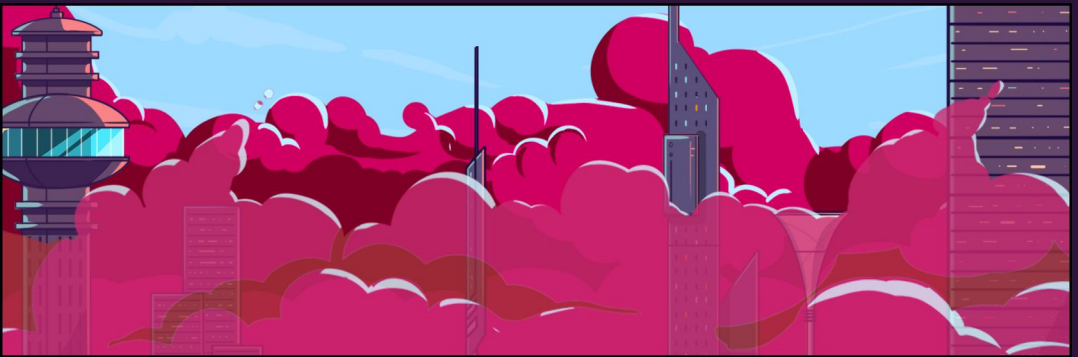
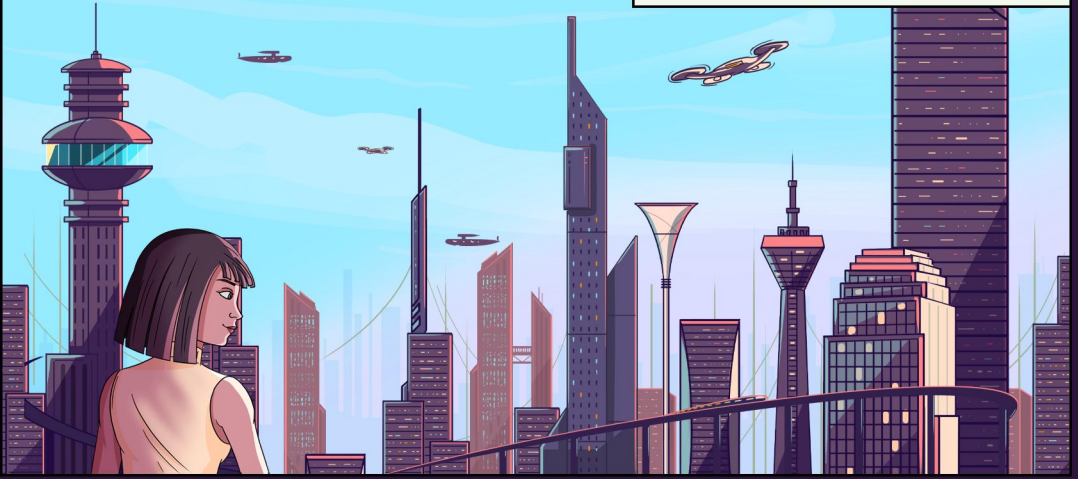




CORTEX CITY

SOC마왕 VS FUTURESOC #01권

청량하고 맑은 어느 날 아침, Cortex City는 바쁘게 일상을 보내는 시민들의 움직임으로 분주합니다.



그런데 갑자기 두꺼운 안개가 도시 전체를 둘러싸고 공격 표면을 덮습니다. 범인은 분명...



