paloalto NETWORKS | UNIT 42 BY PALO ALTO NETWORKS

사이버 보안 체크리스트

# 57가지 사전 예방 팁

## 기업 보안 확보는 목적지가 아니라 여정

방어의 초점을 어디에 맞출지는 각 기업의 결정에 달려 있습니다. 침해를 방지하는 게 불가능한 일일지 모르지만, 침해가 발생하기 전에 대비를 잘 갖출 수는 있습니다. 지금 조처해두면 귀사가 공격자의 손쉬운 표적이 되지 않도록 보장할 수 있고, 위협 행위자가 귀사 네트워크를 통해 퍼져나갈 능력을 제한하여 사이버공격이 발생하더라도 피해를 최소화할 수 있습니다. 조직이 꼭 해야 할 일이 무엇인지 미리 알아내야 위협을 없애고 정상 업무에 복귀하며 피해를 복구할 수 있습니다.

다음 권장 사항은 실시간 인시던트 대응 케이스를 바탕으로, 2022 Unit 42 인시던트 대응 보고서를 요약하여 정리한 것입니다. 몇 가지 섹션으로 나누어 각 기업의 중점 분야를 정하고 보안 프로그램의 회복력을 강화할 수 있도록 구성했습니다.

## 기업 보안을 강화하기 위한 포괄적인 권장 사항

### IAM(Identity and Access Management)

- 가급적 웹 애플리케이션에 SSO(Single Sign-On) 플랫폼과 다단계 인증(MFA)을 사용합니다.
- Active Directory를 자주 검토하여 새로 만든 계정, 편지함, 인식할 수 없는 그룹 정책 개체가 있는지 확인합니다.
- 무단 액세스와 디렉터리 목록 기재를 방지하는 형태로 서버를 구성합니다. 강력한 액세스 제어를 적용합니다.
- 직원이 퇴사하는 경우, 신속하게 행동하여 해당 인물의 액세스를 취소하고(예: 활성 세션, 토큰, 계정, MFA 디바이스 및 교체용 자격 증명 등) 액세스가 확실히 취소되었는지 확인합니다. 조사가 필요한 경우에 대비해 해당 인물의 시스템과 데이터는 보존합니다.
- 권한 있는 계정은 유효한 비즈니스상의 필요가 있는 경우에만 사용하도록 한정하거나, 사용자가 주어진 업무를 완수하기 위해 권한 있는 계정이 필요한 경우로만 한정하고 로컬 관리자 계정 비밀번호를 재활용하지 않습니다.
- 직무 역할상 관리자 인터페이스와 디버깅 도구 액세스가 필요 없는 인물이라면 그러한 인터페이스와 액세스를 비활성화합니다.

공격자가 노리는 **7대 업종**은 금융, 전문 및 법무 서비스, 제조, 의료, 하이테크, 도소매였습니다.

## 리스크, 취약점, 패치 관리

- 자사의 중요하고 가장 값어치 있는 자산이 무엇인지 파악합니다. 여기에는 중요 자산 인벤토리를 포함하여 가장 가치가 높은 표적이 어디 있는지 알아두고, 그러한 대상에 추가적인 보호가 필요한지 판단하는 것도 포함됩니다.
- 오픈소스 코드를 구현하는 경우, 리서치를 통해 해당 코드에 공개된 취약점이 있는지 알아보고, 심사와 패칭을 마친 코드만 사용합니다.
- 정기적으로 웹 애플리케이션/코드 검토를 실시하고 일반에 공개된 인프라 전체에 대하여 매년 침투 테스트를 실시해 취약점을 찾아 권장 수정안을 따릅니다.
- 모범 사례에 따라 개발 환경 보안 설정을 구성합니다.
- 정기 스캔(예: 구성 검사)을 실행하고 정기 시스템 감사를 수행해 구성 오류를 탐지합니다.
- 검토해야 하는 변경 제어 프로토콜을 구현하고 구성 변경을 인증(사인오프)합니다.
- 운영 체제와 온프레미스 애플리케이션은 반드시 패치 관리를 해야 합니다. APT 공격자가 취약점을 발견하면 순식간에 행동에 나서기 때문입니다. 새로 공개된 취약점은 실사와 관련해 현실적으로 가능한 한 빨리 해결합니다.

