PLURA-XDR, 국가안보의 최전선에 서다

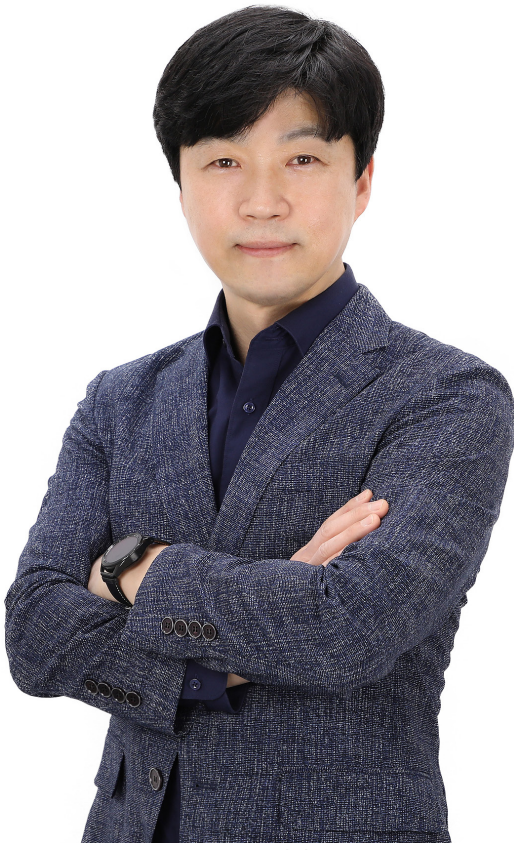
현대전의 중심에 선 정보전쟁

우크라이나와 러시아 간의 전쟁은 국가 안보가 더 이상 전통적인 군사력에만 의존하지 않는다는 중요한 교훈을 남겼다. 정보전이 현대전쟁의 중심에 서면서, 정보보안의 중요성이 점점 더 커지고 있는 것이다. 이제 국방과 외교 분야에서는 최신 기술과 도구를 활용해 정보전에서의 우위를 확보하는 것이 필수적인 일이 되었다.

우크라이나-러시아 전쟁을 통해 사이버전의 중요성도 명확히 드러났다. 이 전쟁은 사이버 공간에서의 공격과 방어가 국가 안보와 전쟁의 승패에 얼마나 결정적인 영향을 미칠 수 있는지를 보여주었다.

사이버 공격은 정부와 군사기관의 통신 시스템 마비, 중요 인프라 공격, 정보 유출, 가짜 뉴스 확산 등 다양한 형태로 나타났다. 이러한 공격들은 전쟁의 양상을 변화시키고 전통적인 전쟁 방식과 결합하여 상대방에게 심각한 타격을 입힐 수 있다. 이에 따라 사이버 보안의 중요성이 강조되고 있는 것이다.

러시아가 독일의 공격을 인정하는 녹음 파일을 공개한 사례는 정보전쟁의 위험성과 전략적 의미를 드러내며, 특히 동맹국들 사이의 불신을 조성하고 분열을 유도하는 전략적 의도를 포함하고 있다.



신승민 큐비트시큐리티(주) 대표이사

단일 정보보안 제품 다단계구축전략, 한계에 직면하다

단일 정보보안 제품의 다단계 구성은 네트워크 기반 정보보안 제품의 암호화된 패킷 분석 불가능성, 웹방화벽의 우회 공격 취약성, 통합보안이벤트관리(SIEM) 시스템의 정보 부족으로 인한 탐지 신뢰성 확보 어려움 등 여러 한계에 직면해 있

다. 이러한 문제를 해결하기 위해 PLURA-XDR이 있다.

PLURA-XDR은 첨단 웹공격, 서버 및 PC 공격 감지 기술에 빅데이터 분석, 인공지능을 결합해 실시간으로 위협을 탐지하고 대응한다. 이 시스템은 호스트 보안, 웹방화벽, 통합보안이벤트관리, 리소스 모니터링, 보안운영 자동화를 통합해 공격 탐지 및 대응을 자동화한다. PLURA-XDR은 다음과 같은 주요 특징을 제공한다.