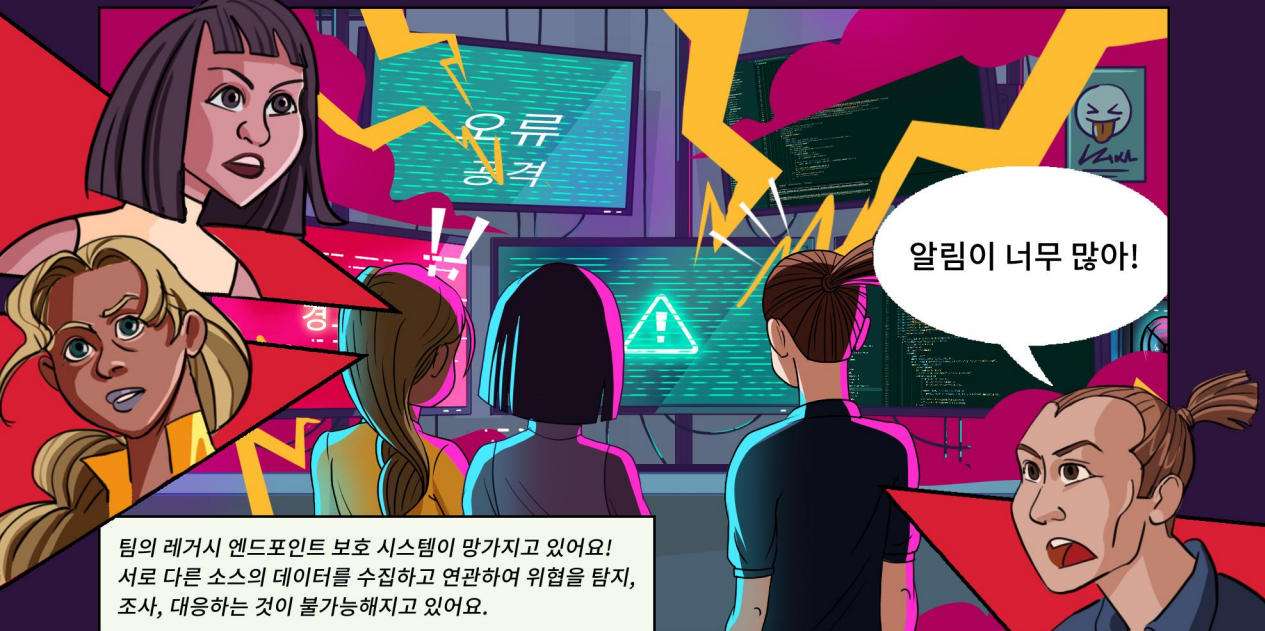
SOC 마왕



SOC마왕입니다!
SecOps 팀의 속적이죠!



왜 그래, 나시라?



알림이 너무 많아!

팀의 레거시 엔드포인트 보호 시스템이 망가지고 있어요!
서로 다른 소스의 데이터를 수집하고 연관하여 위협을 탐지,
조사, 대응하는 것이 불가능해지고 있어요.

나시라는 사이버공격 대응을 도울 수 있는 최고의 팀에게 신속히 연락합니다...

FUTURESOC,
네가 필요해!

FutureSOC 본부...

이봐,
XDR
네 차례야!

XDR은 즉시 나서서 네트워크에 침입의 흔적이 있는지 탐지하고, 공격의 소스를 곧 찾아냅니다.

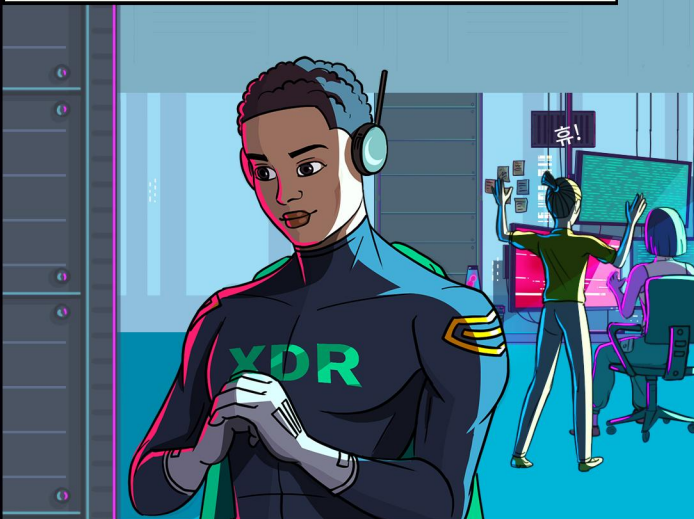
또한, XDR은 빠르게 엔드포인트를 분석해 공격 포인트를 탐지합니다. 그다음 도시 전역의 공격 포인트를 간략하게 정리해서 보여주죠. 마지막으로 연관된 엔드포인트 텔레메트리와 이벤트 데이터를 BigTech Inc.로 보냅니다.