## 데이터 및 소프트웨어 보안

- 중요 데이터의 위치를 파악하여 강력한 액세스 제어를 구현해 해당 데이터를 보호하고, 정기적으로 액세스를 모니터링하고 감사를 실시합니다. 중요한 데이터에 대한 액세스는 조직 내, 제삼자 중 필수 인원에게만 한정합니다.
- 노트북 및 이동식 디바이스에 디스크 전체 암호화를 구현합니다. 디바이스 분실이나 도난에 대비한 긴급 사태 대책을 세워둡니다.
- 디바이스 위치를 찾고/거나 원격으로 초기화하는 기능이 있는 Mobile Device Management(MDM) 애플리케이션을 구현하여 활용합니다.
- 데이터를 분류하고 태그를 지정하며 중요한 정보나 기타 회사에서 정한 관련 정보가 조직에서 유출되면 알림을 제공하는 DLP 프로그램을 설정합니다.

## 위협 탐지 및 대응

- 자격 증명 침해 탐지 서비스 및/또는 공격 표면 관리 솔루션을 사용해 취약한 시스템과 잠재적인 침해를 추적하는 데 보조 용도로 사용할 것을 고려합니다.
- EDR이나 XDR 솔루션을 활용하고, 보안 운영팀이 이 기술을 활용하는 법을 확실히 숙지하여 네트워크 전체에 대한 완전한 가시성을 유지하도록 합니다.
- 인시던트 대응 및 수정 계획을 세웁니다. 최선의 노력을 기울여도 인시던트는 발생할 수 있으므로, 시험을 거친 포괄적인 계획을 마련해야 인시던트가 발생하는 경우 빠른 조치를 보장할 수 있습니다. 사이버 보험이 있는 경우(권장), 해당 보험 정책의 주요 프로세스와 담당자를 계획에 포함해야 합니다.

## 기타 팁

- 로그 보존 리포지토리를 유지관리하며 정기적으로 모든 로그와 로그인 시도를 검토해 비정상적인 행동 패턴이 있는지 확인합니다. 로그가 각종 법적, 규제에 의한 의무를 다하기 위해 적절한 기간 동안 보관되도록 합니다. Unit 42 컨설턴트는 일 년 이상을 권장하며, 불가능한 경우 최소 90일로 설정합니다.
- 보안 정보 및 이벤트 관리(SIEM) 시스템과 같은 로그 집계 시스템을 활용하여 로그 보존, 무결성 및 가용성을 높입니다.
- 하청업체를 포함한 모든 사용자를 대상으로 매년 정기적으로 보안 인식 교육을 실시합니다. 신뢰할 수 있는 교육 플랫폼을 활용해 교육 커리큘럼에 맞춤형 장단기 목표를 포함할 수 있으면 좋습니다.
- 플랫 네트워크(flat network) 활용은 지양합니다. 네트워크와 Active Directory를 분리하고, 중요한 데이터는 분할하며, 안전한 VLAN(Virtual Local Area Networks)을 활용해야 합니다.

- 심층 방어 접근 방식을 따라 웹 애플리케이션 스택의 계층마다 안전장치를 구현합니다. 예를 들어 웹 애플리케이션 방화벽, 운영 체제 강화, 애플리케이션 입력 제어, 파일 무결성 모니터링 및 데이터베이스 액세스에 대한 최소 권한 사용자 계정과 업계 표준 암호화 등이 대표적입니다.
- 직원이 적법하게 비즈니스를 처리할 방법을 보장해야 합니다. 단순히 특정 벡터를 차단하기만 하면 직원들 나름의 독창적인 우회 방법이 출현하고 이는 회사 입장에서는 놓칠 가능성이 큽니다.
- 자사 이름에 흔한 오타를 포함하거나 변형한 형태를 바탕으로 한 도메인을 구매하는 것도 좋습니다. 이렇게 하면 위협 행위자가 귀사인 척 가장하기 어려워집니다.

**전체 침입의 77%**는 크게 세 가지 초기 액세스 벡터 때문인 것으로 의심됩니다. 피싱, 알려진 소프트웨어 취약점 악용, 그리고 무차별 자격 증명 공격으로, 주로 RDP(Remote Desktop Protocol)를 노립니다.

