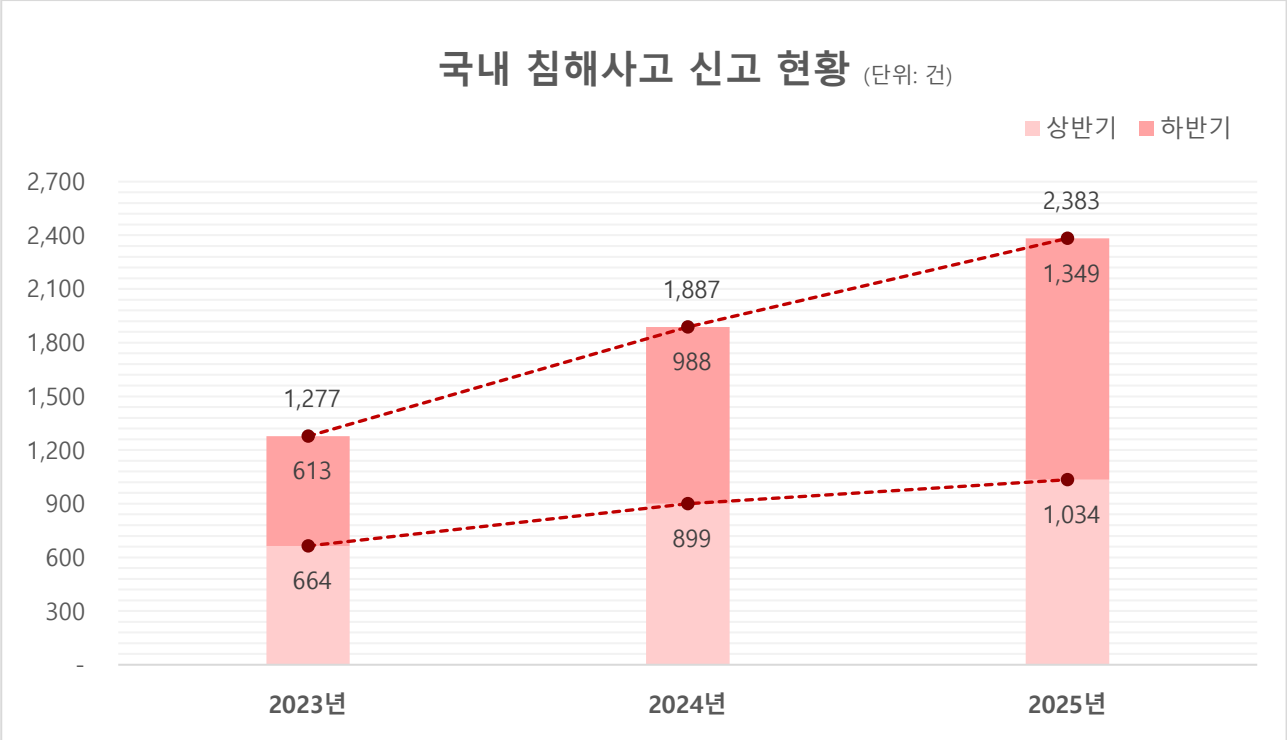
Headline

선제적 보안과 레드팀 기반 사이버 면역 체계 구축 전략

EQST 전략사업팀 이건희 선임

■ 사이버 보안을 위한 두가지 패러다임, 선제적 보안과 사이버 복원력

디지털 전환이 가속화되고, AI 기술이 고도화됨에 따라 사이버 공격은 더욱 정교하고 지능적인 양상으로 진화하고 있으며, 이에 따라 침해사고 발생 빈도 역시 해마다 증가하고 있다. 2023 년부터 2025 년까지 국내 침해사고 신고 건수는 각각 1277 건, 1887 건, 2383 건으로 늘어나고 있으며, 이러한 추세는 앞으로도 지속될 것으로 예견된다.



