측정합니다. 대응성을 개선하려면 분석가가 다른 진실 긍정 경고에 대해 대기하는 동안 거짓 긍정을 조사하는 데 시간을 낭비하지 않아야 합니다. Microsoft는 가차없는 우선 순위를 통해 이를 달성합니다. 분석가의 대응이 필요한 모든 경고는 90%의 진실 긍정이라는 실적을 기록해야 합니다.

- **MTTR(평균 수정 시간)**—많은 SOC와 마찬가지로, Microsoft는 사이버 공격자가 SOC 프로세스와 도구에 효과성 및 효율성을 추구하는 Microsoft 환경에 액세스할 수 있는 시간을 제한하고 있는지 확인하기 위해 사건을 해결하는 시간을 추적합니다.

- **해결된 사건(수동 또는 자동화를 통해)**—수동으로 처리되는 사건의 숫자와 자동화로 해결되는 사건의 숫자를 측정합니다. 이를 통해 직원 수준이 적절한지 확인하고 자동화 기술의 효율성을 측정할 수 있습니다.

- **각 계층 간 에스컬레이션**—분석가 계층 간에 에스컬레이션되는 사건의 숫자를 추적하여 각 계층의 워크로드를 정확하게 확인합니다. 예를 들어, 에스컬레이션된 사건에 대한 계층 1 작업이 계층 2에 완전히 귀속되지 않도록 해야 합니다.

중요한 위생 유지

방법, 방어 및 효과는 다를 수 있지만 간단히 말해서 공격자는 취약점을 악용합니다. 보안 전문가로서의 취약성을 제거하여 업무를 간단하게 만듭니다.

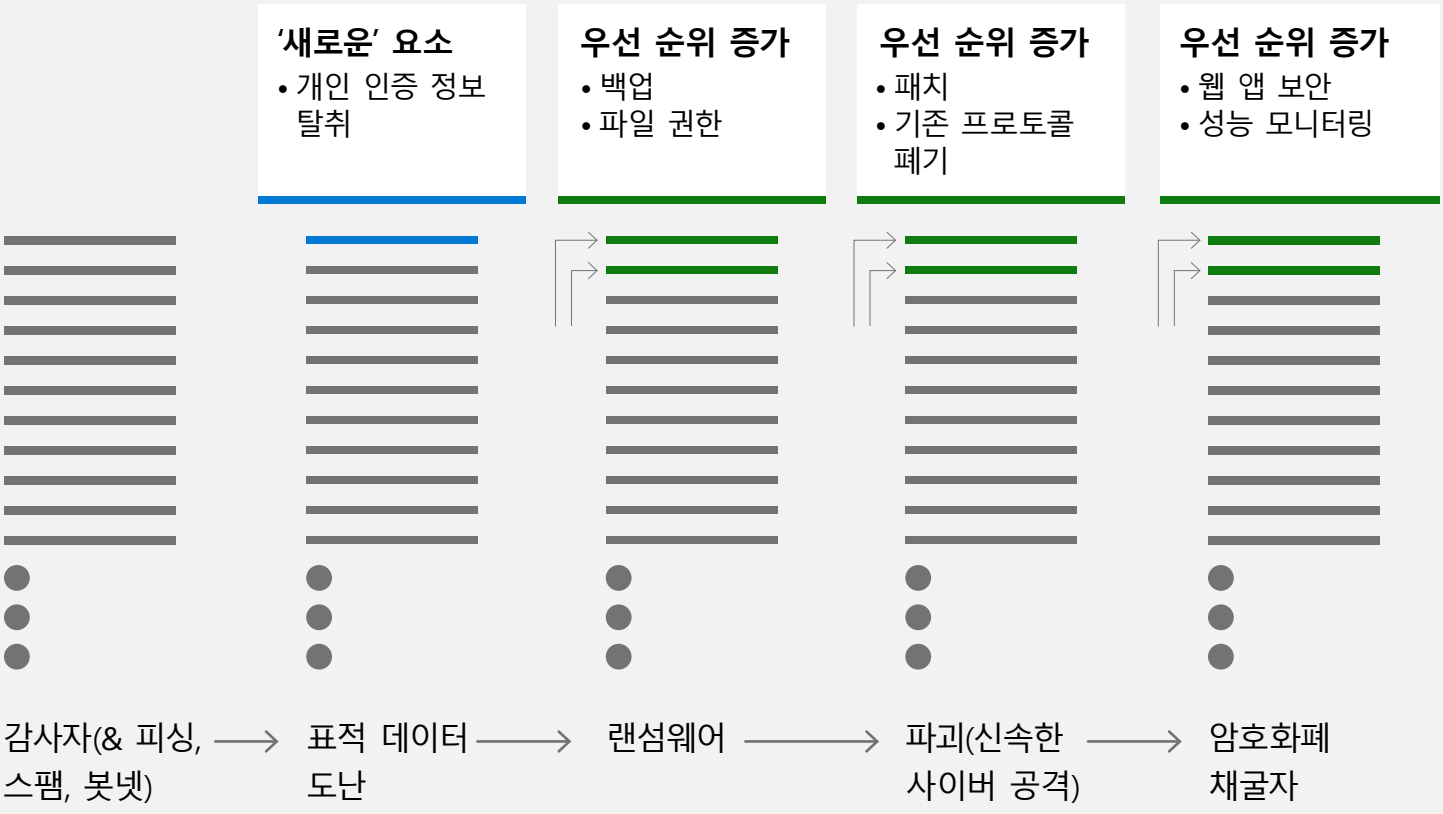
모든 팀은 환경을 업데이트하기 위해 해야 하는 업무가 있습니다. 이러한 업무를 '기술 부채'라고 합니다. 백업하거나 파일 권한을 업데이트해야 합니다. 또는 패치를 해야 하거나 폐기해야 할 기존 프로토콜도 있습니다. 이는 모두 잘 알려진 모범 사례입니다.

