Datasheet

SECUREAUTH

CYBER RISK SERVICES

A trusted source for comprehensive penetration testing, red teaming and application security testing

Do you know if you're vulnerable?

Cybersecurity professionals with expertise in ethical hacking and hands-on experience exploiting vulnerabilities are hard to find, hire, and retain. Even if an organization can build such a team, keeping their skills current requires continual investment in tools and training. These talent constraints can present roadblocks to implementing a well-resourced risk assessment program, including penetration testing, red teaming exercises and application security testing. SecureAuth Cyber Risk Services can help.

What does Cyber Risk Services test?

The Cyber Risk Services team tests 5 major areas of security: applications, security awareness, likelihood of attack, cloud infrastructure, and networked device security.

Determine if an application is secure

+ Mobile, web, desktop
+ Built in-house, by third party, or customized

Security awareness

+ Understand the level of security awareness of the organization against phishing attacks.
  - Targeted phishing campaign
  - Defense readiness
  - User awareness

Likelihood and impact of an attack

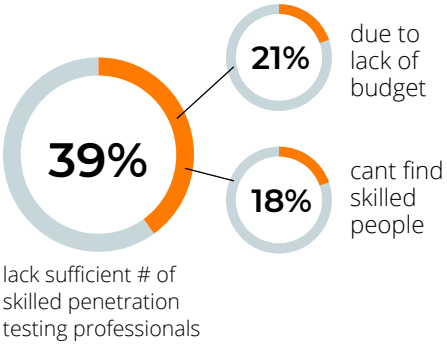
+ Determine the likelihood of an attacker compromising the network and the impact it would have.
  - External facing
  - Corporate
  - Wireless

Cloud infrastructure

+ Determine the security posture of any cloud based infrastructure.

Networked device security

+ Determine if networked devices are secure.
  - Cameras
  - VoIP phones
  - Networked speakers
  - Sensing and monitoring
  - Devices
  - Gateway
  - Data engines
  - Applications
  - Internet of things



2018 SecureAuth Penetration Testing Mini-Report

More than just penetration testing

With over 20 years' global experience, the SecureAuth Cyber Risk Services team uses the latest tactics, techniques and procedures to reduce the risk of compromise by uncovering vulnerabilities wherever they reside in your environment.

The SecureAuth Cyber Risk Services team offers the following:

+ Red teaming
+ Penetration testing
+ Application security testing
+ Real-world techniques, tactics and procedures
+ Actionable and easy-to-follow reports

Data that's useful!

Testing is useless unless it achieves actionable results. With Cyber Risk Services you get reports written by experts that highlight key data and exactly how targets were compromised as well as recommendations on best practices.

With SecureAuth Cyber Risk Services you can continuously pinpoint risks, thwart attacks, inform security and risk decision and help meet your compliance requirements without the need for additional infrastructure or staff.

Services Offered

Red Team

The SecureAuth Red Team tests the resilience of your organization against real world attackers – networks, applications, devices and more. We operate using tactics, techniques and procedures from real-world breaches to achieve specific objectives, while avoiding detection.

Scope

Networks, applications, users, and any vector an attacker is likely to take advantage of.

Objectives

Simultaneously test for vulnerabilities while also testing for defense readiness of the internal security team.

Actors

Consultants mimicking attacker's techniques and tactics. Liaison with internal security team is optional.

Outcome

+ Identify vulnerabilities exploited and attack paths
+ Description of techniques and tactics
+ Level of readiness of your defense team
+ Fixes and mitigations

Penetration Test

Know your attack surface and reduce the likelihood of being compromised by uncovering vulnerabilities across your infrastructure including network, application and social engineering targets. SecureAuth Penetration Testing service unveils vulnerabilities in your environment by creating real-world attack scenarios in a controlled and professional fashion.

Scope

Enumerate components and systems. Networks, applications, and users are usual targets.

Objectives

Think of worst case scenarios:

+ Cloud admin creds stolen
+ IP documents extracted

Actors

Consultants mimicking attacker's techniques

Outcome

+ Identify vulnerabilities exploited and attack paths
+ Description of techniques and tactics
+ Fixes and mitigations

Application Security Testing

SecureAuth Application Security Testing utilizes penetration testing techniques and source code inspection to uncover flaws and weaknesses within mobile, web, desktop and IoT applications.

+ Assess a system or groups of systems that are logically connected and cooperate to provide business functionality
+ Find as many vulnerabilities as possible
+ Evaluate the code quality in terms of security
+ Create running proof-of-concepts of the findings

The Process

Scope of work

+ Calls
+ Documentation
+ Demos

Effort determination

+ Budget limitations
+ SoW delivery

Kickoff

+ Call/Conference
+ Set rules of engagement
+ Meet the team

Execution

+ Daily/weekend updates
+ Notification of high-risk findings

Final delivery report

+ Key findings
+ Recommnded best practices

Validate

+ Confirm findings
+ Follow-up with recommendations

With over 20 years' global experience, SecureAuth Cyber Risk Services is a trusted source for comprehensive penetration testing, red team and application security testing exercises to secure your environment.

Find out more or consult an expert at https://www.secureauth.com/products/cyber-risk-services