출처 : 과학기술정보통신부·한국인터넷진흥원

그림 1. 국내 침해사고 신고 현황(2023 년~2025 년)

지금까지 사이버 보안의 초점은 위협 발생 이후 이를 탐지하고 대응하는 것에 맞춰져 왔으며, 침해사고 발생시 스트레스를 최소화하고, 신속한 복구를 통해 업무의 연속성을 확보할 수 있는 역량인 사이버 복원력(Cyber Resilience)의 중요성이 강조돼 왔다.

하지만 피해를 최소화하려는 노력만으로는 충분치 않다. 사고 발생 이후에 행동하는 보안 체계에서는 침해사고가 빈번해질수록 피해 규모와 복구 비용이 비례하여 증가할 수밖에 없기 때문이다. 또한 침해사고의 발생은 그 자체로도 조직의 평판을 감소시키며, 이는 결국 고객 이탈과 매출 감소로 이어져 장기적인 악영향을 끼치게 된다.

최근에는 사이버 공격이 현실화되기 전에 잠재적 취약점과 침투 경로를 사전에 식별·보완함으로써 침해사고 발생 가능성을 최소화할 수 있는 '예방' 중심의 사이버 보안 전략인 선제적 보안(Preemptive Cybersecurity)이 새로운 패러다임으로 주목받고 있다. 가트너는 2026 년 10 대 기술 전략 트렌드 중 하나로 선제적 보안을 꼽았으며, 2030 년까지 선제적 보안을 위한 지출이 전체 보안 지출의 절반 수준까지 확대될 것으로 전망하고 있다.

선제적 보안과 사이버 복원력은 각각 공격적 성격과 방어적 성격을 지니고 있어 서로 상반된 개념으로 보일 수 있지만, 이들을 완전히 분리해서 바라보는 시각은 올바르지 않다. 선제적 보안 중심의 공격적 보안 전략은 위협을 최소화할 수는 있지만 완전히 제거하기란 현실적으로 어려운 반면, 사이버 복원력 중심의 방어적 보안 전략은 피해를 최소화하고 재발을 방지할 수 있지만 예상을 벗어난 위협을 사전에 대비하기는 어렵기 때문이다.

구분	선제적 보안	사이버 복원력
관점	공격자 관점	방어자 관점
목적	위협 예측 및 사전 차단(예방)	신속한 공격 탐지와 복구(탐지 및 대응)
장점	침해사고 발생 가능성 최소화 가능	침해사고 발생에 따른 피해 최소화 가능
단점	위협의 완전한 제거 어려움	예상하지 못한 위협에 대비하기 어려움

표 1. 선제적 보안과 사이버 복원력의 차이점

이제는 이 두 가지 패러다임을 상호 보완적으로 결합해 나가야 한다. 이러한 접근 방식을 통해 조직은 사이버 공격에 유연하게 대처할 수 있을 뿐만 아니라, 침해사고 발생 가능성 자체를 최소화함으로써 전방위적 사이버 면역체계를 갖출 수 있을 것이다.

■ 선제적 보안을 위한 보안 조직, 레드팀

아직까지는 국내에서 '레드팀(Red Team)'이라는 개념이 다소 생소한 것이 사실이다. 그럼에도 불구하고 최근 대기업을 중심으로 레드팀을 도입하려는 움직임이 확산되고 있으며, 많은 매체에서는 선제적 보안을 현실화하기 위한 방안으로 레드팀 도입을 언급하고 있다.

물론 레드팀이 선제적 보안을 위한 핵심 요소인 것은 분명하다. 하지만 레드팀이 무엇이고 어떤 활동을 하며, 어떻게 운영해 나가야 하는지를 이해하지 못한 채 도입만 서두르게 된다면 레드팀 도입이라는 선택이 자칫하면 선제적 보안 체계를 갖추고 있다는 느낌만 주게 되는 '보안 극장(Security Theater)'으로 전락할 수도 있음을 간과해서는 안된다.