사이버 공격자가 비즈니스 모델을 구축하거나 새로운 공격 기술을 만드는 새로운 방법을 찾게 되면 새로운 방식으로 기존과 동일한 취약점을 악용하기도 합니다. 경우에 따라 이전에는 몰랐던 취약점을 공격자가 악용할 수도 있습니다. 따라서 사이버 공격자의 기술이 진화할 수 있지만, 우수한 기존 기술 위생에 필수적인 요소들도 동일하게 유지됩니다. 오랫동안 알고 있는 방식으로 환경을 최신 상태로 유지하고 사이버 공격자 행동을 기반으로 해야 할 작업을 배우는 것이 새로운 종류의 공격을 포함한 다양한 공격으로부터 조직을 보호하는 데 매우 중요합니다.

사이버 공격자가 비즈니스 모델을 구축하거나 새로운 공격 기술을 만드는 새로운 방법을 찾게 되면 새로운 방식으로 기존과 동일한 취약점을 악용하기도 합니다.

중요한 위생 = 상환해야 할 기술 부채

클라우드로 이 속도를 높일 수 있지만 많은 노력을 기울여야 합니다.



새로운 수익 창출 모델은 동일한 기존 위생 부채의 우선 순위를 단순하게 개편할 뿐입니다.

1. **중요한 위생 요구 사항을 정기적으로 확인하세요.**
2. **현재 일어나고 있는 일을 기반으로 우선 순위를 지정하세요.**
3. **모범 사례 및 우선 순위 목록을 자주 재확인하여 현재 조건에 맞도록 적용하세요.**
4. **'기술 부채'를 제거하기 위해 지속적으로 노력하세요.**

사전 예방적 추적

위협 추적은 조직의 위험을 줄이는 강력한 방법입니다. 그러나 위협 추적은 일반적으로 깊이 있는 전문가만을 위한 복잡성이 높고 신비한 예술 형태처럼 비생산적으로 묘사되기도 합니다. '위협 추적'이라는 용어는 단순히 숙련된 분석가가 환경을 사전 예방적이고 반복적으로 검색하여 다른 탐지를 회피한 사이버 공격 작업을 찾는 프로세스를 의미합니다.

추적이 사후 처리, 경고 및 탐지를 보완하므로 사이버 공격자보다 선제적으로 앞서 나갈 수 있습니다. 추적을 사후 활동과 구분하는 것은 추적자가 문제를 통해 생각하고, 동향 및 패턴을 식별하며, 더 거시적인 관점을 확보하는 데 긴 집중 시간을 할애하는 추적의 사전 예방적인 특성입니다. 성공적인 추적 프로그램은 온전히 사전 예방적이지는 않지만, 사후 대응 노력과 사전 예방적인 노력 사이에 지속적인 주의의 균형이 필요합니다.

위협 추적자는 기술을 예리하게 유지하고, 경고 대기열의 동향을 감독하기 위해 사후 대응 부서와의 연결을 계속 유지해야 합니다.

Microsoft의 SOC는 분석가를 다양한 유형의 위협 추적 작업에 활용하여 위협 추적에 접근합니다.

1. 사전 예방적인 적 연구 및 위협 추적.
대부분의 위협 추적자가 많은 업무 시간을 할애하는 부분입니다. 보안 운영 팀은 경고, 외부 손상 지표 및 기타 소스 등 다양한 소스를 검색합니다. 주로 TI(위협 인텔리전스), 환경의 비정상적인 관측 및 추적자의 개인 경험을 기반으로 사이버 공격자가 수행할 수 있는 작업에 대한 구조화된 가설을 구축하고 이를 구체화하기 위해 노력합니다. 실제로 이러한 유형의 위협 추적은 다음을 포함합니다.

