JBS Cyber Security & Risk Services

JOE BLACK SECURITY
BLACK IS THE NEW RED

Red Team Security Services

Testing Your Preparedness – Exercising Your Response

고객의 대비책을 점검

해커들은 점점 더 영악해지고, 그들의 전략들은 더 진보하고 진화하며 당신의 내부 보안 팀보다 훨씬 더 많은 자금을 지원받습니다. 이런 종류의 위협에 대응하는 것은 더이상 선택이 아닙니다. 공격적인 사전 대책을 강구하는 것은 당신의 기관에 있는 사람들과 절차, 방침, 제품들만 확인하는 것에 대해서만 국한되지 않고 당신의 기관이 현실 세계의 공격에 대책을 마련하기 위해 필요합니다.

Joe Black Security는 이러한 공격의 타깃이 되는 일에 실제 위험 없이 현실 세계 공격 시나리오를 시뮬레이트하는 진보된 기술들을 제공할 수 있습니다.

RedTeam의 접근 방법은 다음과 같은 시뮬레이션을 합니다.

회사의 시설이나 직원들을 향한 물리적 사회적 공격은 민감한 데이터의 유출을 일으킬 수 있고 네트워크로 좀 더 침투해 들어갈 수 있는 전달자로써 이용될 수 있고, 사기성 전자메일에 반응하거나 악성 바이러스가 담긴 파일들을 다운로드하는 등의 행동들을 하거나 가공의 형태로 개인적인 정보를 노출시킬 수 있는 직원들에 대해 보안 의식을 테스트 합니다.

외부 네트워크와 Wi-Fi, VoIP 및 취약한 웹 APP과 같이 인터넷과 접하는 자산으로의 사이버 공격은 기관 전체의 백엔드 인프라를 노출시키기 위해 공격자로부터 착취 될 수 있으며, 공격자가 Domain Admin을 얻을 수 있도록 이끄는 내부 자산을 향한 공격은 얼마나 쉽게 귀하의 소중한 자산들이 도난당할 수 있는지를 보여줄 것입니다.

고객의 대응을 연습

RedTeam이 하는 일(=이하 Red teaming)은 단지 보안에만 국한되지 않습니다. Red teaming은 고객의 기관이 실제 모의 사건과 긴급상황에 어떻게 반응하는지, 이것이 어떤 계기가 되고 업무 연속성 계획에 어떻게 적용될 것인지, 혹은, 고객의 긴급 사태 발생에 얼마나 적절한지, 그리고 어떤 조건 아래에서 이것들이 더 실패할 개연성이 있는지와 같은 리질리언스에 관한 것입니다.

Red teaming은 기술이든 사람, 혹은 절차에 예외없이 다수의 실패 요인들을 확인할 것입니다. 이는 단계적인 위기의 발달을 예측하는 능력인 고객의 상황적인 인식을 확인할 것이며 기관의 대응 효율성과 감시, 멘토링 및 보고를 포함하는 평가를 위한 넓은 기반을 제공할 것입니다.

고객의 위험요소 완화

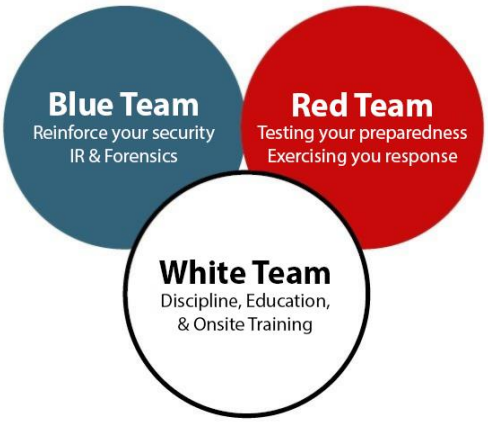
테스트 환경 내에 아직 처리되지 않은 어떤 취약점들의 즉각적인 개선을 위한 단기간의 전략적 해결책

테스트하는 동안 발견된 취약점들의 모든 잠재적인 반복을 사전 대비적으로 좌절시킬 장기간 전략적 조치

실제 상황 시나리오와 그에 따른 수행의 확실한 증거를 바탕으로 한 강력한 업계의 모범 사례와 최종 판단 리스트

일관되고 지속된 보안 위험 감시와 보안 자세 강화를 보장하는 끊임없는 보안 진단과 개선을 위한 노력의 프로그램에서의 즉각적인 대응. BLUE TEAM의 서비스를 보십시오.

JBS CYBER SECURITY & RISK SERVICES



레드팀 서비스는 다음을 포함합니다:

- ✓ 중요한 직원들로부터 오픈 소스 정보를 모으고 이 정보들을 가지고 직원들을 이용함
- ✓ JBS LeakDB 접근
- ✓ 네트워크로 더 침투하도록 강요받거나 민감한 데이터를 노출하도록 이용당할 수 있는 직원과의 타협
- ✓ 윤리적인 스피어 피싱(Spear Phishing)
- ✓ 물리적으로 기반시설에 침투하고 내부 장치와 네트워크에 접근
- ✓ 물리적 장치에 담긴 사용자 지정 악성 프로그램을 직원들에게 전달
- ✓ 경계 태도와 프로토콜을 고수하고 보안 카메라를 열거, 보도를 평가하는 등의 전반적인 물리적 보안 대책의 진단을 제공
- ✓ 대응 프로세스와 속도, 그리고 침투사건의 효과를 확인
- ✓ 다음과 같은 침투 테스트:
  - VPN 포함 인프라
  - 경영진의 거주지 포함 Wi-Fi 네트워크
  - 모바일[코드 리뷰] 포함 애플리케이션
  - IoT 장치