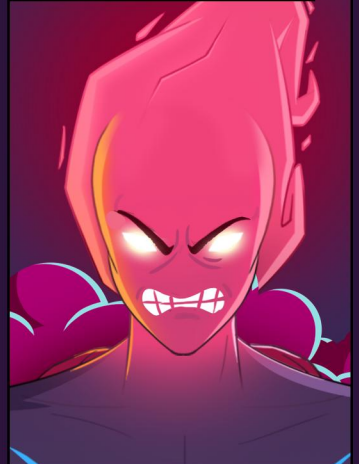
XDR이 위협을 탐지하고, 조사하고, 대응하고, 또한 위협을 추적함으로써 강하게 반격했습니다!



굉장한 탐지 능력과 대응 능력, 그리고 클라우드 환경 스케일링 능력으로 나시라의 팀이 공격을 물리치는 데 필요한 정보를 쫓네요!



하지만 SOC마왕은 만만한 상대가 아닙니다! 도시의 일부가 아직도 스며드는 안개 속에 묻혀 있습니다...



나시라와 XDR은 더 튼튼한 보안을 위해 FutureSOC 팀에 연락합니다.



지금 갈게!



Xpanse는 SOC마왕보다 먼저 취약성을 찾아냅니다. 계속해서 에셋을 발견하고 탐지하여 위험을 사전에 완화하죠. 에셋 뷰를 아웃사이드 인 매핑과 교차 연관 시키고...



모든 정보를 흡수하여 새로운 공격에 대한 노출과 공격의 진행 과정을 이해합니다. 안개가 거의 박멸되었습니다!



XSOAR가 도착해 Xpanse의 마무리를 돕습니다!

XSOAR





터보차지
조사 & 대응

미래 사건 자동 대응

수동 작업 자동화

조직 전역에서
액션 구성

SOC
도구와
호환성 우수

눈 깜짝할 새에 XSOAR는 나시라의 도구로부터
알림을 추출해 엔드포인트, 유저, 호스트, 취약성,
멀웨어, 공격자 자료에 관한 정보에 액세스하고 즉시
격리를 실행합니다.

XSOAR가 안개를 퇴치합니다! 공격 표면
전체가 드디어 감소되고 확보되어 나시라의
팀이 완전한 뷰를 볼 수 있습니다!

활성화



수익



SOC마왕의 공격이 저지되고 다시 평화가 찾아오자, XSOAR는 나시라와 팀의 시스템에 자동화를 더하여 서플라이 체인, 네이션 스테이트, 제로 데이 공격을 막는 방법을 가르쳐 줍니다.



FutureSOC 팀은 AI와 머신러닝을 활용하여 나시라의 팀이 수신하는 알람을 우선화하고 워크플로우를 간소화하여 복구과정을 단축하는데 도움을 줍니다.

그 성공의 비밀은 Cortex의 정교한 제품 스위트였습니다. 엔드포인트 보안, 탐지, 대응, 자동화, 공격 표면 관리 기능 덕분에 나시라와 팀은 바쁜 업무에 보내는 시간을 줄이고 야근과 주말 근무도 필요가 없어졌습니다!



결과

네트워크, 클라우드, 신원 데이터에 대한 단일 진실 공급원과 인터넷에 노출된 에셋 위험도 파악을 통해 위협을 정확하게 탐지하여 나시라와 팀은

SOC마왕의 찾기 힘든 공격을 탐지하고 SOC의 힘을 최대한 발휘해 대응할 수 있었습니다.



보안 사건에 대한 완전한 가시성과 조직화된 대응을 통해 여러분도 네트워크와 에셋을 사전에 방어하고 보호하여 장밋빛 미래를 누릴 수 있습니다.

지금 바로 Cortex와 함께 미래의 SOC를 향한 여정을 시작하여 클라우드 네이티브 세계의 변화하는 요구에 발맞추세요.

이야기를 모두 확인하셨다면 바로 다음 데모를 요청하세요.

www.paloaltonetworks.co.kr/cortex/request-demo

