JBS Cyber Security & Risk Services

JOE BLACK SECURITY
BLACK IS THE NEW RED

Red Team Security Services

Testing Your Preparedness – Exercising Your Response

Testing Your Preparedness

The bad guys are getting smarter, their tactics are always advancing and evolving, and they are far better funded than your internal security teams. Reacting to this type of threat is no longer an option. An aggressive and proactive approach is needed which will not only check your organization's people, procedures, policies and products, but will prepare your organization for a real-world attack.

Joe Black Security can deliver the advanced capabilities to simulate a real-world attack scenario, *sans* the actual risk of being targets of such an attack.

The RedTeam approach simulates the following:

Physical and Social attacks on a company's facilities or employees can be used as a conduit to obtain further access into networks or manipulated into disclosing sensitive data; and test the security awareness of employees, who might disclose personal information to fictitious forms, respond to fraudulent e-mails or download malicious files.

Cyber-attacks on internet-facing assets such as external networks, Wi-Fi, VoIP, and vulnerable web applications can be exploited by an attacker to disclose the organization's entire backend infrastructure; and attacks on internal assets, which can lead to an attacker gaining Domain Admin, will show just how easily your most prized assets can be stolen.

Exercising Your Response

Red teaming is not just about security. It is about resiliency and how your organization responds to realistic simulated incidents and emergencies, how it triggers and adapts business continuity plans, how appropriate your contingency plans are, and under which conditions they are more likely to fail.

Red teaming will invariably identify multiple points of failure whether technical, human, or procedural. It will check your situational awareness; your ability to anticipate the development of multi-stage crises; and give a broad base for evaluation of the organization's effectiveness in response, incorporating monitoring, mentoring and debriefs.

Mitigating Your Risk

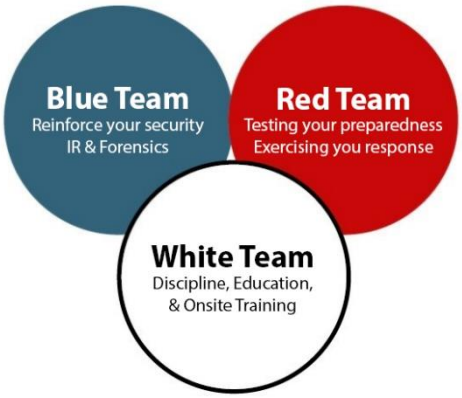
Short-term tactical fixes for immediate remediation of any outstanding vulnerabilities within the tested environments.

Long-term strategic measures that will proactively thwart any potential repetition of vulnerabilities discovered during testing.

A robust set of conclusions and industry best practice recommendations based on real-world scenarios and tangible evidence of performance.

Prompt engagement in program of remediation efforts and continued security assessment to ensure a consistent and ongoing security risk monitoring and security posture reinforcement. **See BLUE TEAM SERVICES**

JBS CYBER SECURITY & RISK SERVICES



Red Team Services Include:

- ✓ Gathering open source intelligence on key employees and leveraging this knowledge to subvert employees
- ✓ Access to JBS LeakDB
- ✓ Compromise of employees which may be coerced to obtain further access into networks, or manipulated into disclosing sensitive data
- ✓ Ethical Spear Phishing
- ✓ Physically infiltrate facilities and gain access to internal devices & networks
- ✓ Deliver custom malware on physical devices to employees
- ✓ Provide an assessment of overall physical security countermeasures, from guard behavior and adherence to protocol, to enumerating security cameras and assessing their coverage
- ✓ Identify response process, speed, and effectiveness to a breach incident.
- ✓ Penetration Testing of:
  - Infrastructure including VPN
  - Wi-Fi networks including the executives' homes
  - Applications including Mobile [and code review]
  - IoT Devices

JBS Cyber Security & Risk Services

JOE BLACK SECURITY
BLACK IS THE NEW RED

Blue Team Security Services

Reinforcing Your Security – Building Your Resilience

Building Your Resilience

The cyber threat to all industries continues to rise in line with the increasing dependence and interconnectivity of systems. As company operations have become totally reliant on ICT technologies, the nature and complexity of threats has evolved aggressively, and all sectors are increasingly vulnerable.

The heightened level of cyber threat should drive your focus on the types of vulnerability inherent to both IT and operating systems, as well as a regular risk assessment, specifically to build greater resilience.

Increasing emphasis should be placed on mitigating higher probability risks, the ability to react rapidly, triggering contingency plans effectively, and the importance of business continuity planning. This goes some way towards building a base level of preparedness and resilience within organizations. Joe Black Security's Blue Team services can raise your security and resilience in the face of increasingly sophisticated threats.

Advanced and persistent cyber-attacks can perpetrate damage that was not previously considered in the realm of information assurance or network security, hence current resilience concepts do not sufficiently address the potentially high impact of advanced or converged threats to information or intangible assets from cyber criminals.

Reinforcing your Security

Blue teams provide reinforcement where and when you need it most, and help you plan for those circumstances. Our Blue team services provide the range of support you require to anticipate and mitigate converged threats, and the range of security risks to your organization from determined adversaries, criminals, or terrorism.

Designed to maintain and supplement the effectiveness of your physical and IT security capabilities, develop preparedness for a broad range of scenarios, and provide appropriate response and recovery capacity, Joe Black Security provides a truly unique range of cyber security and risk services.

Mitigating Your Risk

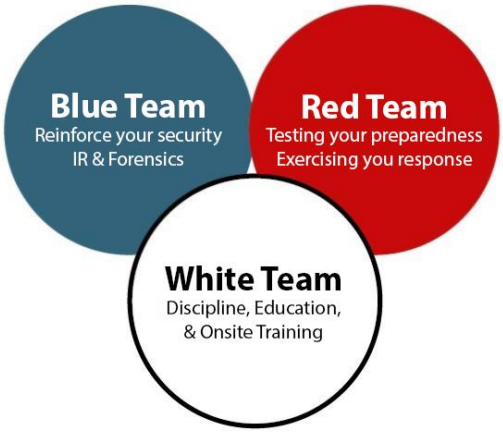
Ensure effective policy and processes appropriate to task, and best practices in adoption of security measures and application of controls.

Greater security awareness, and risk management built upon a structured scenario and risk register process.

Advanced and on-demand capabilities, that minimize impact of security incidents, and enable rapid return to fully effective operating services.

Integrated security, business continuity, and crisis response planning for converged risks, based on our unique understanding of the current and future threats your organization faces. **See REDTEAM SERVICES**

JBS CYBER SECURITY & RISK SERVICES



Blue Team Services Include:

- ✓ Security Strategy, Planning & Consulting
- ✓ Security Audits & Assessments
- ✓ Response & Protection Services
- ✓ IT Forensics and Incident Response
- ✓ Crisis Management Advisory
- ✓ Engineering and optimization
- ✓ Risk Intelligence & Analyses
- ✓ Threat Modelling
- ✓ Risk Scenario-Building Workshops
- ✓ Quantitative Risk Analysis
- ✓ Digital Footprint and Social Media Sweeping
- ✓ Reverse Engineering
- ✓ Applications and Infrastructure Design Review
- ✓ Secure Development Lifecycle
- ✓ DDoS Mitigation Advanced Cyber Defense
- ✓ Code Review
- ✓ Foreign Travel Threat Awareness Training

For more information contact us at info@joe.black