레드팀을 한줄로 정의하자면, "공격자의 사고(Adversarial Thinking)"를 기반으로 현재 조직의 공격 표면(Attack Surface)에서 발생 가능한 위협을 사전에 식별하고, 취약성을 보완하기 위한 현실적인 방향성을 제시하는 보안 조직"이다.

레드팀은 컴플라이언스 대응을 위한 취약점 진단(Vulnerability Assessment)뿐만 아니라, 침투 테스트(Penetration Test), 피싱 캠페인(Phishing Campaign), 물리적 보안 테스트(Physical Security Test) 등 기술적·관리적·물리적 공격 표면(Attack Surface)에 대한 보안 활동을 수행하며, 운영 주체에 따라 인하우스(In-house)형태의 레드팀과 아웃소싱(Outsourcing)형태의 레드팀으로 분류할 수 있다.

먼저 인하우스 레드팀은 조직 내부에서 상시적으로 운영되는 팀으로, 조직 내부 시스템과 비즈니스 프로세스에 대한 깊은 이해를 보유하고 있다. 이들은 조직의 내부 구성원으로 구성되며 외부에 공개하기 민감한 시스템에 대한 보안 점검이나 타 부서와의 긴밀한 협조가 필요한 보안 활동 등 높은 신뢰도가 요구되는 과업을 효과적으로 수행할 수 있다. 하지만 이들은 조직 내부의 문화나 의사결정 구조에 영향을 받기 쉬워 편향이 발생할 가능성이 있고, 외부자 시각에서의 비판적 접근이 어려울 수도 있다는 한계점이 존재한다.

반면 아웃소싱 레드팀은 조직 외부의 전문가 집단으로 이루어져, 장기 또는 단기 프로젝트 성으로 운영된다. 이들은 다양한 고객과 산업군을 대상으로 한 풍부한 수행 경험과 실전형 침투 전략을 바탕으로 외부자 관점에서 조직의 보안 체계를 객관적으로 평가할 수 있다는 장점이 있다. 하지만 아웃소싱 레드팀은 외부 인력으로 구성되기 때문에 보안 활동 수행 과정에서 획득한 인사이트를 조직에게 내재화하기 위한 지식 이전이 불완전할 수 있으며, 인하우스 레드팀에 비해 신뢰하기 어려울 수 있다는 단점도 있다.

구분	인하우스 레드팀	아웃소싱 레드팀
구성	내부 직원	외부 전문가
장점	높은 조직 이해도와 신뢰성 보유	실전형 침투 전략과 창의적 시각 보유
단점	편향 발생 가능, 비판적 접근 어려움	지식 이전 불완전, 비교적 낮은 신뢰도

표 2. 인하우스형 레드팀과 아웃소싱형 레드팀의 차이점

레드팀 도입을 고려하고 있다면, 조직의 보안 성숙도를 충분히 고려하는 것이 중요하다. 체계적인 보안 운영 환경이 확보되지 않은 상태에서는 레드팀의 도입 효과를 극대화하기 어려우며, 보안 역량이 충분히 성숙하지 않은 조직에는 레드팀 도입이 오히려 비효율적인 보안 지출 요인으로 작용할 수 있기 때문이다.

만약 조직의 보안 성숙도가 낮거나 자체적으로 평가하기 어려운 상태라면 아웃소싱 레드팀 서비스를 통해 공격 표면 관리 역량을 강화한 뒤 인하우스 레드팀을 도입하는 것이 좋다.

반면, 보안 성숙도가 높으며 이미 인하우스 레드팀을 운영중인 조직이라면 아웃소싱 레드팀을 보다 적극적으로 활용할 수도 있다. 앞서 설명했듯이 아웃소싱 레드팀은 외부 전문가로 이루어져 내부 조직이 가진 지식적 한계를 보완할 수 있다. 이에 입각하여 아웃소싱 레드팀 활동을 통해 최신 위협 동향과 공격 트렌드를 반영한 위협 시나리오를 도출하고 인하우스 레드팀은 이를 조직의 환경과 운영 특성에 맞게 최적화하는 하이브리드 형태의 레드팀을 운영하게 된다면 레드팀 활동의 효율을 크게 향상시킬 수 있을 것이다.