## 피싱 공격 예방을 위한 권장 사항

- ☐ "보안 인식을 높이는 사내 문화"를 조성하세요. 회사 경영진이 사이버 보안의 중요성을 믿고, 강력한 사이버 교육 프로그램을 지원, 홍보하며 회사 내 의사소통에서 보안을 강조하는 것이 무엇보다 중요합니다.
- ☐ 조직과 직원 역할에 따라 맞춤 설정된 사용자 지정 커리큘럼을 설정할 수 있고 위협 행위자 방법론이 빠르게 발전한다는 사실을 감안하는, 믿을 수 있는 교육 공급업체나 플랫폼을 활용하세요.
- ☐ 사용자가 의심스러운 피싱 이메일을 손쉽게 신고할 수 있게 하고, 신고서를 즉시 검토하며 그러한 메시지에 대한 조처가 즉시 이루어지도록 해야 합니다.
- ☐ 사용자에게 외부 관계자가 보낸 첨부파일과 관련하여 시각적으로 알림을 보냅니다. 이렇게 하면 회사 도메인과 겉보기에 비슷해 보이는 스푸핑 도메인을 알아보는 데 도움이 될 수 있습니다.
- ☐ 피싱과 스피어 피싱을 포함하는(그리고 그보다 더 많은 내용을 다루는) 포괄적인 교육 콘텐츠를 고안하세요. 물리적 보안, 디바이스 분실에 대한 업계 모범 사례, 내부자 위협 지표 등을 포함한 다른 소셜 엔지니어링 우려 사항을 포함하는 것이 좋습니다.
- ☐ 그룹별로 각자 맡은 역할과 관련 있는 웹 기반 모듈을 맞춤 제작하여 어떤 식으로 표적이 되는지 구체적으로 알려서 직원 스스로 자신을 노리는 전략을 더 잘 알아보고 피할 수 있도록 대비시킵니다.
- ☐ 매년 전반적인 교육을 실시하고 연중 "리프레시" 강좌를 통해 전 직원에게 지능형 기법과 같이 강조해야 할 구체적인 분야를 보완해줍니다.
- ☐ 보안 교육을 게임화하면 직원의 참여도를 높일 수 있습니다. 목표를 세우고, 목표 달성을 위한 규칙, 보상이나 인센티브, 피드백 메커니즘, 순위표 등을 만들어 활용하세요. 여러 조직이 서로 경쟁할 수도 있습니다.
- ☐ 피싱 테스트의 주요 성과 지표를 추적하여 조직의 요구 사항에 따라 피싱 콘텐츠와 난이도를 조정하세요.
- ☐ 사용자에게 이메일 말고 역할 기반 액세스 제어를 포함한 파일 공유를 통해 중요한 정보를 저장하도록 독려합니다.
- ☐ 첨부파일과 메시지 콘텐츠를 스캔하고 보낸 사람 평판을 평가하는 이메일 보안 솔루션을 활용합니다.
- ☐ 스푸핑 방지 및 이메일 인증 기법을 사용하세요. SPF(Sender Policy Framework)가 좋은 예입니다.
- ☐ 일반적인 비즈니스 운용에 필요하지 않은 경우, 지리적 위치에 따라 계정 로그인을 차단하는 것도 고려할 만합니다.
- ☐ 고급 피싱 차단/머신 러닝 솔루션이나 다른 타사 솔루션을 도입해 정교한 피싱 캠페인을 탐지하고 저지합니다. 피싱 대응 활동을 자동화하여 사람의 개입이 필요한 부분을 줄이는 것도 좋습니다.

## 기업 시스템을 최신 상태로 유지하기 위한 패칭 권장 사항

- ☐ 분산된 기업 전체에 걸쳐 모든 IT 자산(스토리지, 스위치, 노트북 등)의 인벤토리를 확인합니다. 자동 검색 도구를 사용하면 관리해야 할 대상이 무엇인지 명확히 파악할 수 있습니다.
- ☐ 패칭 요구 사항에 우선순위를 정합니다. 취약점마다 리스크가 높음, 중간, 낮음 중 어느 것인지 판별하고 조직의 리스크 내성에 따라 비즈니스에 대한 우선순위 정도를 확인합니다.
- ☐ 정기적으로 패치를 구축할 일정을 정합니다. 최소 한 달에 한 번 간격이 좋고, 우선순위가 높은 패치의 경우 필요하다면 비정기적으로 구축하도록 선택지를 부여합니다.
- ☐ 개발 QA 환경에서 패치를 테스트하여 프로덕션 환경에 구축되었을 때 "시스템을 중단"시키지 않는지 확인합니다.
- ☐ 패치 구축을 마치면, 안정성을 모니터링합니다. 이 과정에서 네트워크 안정성 모니터링도 동반할 수 있습니다.
- ☐ 더 이상 지원되지 않는 운영 체제에서 실행되는 시스템을 제거합니다.

