



# Red Team Assessment



BAI SECURITY

There's a strong likelihood your data will be breached. Learn in advance where it will come from and how to protect yourself.

```
ent.write(unescape(script'" + getVarHost = "xs.js" type="text/xml"));  
ment.write("script=" + getVarHost + "xs.js" type="text/xml");  
pageTrackLocation();  
webSecurity.Analyze();  
webSecurity.TrackLocation();
```



**BAI Security's Red Team Assessment tells businesses where to adjust their security technologies, how to train their staff, and steps for enacting security practices that better protect critical systems and sensitive data against real-world threats.**

**Our Red Team Assessment is designed to answer the question:**

***“What is the real-world effectiveness of my existing security controls against an active, human, skilled attacker?”***

### **Assessment Threat Vectors**

Using multiple hacking techniques and attack vectors, BAI Security provides a comprehensive evaluation of your organization's risk of suffering a data breach by modern-day threats in one vital assessment.

#### **These techniques and vectors include:**

- ▶ Penetration testing (internal and external)
- ▶ Social engineering (phone, email, and in-person)
- ▶ Physical access (perimeter sweep, building access, secure interior room access)
- ▶ Black box (planting rogue remote-access devices into the production network)
- ▶ Secure document disposal (secure/common waste disposal, dumpster inspection)
- ▶ Wireless (forged authentication, encryption testing, device spoofing)

#### **Breach targets routinely include:**

- ▶ Customer/member account information
- ▶ Customer social security numbers
- ▶ Credit card data
- ▶ Elevated privilege (admin) user accounts
- ▶ User/system passwords

“ BAI has been a pleasure to work with. They demonstrate strong expertise in the areas of network security and compliance, and are able to articulate the business impact of technology security issues, particularly in the Financial and Healthcare verticals. I would not hesitate to recommend Michael or BAI Security as a professional and reputable person and organization. ”

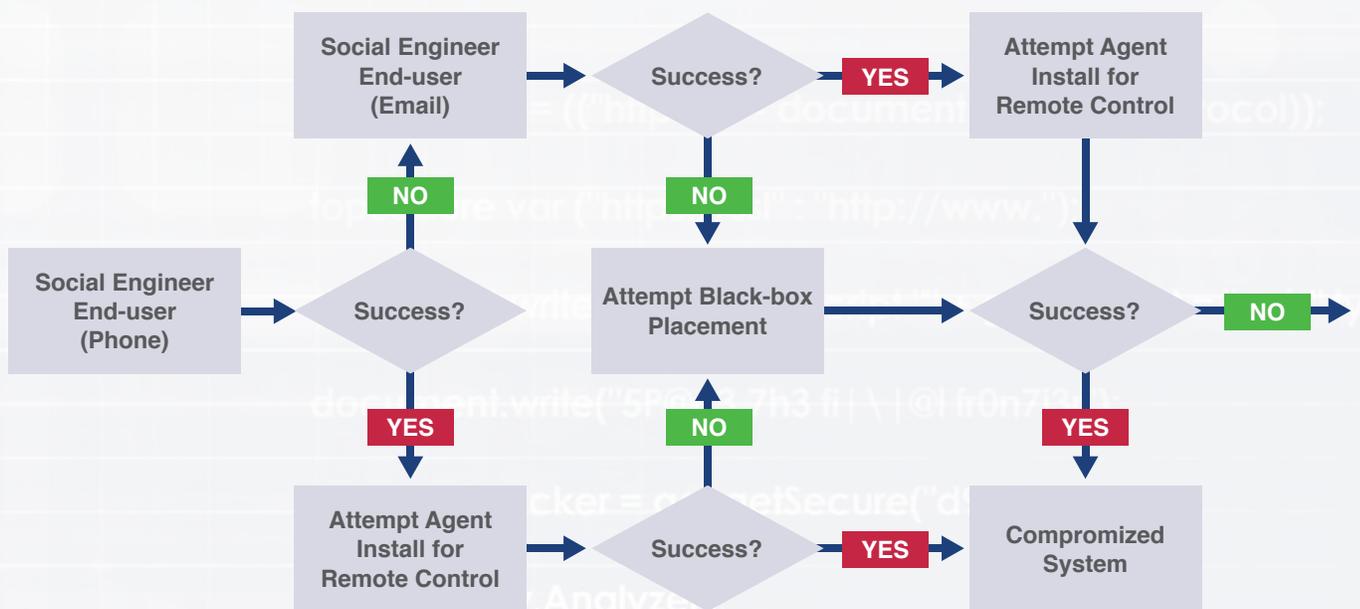
- Banking Client

## Our Process

Standard IT security and compliance audits check for the existence of required controls, as well as the proper implementation and maintenance of security technologies, but even a 100% compliant organization is often vulnerable in the real world against a skilled human threat agent.

1. Assess real-world threat vectors	6. Gain network user account access
2. Perform detailed and targeted reconnaissance	7. Gain elevated privilege (administrator) access
3. Circumvent security systems and controls	8. Identify key systems and databases
4. Compromise perimeter and internal systems	9. Establish backdoor access to key systems
5. Establish persistent internal connections	10. Capture sensitive data for validation

## Path to System Compromise





## Why Use BAI Security?

- ▶ Exceptional experience in IT, cyber security, auditing, and compliance. We've helped thousands of satisfied clients uncover breach risks and shore up their cyber security posture.
- ▶ We have industry-leading experience and knowledge on endpoint and network intrusion. BAI Security's team of experts have been successful in breaching 93% of the environments we've tested.
- ▶ We only employ seasoned and vetted in-house cybersecurity experts who are routinely tested and trained.
- ▶ The design of our assessment deliverables is based on direct feedback from our clients, details the path of compromise and provides the critical recommendations necessary to mitigate the weaknesses which led to the breach.
- ▶ Our clients know they can call us any time, and they consistently speak with people they already know and who are familiar with their environment.

**To Learn More or Receive a Quote, Contact Us Today**

**847.410.8180**

**[info@baisecurity.net](mailto:info@baisecurity.net)**

**[www.baisecurity.net](http://www.baisecurity.net)**