■ 레드팀의 구성과 역할

레드팀은 역할과 책임에 따라 리더(Leader), 오퍼레이터(Operator), 그리고 엔지니어(Engineer)로 구성할 수 있다.

레드팀 리더는 레드팀 활동을 총괄하며, 기술적 실행보다는 주요 이해 관계자들과의 소통과 전략적 의사결정에 집중하는 관리자의 역할을 담당한다. 리더는 레드팀 활동이 원활하게 수행될 수 있는 기술적·문화적 환경을 조성하고, 레드팀과 이해관계자들이 효과적으로 소통할 수 있도록 지원해야 한다. 이에 따라 리더에게는 전략적 사고, 팀 관리 능력, 협력적 사고방식과 효과적인 커뮤니케이션 스킬이 필수적으로 요구된다.

레드팀 오퍼레이터는 레드팀 활동의 최전선에서 리더의 지시 아래 실제 공격 테스트를 수행하는 역할을 한다. 오퍼레이터는 모의 공격의 전 과정에 걸친 실제 공격자들의 TTPs(Tactics, Techniques, Procedures)를 정확히 이해하고, 조직의 보안 상태에 가장 적합한 공격을 수행할 수 있어야 한다. 그렇기 때문에 이들에게 가장 중요시되는 역량은 깊이 있는 오펜시브 시큐리티(Offensive Security) 지식과 네트워크 및 데이터 분석 능력이다. 뿐만 아니라 이들은 수행 결과를 이해관계자들이 이해하기 쉽게 설명하거나 문서화할 수도 있어야 하기 때문에 소프트 스킬도 이들이 보유해야 할 중요한 역량 중 하나다.

레드팀 엔지니어는 팀의 규모에 따라 오퍼레이터가 겸하는 경우도 있다. 이들은 레드팀 오퍼레이터가 실전에서 활용할 수 있는 공격 툴을 개발하고, C2(Command & Control) 프레임워크와 같은 공격자 인프라를 설계·구축하는 핵심 개발 전문가다. 이들은 조직의 방어 체계를 넘어설 수 있는 정교한 침투 도구를 반복적으로 개발할 수 있어야 하기 때문에, 매우 높은 수준의 개발 능력과 오펜시브 시큐리티 지식이 필수적으로 요구된다.

역할	필요 역량
레드팀 리더	전략적 사고, 팀 관리 능력, 협력적 사고 방식 및 커뮤니케이션 스킬
레드팀 오퍼레이터	오펜시브 시큐리티 지식, 네트워크 및 데이터 분석 능력
레드팀 엔지니어	오펜시브 시큐리티 지식, 높은 수준의 개발 능력

표 3. 레드팀 구성원 별 필요 역량 예시

■ 레드팀 활동 수행 절차

레드팀 활동 수행 절차는 계획(Planning)과 수행(Execution), 보고(Reporting) 세 가지 단계로 구분할 수 있다.

레드팀 활동 착수를 위한 첫 번째 과정인 계획 단계에서는 레드팀 리더와 이해관계자들간의 사전 미팅을 통해 목표와 정의, 성공 기준 등 레드팀 활동 계획 수립을 위한 제반 사항에 대한 협의가 이루어지며, 이 과정에서 레드팀과 이해관계자 모두가 준수해야 할 일종의 수행 지침인 교전 규칙(Rules of Engagement, ROE)에 협의사항을 빠짐없이 기록하게 된다.

미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)의 NIST 800-115 가이드에서는 ROE 템플릿에 포함되어야 할 내용들을 아래와 같이 정의하고 있다.