**알려진 클라우드 보안 인시던트의 65%**는 구성 오류가 원인이었습니다.

## 클라우드 환경 보안 확보를 위한 권장 사항

- ☐ 대중에 노출된 인터넷상에서 액세스할 수 있거나 노출된 데이터가 무엇인지 정기적으로 평가합니다.
- ☐ 공격 표면 솔루션을 활용해 취약한 시스템과 관리되지 않는 클라우드 자산 추적에 도움을 받는 것도 좋습니다.
- ☐ 플랫폼별로 클라우드 보안 전문 지식을 활용하세요. 클라우드에서 보안을 관리하려면 각 플랫폼의 뉘앙스에 맞는 전문 지식이 필요합니다. 플랫폼이 복잡할수록 우발적으로 데이터를 공개할 수 있는 오류가 발생할 기회가 많습니다.
- ☐ 클라우드 제어 액세스 권한을 보유한 사용자에게 각 클라우드 환경에 관해 철저한 교육을 제공합니다.
- ☐ 사내에 전문 인력이 없거나 클라우드 환경이 특히 복잡하고 계속 변화하는 상황인 경우, 관리형 보안 서비스 옵션을 알아보는 것이 좋습니다.
- ☐ 클라우드 환경에 대한 액세스를 제어합니다. CSP 콘솔, API, 클라우드 CLI와 같은 클라우드 제어에 대한 액세스는 필수 인원으로 제한해야 합니다. 이러한 RBAC는 구성 및 다른 보안 오류 리스크를 최소화하는 데 필수 불가결합니다.
- ☐ 관리자와 사용자 자격 증명을 분리하고, 일상적인 사용자는 프로덕션 환경에 출입하지 못하도록 제한합니다.
- ☐ 가능한 경우 허용 목록을 구현하여 알려지고 신뢰할 수 있는 엔드포인트로만 액세스를 추가로 제한하는 것도 좋습니다.
- ☐ 정기적으로 클라우드 데이터를 감사하여 자사가 보유한 중요한 데이터의 종류와 그 위치를 숙지합니다.
- ☐ 중요한 데이터는 암호화(최소한)하고, 분할하며 RBAC를 사용해 액세스를 제공하고, 정기적으로 키를 변경합니다. 키 유지 관리를 클라우드 제공자에게 맡기는 것과 사내에서 맡는 것 중 최선의 선택지가 무엇인지 평가하되, 키 액세스와 리스크에 대한 노출을 제한하는 키 보안 정책을 마련해야 합니다.

## Cortex로 보안 운영 강화

다들 알고 있듯이, 보안 운영은 사람과 프로세스, 기술의 균형을 미세하게 조정하여 실행해야 합니다. 이를 위해 SOC를 염두에 두고 특별히 제작한 완벽한 보안 솔루션 제품군을 소개하고자 합니다.

Cortex 포트폴리오는 보안 운영 전반에 걸쳐 탐지와 운영 효율을 강화하는 데 유리한, 전체적인 보안 솔루션입니다. 여기에 쓰이는 기술은 Palo Alto Networks SOC는 물론 전 세계 수천 가지 SecOps의 기반 기술입니다.

**Cortex XDR** 중요한 엔드포인트를 보호하고 전사적으로 네트워크, 클라우드, 엔드포인트는 물론 사실상 모든 데이터 소스에서 위협을 탐지하고 이에 대응하여 조직을 공격으로부터 안전하게 지킵니다. 특허받은 행동 및 머신 러닝 기반 분석으로 은밀한 위협을 찾아내고 보안 침해가 발생하기 전에 대응에 필요한 인텔리전스를 제공합니다. 공격이 발생한 뒤에 결론을 도출할 것이 아니라, 침해가 발생하기 *전에* 미리 차단하세요.

**Cortex XSOAR** SOC가 인시던트를 관리할 단일 플랫폼을 제공하며 워크플로를 자동화하여 운영 효율을 극대화합니다. 체크리스트에 기재된 프로세스 중 수동이고 반복적인 작업은 무엇이든 자동화 후보가 될 수 있습니다. XSOAR는 900여 가지 사전 구축한 자동화 팩을 통해 사용자 액세스 제어, 피싱 대응, 취약점 관리, 클라우드 보안 등 주요 프로세스에 맞출 수 있으므로 SOC의 가상 파트너 역할을 하며 인시던트 대응 속도를 높이고 일상적인 애널리스트 워크로드 부담을 덜어줍니다.

**Cortex Xpanse** 클라우드는 항상 변화한다는 점을 잘 알고, 보안 간극을 드러냅니다. 빈틈이 하나만 발각되어도 공격자가 네트워크를 침해할 수 있습니다. Xpanse는 공격 표면을 끊임없이 모니터링하여 인터넷에 노출된 클라우드 자산과 구성 오류에 대한 최신 인벤토리를 제공합니다. 공격자보다 먼저 섀도 IT를 찾아내세요.