- **데이터(쿼리 또는 수동 검토)를 통한 사전 예방적 검색.**
- **TI 및 기타 소스를 기반으로 한 가설의 사전 예방적 개발. (MITRE ATT&CK 지식 베이스 운영화를 참조하세요)**

2. 레드 및 퍼플 팀 협동. 환경을 보호하는 블루 팀으로 근무하는 일부 위협 추적자는 공격을 시뮬레이션하는 레드 팀 및 환경에 대한 승인된 침투 테스트를 수행하는 다른 팀과 협력합니다. 위협 추적자에게 순환되는 의무이고 일반적으로 레드 팀과 블루 팀이 모두 본인의 업무를 하고 서로에게서 배우는 퍼플 팀 협동을 포함합니다. 각 활동은 기업의 제품 엔지니어링 팀 및 기타 보안 팀과 함께 SOC 전체에서 공유되는 교훈을 확인하는 완전히 투명한 검토 절차로 이어집니다.

3. 사건 및 에스컬레이션. 사전 예방적인 추적자는 감시실에서 떨어진 어딘가에 격리되지 않습니다. 추적자들은 사후 대응형 분석가와 함께 배치되어 서로 자주 체크인하고, 작업을 공유하고, 흥미로운 결과 또는 관찰을 공유하며, 일반적으로 현재 운영에 대한 상황 인식을 유지합니다. 위협 추적자는 추적 작업에 모든 시간이 할당되지 않고, 유연하게 근무하며 필요한 순간에 바로 참여합니다.

이러한 기능은 서로 격리되어 있지 않습니다. 팀의 구성원들은 동일한 시설에서 작업하며 서로 자주 체크인합니다.

MITRE ATT&CK 지식 베이스 운영화

MITRE ATT&CK 지식 베이스는 귀중한 정보 수집물이지만 위협적일 수 있을 정도로 많은 양의 정보입니다. 좋은 소식은 기술 제품이 MITRE ATT&CK에서 가치를 도출하는 노력을 줄이도록 도울 수 있다는 것입니다. Microsoft 의 보안 솔루션을 포함한 오늘날의 많은 도구들은 이미 지식 베이스에 대한 많이 매핑되었습니다. 실제로 최근 **Azure용 보안 스택 매핑 연구 프로젝트**에서는 보안 컨트롤을 완화하는 MITRE ATT&CK 기술에 연결하는 매핑 라이브러리를 도입했습니다. 그러나 매핑은 일반적으로 포괄적이지 않습니다. 조직은 도구가 기본적으로 커버하는 위치와 여전히 격차가 있는 위치를 평가해야 합니다.

격차가 있는 경우 조직에 가장 적합한 MITRE ATT&CK 지식 베이스 영역에 기존 도구와 기술의 매핑을 사용자 맞춤하여 적용 여부를 확인할 수 있습니다. 또한 MITRE ATT&CK 지식 베이스에 포함된 모든 것이 필요하지 않을 것입니다. 적의 관점에서 지식 베이스를 살펴보세요. 전 세계의 모든 적이 귀하의

조직이나 비즈니스를 목표로 삼고 싶어하는 것은 아닙니다. 귀사와 같은 비즈니스를 목표로 하는 적을 확인하고 공격에 이용하는 기술을 이해하여 추적해야 하는 지식 베이스의 정보의 양을 줄입니다. 귀하의 조직을 대상으로 할 가능성이 가장 높은 적과 기술을 기반으로 탐지를 구축할 수 있습니다.

이러한 방식으로 MITRE ATT&CK 지식 베이스는 조직을 악용하려는 사이버 공격자가 수행할 가능성이 높은 작업을 개념화하고 잠재적 공격 패턴에 대한 탐지를 사전에 구축하도록 이용할 수 있는 도구가 됩니다.

IT와 친밀한 관계 구축

많은 조직에서 보안 운영으로 기술 환경을 제어하지 않습니다. 환경이 도구화되는 방법은 IT에 달려 있는 경우가 많습니다. 팀이 보유한 대응 및 수정 옵션은 IT가 독립적으로 결정한 기술 선택에 의존하는 경우가 많습니다. IT와의 관계 및 상호 기능 인식을 구축하는 것이 도움이 될 수 있습니다. 각 팀이 다른 팀이 하고 있는 업무와 조직을 보호하기 위해 임무의 일부를 수행할 때 직면한 과제와 한계를 알면 보안 운영의 현대화를 가속화하고 보안을 강화할 수 있습니다. 또한, 성공적인 수정을 위해서는 IT 담당자의 조치가 필요한 경우가 많습니다. IT 인력 역할, 책임 및 IT 팀 구성원의 기술 집합에 대한 좋은 관계와 지식을 보유하면 사건이 발생했을 때 팀이 적절한 사람에게 더 빨리 연락할 수 있습니다.