항목	내용(예시)
Purpose	문서의 목적, 보안 테스트 대상 조직, 실행 조직, 목표
Scope	테스트 범위 및 유형, 제외 범위 및 산출물
Assumptions and Limitations	제약사항과 가정사항
Risks	내재적 위험 및 완화 기법
Document Structure	ROE 문서의 구조
Personnel	보안 테스트와 연관된 모든 조직과 인원 목록
Test Schedule	테스트 스케줄과 마일스톤
Test Site	테스트가 허가된 장소, 제한 구역
Test Equipment	보안 테스트에서 사용될 하드웨어, 소프트웨어, 미 허가 장비
General Communication	의사 소통 계획(일정, 장소, 주기 등)
Incident Handling and Response	사고 대응 및 복구 절차
Target System/Network	테스트 대상(시스템과 네트워크 대역 등)
Nontechnical Test Components	비기술적 테스트 활동(인터뷰, 리뷰 등)
Technical Test Components	기술적 테스트 활동(네트워크 스캔, 정보 수집, 침투테스트 등)
Data Handling	테스트 데이터 수집, 저장, 전송, 파기 방법과 절차
Reporting	보고서 요구사항, 보고 주기
Signature Page	이해관계자 및 조직 고위 경영진(CSO, CISO, CIO) 서명

출처 : 미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)

표 4. ROE 항목 예시

ROE 작성과 서명이 완료되면 작성된 내용을 준수하여 레드팀 활동을 수행하게 된다. 이 단계에서 레드팀 오퍼레이터는 정찰(Reconnaissance), 초기 침투(Initial Access), 실행(Execution), 지속성 확보(Persistence), 유출(Exfiltration)등 다양한 TTPs 를 활용하여 목표를 달성하기 위한 모의 공격을 수행하게 된다. 또한 레드팀 엔지니어는 이 과정에서 오퍼레이터와 협업하며 효과적인 목표 달성을 위해 지원한다.

수행 과정에서 가장 핵심적인 요소 중 하나는 바로 오퍼레이터 로그(Operator Log) 기록이다. 오퍼레이터 로그는 모의해킹 과정의 투명성과 재현성, 후속 분석을 위한 핵심 산출물로, 타임스탬프와 행위자, 이벤트 유형, 결과 등의 내용이 포함된다.

만약 수행 과정에서 보안 체계가 견고하여 초기 침투가 불가능하다고 예상될 경우, 레드팀 리더의 판단과 ROE 에 작성된 예외 처리 절차에 따라 조직의 특정 자산(내부 서버 또는 계정 등)이 이미 침해되었다고 가정하고 후속 공격(Post-Exploitation)을 집중적으로 테스트하는 침해 사고 가정 시나리오(Assumed Breach Scenario) 형태로 전환하여 진행할 수도 있다.

필드	값
Timestamp	20260118_121411
Source	10.10.10.22
Destination	192.168.1.12
Target	TARGET-LINUX01
Event Type	Active Scanning
Command	nmap -sT -Pn 192.168.1.12
Result	Ports: 80/open, 443/open, 8443/open

표 5. Operator Log 예시

모든 테스트가 종료되면 레드팀 리더는 오퍼레이터의 활동 결과를 분석하고 개선 사항을 정리하여 보고서를 작성한다. 보고서에는 일반적으로 경영진을 위한 핵심 요약(Executive Summary)부터 식별된 취약점과 성공한 위협 시나리오, 위협 평가 결과와 함께 탐지 및 대응 성과를 정량적으로 표현할 수 있는 핵심 성과 지표(Key Performance Indicator)가 반드시 포함되어야 한다.