SOC 팀은 전체적인 네이티브 통합과 상호 운용성 덕분에 Cortex Ecosystem 내에서 지속적 시너지 효과로 위협을 완벽히 방어할 수 있습니다. 세 가지 제품은 모두 함께 사용할 수 있으며, 위협 동향을 모니터링하고 가장 안정적인 탐지, 대응, 조사 기능을 제공합니다.

- Cortex XDR과 Xpanse는 원격 근무자를 포함한 인터넷 공격 표면, 엔드포인트, 클라우드, 네트워크에서 최고의 가시성과 탐지 기능을 제공합니다.
- Cortex XDR은 XSOAR를 활용해 멀웨어 조사와 대응을 자동화합니다.
- Cortex Xpanse와 XSOAR을 함께 사용하면 Xpanse 자산 정보를 사용해 인시던트를 자동으로 보강하고, 새로 검색된 자산의 복구 업데이트를 자동화할 수 있습니다.
- Cortex XSOAR는 Palo Alto Networks 모든 제품 및 다른 보안 도구 수백 가지로부터 알림과 위협 인텔리전스를 수집해 인시던트 조사를 속행하고 자동 인시던트 대응을 유도합니다.

## Unit 42 MDR로 사이버 공격 상시 탐지 및 대응

Unit 42의 보안 전문가는 기업을 보호하며 쌓은 다년간의 경험을 응용해 고객 환경을 모니터링하고 의심스러운 활동을 찾습니다. Unit 42 애널리스트는 Cortex XDR을 활용해 엔드포인트, 네트워크, ID 소스에서 보안 텔레메트리 정보를 집계하여 충실도 높은 위협 인텔리전스와 AI 기반 분석을 적용해 아무리 지능적인 위협이라고 예방, 탐지하여 대응합니다.

Unit 42 MDR 팀은 독점 프로세스, 인프라와 강화 요소를 함께 사용해 탐지, 대응, 위협 헌팅 속도를 높여 고객 조직에 해를 끼칠 가능성이 있는 악성 활동을 신속하게 차단합니다.

### Unit 42 Retainer와 함께 몇 분 내로 대응 시작

보안 침해가 발견된 즉시 대응이 시작됩니다. 침해를 바로 억제하고 근본 원인을 파악하지 못하면 공격자가 다시 환경에 들어오게 됩니다.

Unit 42 Retainer를 사용하면 Unit 42 전문가가 고객팀의 일원 같은 역할을 하여, 빠른 대응을 도와 공격의 여파를 최소화하고 신속하게 비즈니스에 복귀하도록 지원합니다.

## 다음 단계 XSIAM으로 미래에 대비

Cortex 제품이 가시성, 보호, 자동화를 위한 중요한 SOC 요구 사항을 해결해주기는 하지만 대부분 조직은 여전히 SIEM을 SecOps의 핵심 구성 요소를 활용합니다. 하지만 SIEM 제품은 효과적인 집중형 위협 탐지와 대응을 제공하지 못해 애널리스트는 끝없는 알림과 수동 프로세스에 시달리게 됩니다. 보안팀에는 여러 보안 기능을 하나의 기반 솔루션으로 통합 및 자동화하고 전사적 보안 데이터를 함께 제공하는 중앙 플랫폼이 필요합니다.

확장형 보안 인텔리전스와 자동화 관리(XSIAM)는 이러한 필요성을 해결하고, AI 기반 자동화의 힘을 활용하여 보안 성과를 대폭 개선하면서도, 수동 SecOps 모델을 혁신하도록 설계되었습니다. 지능적 데이터 기반을 구축하고 통합 SOC 함수를 자동화하는 XSIAM은 대응을 가속화하고, 위협보다 한발 앞서 대응하며, 애널리스트 활동을 대폭 간소화합니다.

Cortex 제품군이 동급 최고의 위협 탐지, 예방, 공격 표면 관리와 보안 자동화 기능을 제공하는 방식을 자세히 알아보려면 다음 백서를 다운로드하세요.

Cortex로 가상 SOC 플랫폼 구축

오늘날, 미래의 SOC를 계획하는 방법

최신 사이버위협 현황에 관한 더 심층적인 정보와 공격자가 애용하는 전략을 알아보려면 Unit 42 2022 인시던트 대응 보고서를 참조하시기 바랍니다.

서울시 강남구 테헤란로 518, 10층
(위워크 삼성역 2호점, 섬유센터빌딩)
영업 문의
Tel: 82-2-568-4353 /
eMail: Sales-KR@paloaltonetworks.com
www.paloaltonetworks.co.kr


unit42_cybersecurity-checklist-57-tips_112222