● **선제적 대응** : 웹, 서버, PC 공격을 즉각 감지하고 빠르게 대처하여 공격 전에 대응한다.

● **제로데이 공격 대응** : 아직 알려지지 않은 보안 취약점을 대상으로 한 공격을 빅데이터 분석으로 미리 파악하고 대처한다.

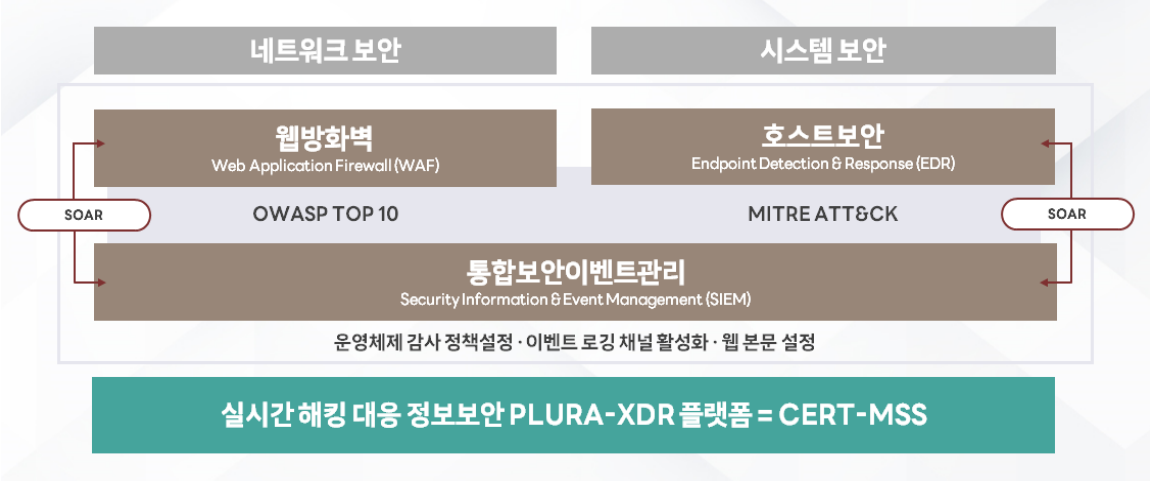
● **웹 취약점 공격 대응** : 웹사이트가 공격받을 때 필요한 정보를 수집하고 분석하여 공격을 방어한다. 특히 요청본문(Post-body)과 응답본문을 분석하여 대응하는 방식은 세계적인 특허기술로, 이 과정에서 웹사이트 공격을 차단하는 데 필요한 조치를 취하게 된다.

● **PC 공격 대응** : 이메일이나 다른 경로를 통해 시도되는 해킹 공격을 분석하고 방지한다. 사용자의 행동 분석을 기반으로 해킹 시도를 감지하고 대응하여 PC를 보호한다.

● **실시간 감지 및 대응 기능** : 모든 유형의 공격에 즉각적으로 대응. 이를 통해 발생하는 위협을 실시간으로 감지하고 자동화된 방식으로 적극적으로 대처할 수 있다.

● **고급 분석 기능** : 마이터 어택(MITRE ATT&CK) 등 최신 분석기술을 활용하여 복잡한 공격 패턴을 식별하고 예측한다. 이 기능은 보다 복잡한 위협에 대한 이해를 높이고, 예방 조치를 개선하는 데 도움을 준다.

PLURA-XDR은 위와 같은 기능을 바탕으로 국가 안보에 있어 필수적인 도구일 뿐만 아니라 안보를 한 단계 더 강화하는 중요한 역할을 제공한다. KDDJ



큐비트시큐리티(주)의 PLURA-XDR 플랫폼 구성