항목	내용(예시)
ASR(Attack Success Rate)	전체 공격 횟수와 성공한 공격 횟수에 따른 성공률
Detection Coverage	전체 공격 횟수와 탐지된 공격 횟수에 따른 탐지 비율
MTTC (Mean Time to Compromise)	공격 시작부터 목표에 침투를 성공할 때까지 걸린 시간
MTTD (Mean Time to Detect)	공격자가 침투한 시점부터 이를 탐지할 때까지 걸린 시간
MTTR (Mean Time to Respond):	침투 탐지 후 대응 완료할 때까지 걸린 시간

표 6. 핵심 성과 지표(KPI) 예시

보고서 작성이 완료되면 경영진과 운영팀, 탐지와 대응을 담당하는 블루팀(Blue Team) 등 이해관계자들에게 이를 배포하고, AAR(After Action Review) 또는 디브리핑(Debriefing) 세션을 개최하여 레드팀 활동을 리뷰한다. 이후 조직에서는 확인된 취약 사항에 대한 보완 조치를 진행하게 되며, 조치가 완료되면 조치 여부를 재 검증하기 위한 후속 활동인 이행 점검(Remediation Verification)을 진행하는 것으로 레드팀 활동이 마무리된다.

■ 침해 및 공격 시뮬레이션을 통한 레드팀과 블루팀의 통합

레드팀 활동은 대부분 공격 행위가 단발성으로 이루어진다. 하지만 만약 위협 시나리오를 반복적으로 테스트할 수 있다면 블루팀은 위협 시나리오에 대한 탐지 능력이나 대응 속도를 점진적으로 향상시킬 수 있을 것이다.

침해 및 공격 시뮬레이션(Breach and Attack Simulation, BAS)은 이러한 한계점을 극복할 수 있는 레드팀 활동으로, TTPs 단위로 구분된 위협 시나리오를 반복적으로 시뮬레이션 할 수 있도록 구조화하고 필요에 따라 이를 재시뮬레이션하는 방식으로 진행된다.

BAS 는 위협 시나리오를 반복해서 테스트할 수 있기 때문에, 침해사고 사후 검증 목적으로도 활용할 수 있다. 만약 조직에서 침해사고가 발생했다면 사고 원인을 분석하고 재발 방지를 위한 대책을 수립할 것이다. 이때 재발 방지 대책이 적용된 이후 BAS 를 활용하여 침해사고 시나리오를 시뮬레이션한다면, 적용된 보안 대책의 실효성을 평가할 수 있을 것이다.

BAS 는 앞서 설명한 레드팀 활동 이행 점검과 같이 수동으로 진행할 수도 있지만, 자동화 BAS 플랫폼을 도입한다면 점검 과정을 완전히 자동화할 수 있어 생산성을 극대화시킬 수 있다. 대부분의 자동화 BAS 플랫폼들은 다양한 보안 시스템들과 연동할 수 있는 기능과 탐지 성공률, 대응 시간 등의 핵심 지표를 실시간으로 파악할 수 있는 직관적인 인터페이스를 제공한다. 이는 곧 조직이 SOC(Security Operations Center)나 MSSP(Managed Security Service Platform)/MDR(Managed Detection and Response)을 고도화하는 데에도 큰 힘이 되며, 경영진은 이를 참고하여 ROI(Return on Investment)를 측정하거나 전략적인 의사결정을 내리는 데 도움을 받을 수도 있다.

이처럼 BAS 를 활용하면 선제적 보안과 사이버 복원력, 레드팀과 블루팀을 효과적으로 통합할 수 있다. 레드팀은 발생 가능성이 존재하는 위협 시나리오를 도출한 뒤 BAS 를 통해 시나리오를 구조화하고 반복적인 시뮬레이션 환경을 구축한 뒤, 블루팀은 이를 통해 탐지·대응 체계를 개선해 나간다. 그리고 이러한 과정을 반복함으로써, 레드팀과 블루팀이 통합된 퍼플팀(Purple Team) 운영체계를 구축해 나갈 수 있을 것이다.

그림 2. 지속적 공격 검증 절차

하지만 이면에는 현실적인 어려움 또한 존재한다. 레드팀은 위협 시나리오의 현실성을 검증하기 위해 적극적이고 실험적으로 접근하고자 하는 성향이 강한 반면, 블루팀은 실시간 보안 모니터링, 탐지와 사고 대응 등 운영의 안정성과 연속성 유지에 초점이 맞춰져 있어 보수적인 성향이 강하다. 따라서 블루팀은 레드팀의 공격 시나리오가 실제 운영 환경에 영향을 미칠 수 있다는 우려로 정보 공유와 협력을 주저하기도 하는데, 이러한 구조적 차이가 두 팀의 통합을 어렵게 하는 주요한 원인이다.