지속적인 개선

공격이 해결되어도 적들은 일어난 일에 대해 배우려고 노력하고 새로운 아이디어와 도구로 다시 시도할 것이라고 가정해야 합니다. 또한 분석가는 기술, 프로세스 및 툴링을 개선하기 위해 각 사건으로부터 학습하는 데 집중해야 합니다. 이러한 지속적인 개선은 공식적인 사례 검토에서 분석가가 사건과 흥미로운 관찰에 대한 이야기를 들려주는 일상적인 대화까지, 많은 비공식적 및 공식적 프로세스를 통해 발생할 수 있습니다.

업무량이 허용하는 한 조사 팀도 적을 사전 예방적으로 추적할 수 있으며, 이를 통해 조사 팀은 예리함을 유지하며 기술을 성장시킬 수 있습니다. 마지막으로, 퍼플 팀 협업은 목표 중 하나인 지속적인 개선으로 설계되어야 합니다. 레드 팀이 훈련에서 수비수의 탐지를 성공적으로 회피했으므로 모두가 배우고 더 발전할 수 있는 중요한 기회로 포용해야 합니다.

최종 권장 사항

보안 운영을 현대화하는 것은 중요한 과제입니다. 조직 전체의 이해관계자가 참여해야 하며 한 번에 모든 업무를 완료할 수 있다고 생각해서는 안 됩니다. 그러나 이러한 작업들은 취약점을 줄이고, 가시성을 증가시키고, 고급 기술을 보유한 공격자를 방어할 때 효율성과 유효성을 개선하기 위해 지금 바로 할 수 있는 몇 가지 작업입니다.

1. 제로 트러스트 수용 – 제로 트러스트 모델은 명시적으로 검증하고, 낮은 권한의 액세스 개념을 활용하며, '위반을 가정'하는 사고 방식을 유지하는 것입니다. 보안을 위한 제어 평면을 네트워크 경계에서 ID로 이동하여 제로 트러스트 여정을 시작하세요.

2. 높은 권한의 계정 분리 – 공격자가 가장 공격하기 쉬운 조직의 계정을 식별하고 PAW(Privileged Access Workstation)로 분리하여, 관리자 계정을 보호합니다. 관리자 계정이 손상될 경우 가장 많은 피해가 발생할 수 있으므로 계정을 분리하여 보호 작업을 시작하세요.

3. 공급망 강화 – 이 가이드의 모범 사례 섹션에서 소개한 '왼쪽으로 이동' 정신에 부합합니다. 악성 코드 또는 구성 요소를 공급업체로부터 받는 소프트웨어 제품에 몰래 숨겨두는 것은 사이버 공격자가 방어를 회피하기 위해 더욱 일반적으로 이용하는 방법입니다. 공급업체가 보안을 유지하기 위해 무엇을 하고 있는지, 귀사에서 무엇을 어디에 이용하는지 파악하고, 더 나은 자산 관리에 지속적으로 투자함으로써 공격 체인에 대한 인식을 더욱 넓히세요.

4. 침투 테스트에 투자 – 공격받기 전에 살펴보세요. 침투 테스트를 수행하여 공격받기 전에 실패 지점을 찾습니다. 침투 테스트의 결과를 성적표가 아닌 지속적인 개선 프로세스의 입력으로 이용합니다.

5. 포괄적인 조사 기능을 보유했는지 확인 – 전체 환경에서 조사할 수 있는 능력을 보유했는지 확인합니다. 엔드포인트에서 ID, 데이터에서 IoT, 클라우드 전반 등 다양한 관점에서 포괄적인 가시성을 확보할 수 있도록 노력하세요. 보안 유지에 매우 중요한 신속한 조사와 조기 탐지를 수행할 수 있습니다.

6. 보안 운영 도구 통합 – 통합된 접근 방식을 수용하여 커버리지의 격차와 사일로를 제거합니다. 통합된 클라우드 네이티브 SIEM 및 XDR을 활용하여 분석가에게 폭넓고 깊이 있는 접근 범위를 모두 제공합니다.

Microsoft의 통합 보안 솔루션이 보안 운영을 현대화하고 조직을 보호하기 위해 필요한 가시성을 제공하도록 지원하는 방법에 대해 자세히 알아보세요.

SIEM 및 XDR: 랜섬웨어에 대항할 수 있는 동맹 >

SOC 효율성 향상을 위한 통합 접근 방식 >

Microsoft Security