For more information contact us at info@joe.black

JBS Cyber Security & Risk Services

JOE BLACK SECURITY
BLACK IS THE NEW RED

Blue Team Security Services

Reinforcing Your Security – Building Your Resilience

고객의 리질리언스 구축

모든 산업을 향한 사이버 위협은 의존성 증가와 시스템의 상호연결성과 일직선을 이루며 꾸준히 증가합니다. 회사 운영이 전적으로 ICT 기술에 의존하기 시작했을 때부터, 위협의 본성과 복합성은 공격적으로 진화해왔고, 모든 분야들은 점점 더 취약해졌습니다.

나날이 높아져가는 사이버 위협의 수준은 구체적으로 보다 큰 리질리언스를 구축하기 위해 고객의 관점을 정기적인 위험요소 평가뿐만 아니라 IT와 시스템 운영에 내재된 범주의 취약점으로 몰고갑니다.

고객은 더 높은 개연성이 있는 위협요소와 빠르게 반응하는 능력, 효과적으로 작동시키는 대응조치, 그리고 업무 연속성 계획을 경감시키는데 점점 주안점을 두어야 합니다. 이는 기관 내에 대책과 리질리언스의 기본적인 수준을 구축하는 데에 많은 도움이 됩니다. Joe Black Security의 블루팀 서비스는 점점 늘어가는 정교한 위협에 직면한 고객의 보안과 리질리언스를 높힐 수 있습니다.

끊임없이 진보하고 지속되는 사이버 공격들은 정보보증이나 네트워크 보안의 영역에서 먼저 간주되지 않았던 손해를 일으킬 수 있습니다. 이런 이유로 현재의 리질리언스 개념은 잠재적으로 정보나 사이버 범죄의 무형 자산을 향해 진보되거나 융합된 위협의 높은 영향을 충분히 설명하지 못합니다.

고객의 보안 강화

블루팀은 고객이 가장 필요로 하는 곳이나 필요할 때에 보안 강화를 제공하고 고객이 이런 환경들을 위해 구상하는 것을 돕습니다. 우리 블루팀 서비스는 고객이 기대하고 집중된 위협을 경감시키기를 요구하는 다양한 지원과 결정된 상대 적수, 범죄자 혹은 테러로부터 고객의 기관의 보안 범위를 제공합니다.

고객의 물리적인 IT 보안 기능들의 효용성을 보완 및 유지하고, 폭넓은 시나리오의 범위에 대비하여 개발하고 적절한 대응과 용량복구를 제공하는 Joe Black Security는 진정으로 사이버 보안과 위험 서비스의 유일무이한 범위를 제공합니다.

고객의 위험요소 완화

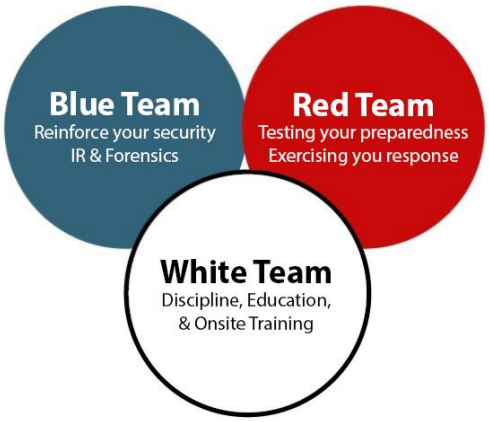
효과적인 정책과 업무를 위한 적절한 절차 및 보안 방안과 제어 어플리케이션을 도입하여 최상의 업무를 확립

설계된 시나리오와 위험요소 등록 절차를 바탕으로 한 최상의 보안인식과 위험요소 운영

보안 사고의 영향을 최소화하고 완전히 효과적인 서비스 운영으로의 빠른 복귀를 가능케 하는 진보된 온 디맨드 기능들

통합된 보안, 비시니스 연속성, 그리고 당신의 기관이 직면한 현재와 미래의 위협에 대한 우리의 특별한 이해에 기반한 집중된 위험요소 위기 대응 계획. REDTEAM의 서비스를 보라.

JBS CYBER SECURITY & RISK SERVICES



블루팀 서비스는 다음을 포함합니다:

- ✓ 보안 전략, 기획 & 컨설팅
- ✓ 보안 감사 & 진단
- ✓ 대응 & 보호 서비스
- ✓ IT Forensics와 사고 대응
- ✓ 위기 운영 자문
- ✓ 엔지니어링 & 최적화(optimization)
- ✓ 위협요소 정보 & 분석
- ✓ 위협 모델링
- ✓ 리스크 시나리오 빌딩 워크샵
- ✓ 양적 위험요소 분석
- ✓ 디지털 풋프린팅과 소셜 미디어 스위프
- ✓ 리버스 엔지니어링(Reverse Engineering)
- ✓ 어플리케이션과 인프라 디자인 리뷰
- ✓ 안전한 생활주기 개발
- ✓ DDoS 완화 진보된 사이버 방어
- ✓ 코드 리뷰
- ✓ 해외 출장 위협 인식 트레이닝