이러한 어려움을 해결하기 위해서는 경영진의 강력한 의지와 주도적인 움직임이 필요하다. "보안의 사각지대를 확인하고 개선하는 것이 우리의 목적"이라는 메시지를 조직 전반에 명확히 전달하고, 레드팀과 블루팀 협업을 적극적으로 지원하는 문화가 조성되어야 한다. 물론 단기간에 완벽한 협업 환경을 구축하기는 어려울 수 있지만 단계적인 접근과 지속적인 노력을 통해 이를 실현해 나가는 것이 바람직하다.

■ 맺음말

흔히 서로 정반대에 서 있다고 여겨지는 것들이 실제로는 서로를 보완하며 더 강한 조화를 이루는 경우가 많다. 예를 들어, 바람과 돛의 관계가 그렇다. 바람은 배를 흔들고 방향을 바꾸게 하지만, 돛이 없다면 그 어떤 배도 앞으로 나아갈 수 없다. 바람이 위협처럼 보여도 돛과 함께할 때는 추진력이 된다.

마찬가지로, 미리 위험을 예측하고 대비하는 '선제적 보안'과, 공격을 받아도 빠르게 회복할 수 있는 '사이버 복원력'은 서로를 밀어내는 힘이 아니다. 이들은 함께 있을 때야 비로소 조직을 올바른 방향으로 나아갈 수 있게 만들어주는 동력이 될 것이며, 이들이 조화롭게 어우러짐으로써 조직은 '예방', '탐지', '대응'이 유기적으로 연결된 사이버 면역 체계를 갖출 수 있을 것이다.

SK 쉴더스는 국내 최대 규모 화이트 해커 그룹 EQST(Experts, Qualified Security Team)를 통해 고객이 '선제적 보안' 과 '사이버 복원력'의 통합을 위해 나아가야 할 방향성을 제시할 수 있는 전문 모의해킹 컨설팅 서비스를 제공하고 있다.

EQST 는 20 여년간 공공·기업·금융·제조 등 산업군별 B2B 사업을 수행해왔으며, New ICT 분야를 선도하는 내부 연구조직에서 분석한 최신 사이버 보안 트렌드와 SK 쉴더스 통합 관제 플랫폼인 시큐디움(Secudium)의 방대한 위협 인텔리전스(Threat Intelligence, T.I)를 바탕으로 전문성과 트렌드, 노하우가 결합된 EQST 위협 시나리오 DB(EQST Threat Scenario Database)와 자체적인 모의해킹 방법론을 설계·구현하였다.

그리고 EQST 는 이를 기반으로 각종 컴플라이언스에 대응 가능한 취약점 진단 컨설팅부터 ASM(Attack Surface Management)과 모의해킹을 결합한 보안 점검 및 실전형 아웃소싱 레드팀 서비스까지 폭넓은 보안 컨설팅 서비스를 제공하고 있다. 만약 독자가 조직의 사이버 보안 성숙도 향상을 위해 '선제적 보안 전략'을 고려하고 있다면, 독자적인 전문성을 보유한 EQST 보안 컨설팅 서비스를 통해 선제적 보안을 위한 최적화된 지원을 받을 수 있을 것이다.

■ 참고문헌

[1] Gartner, "Gartner Identifies the Top Strategic Technology Trends for 2026"

[2] Gartner, "Gartner Top 10 Strategic Technology Trends for 2026"

[3] 과학기술정보통신부·한국인터넷진흥원, "25년 사이버 위협 하반기 동향 및 26년 전망"

[4] NIST, "Technical Guide to Information Security Testing and Assessment"