Table of Contents

Executive Summary

Shadows Government is a virtual company that employs human resources throughout the world whom possess specific expertise and skill sets with regard to security, networking, web development, database administration and other facets of Information Technology & Security. This business model allows Shadows Government to assign the absolute best developer, programmer, web designer and/or pen-tester to your specific project. Shadows Governments' business model adheres to a one-to-one customer to project methodology, this guarantees that each and every customer will have one and only one point of contact for their project and subsequently access to the developer 24/7. Shadows Government seeks out individuals that have a passion for computing and security thereby allowing us to find the very best talent throughout the world. Shadows Government does NOT outsource our projects to anyone or any company, we handle everything in-house. Shadows Government employee must pass a rigorous Information Technology skill assessment to be considered available for our client projects. Projects are assigned to our employees by the project manager ensuring the proper expertise is provided to the client. All client projects are monitored on a daily bases by the project manager for customer satisfaction, timeline benchmarks and review purposes.

Solutions & Services

Penetration Testing

- External Penetration Testing
- External Penetration Testing
- External Penetration Testing
- External Penetration Testing
- Mobile App Penetration Testing
- Product Penetration Testing
- Wireless Penetration Testing
- Social Engineering Testing
- Advanced Threat Simulation

Application Security

- Application Penetration Testing
- Mobile App Penetration Testing
- Secure Code Review
- Threat Modeling Exercises
- Secure SDLC Integration
- Secure Policy Creation

Network Security

- External Network Assessments
- Internal Network Assessments
- Wireless Security Reviews
- Critical Server Reviews
- Active Directory Reviews
- Sensitive Data Flow Analysis
- Firewall Security Reviews
- VPN Security Reviews
- Network Architecture Reviews
- Mobile Device Reviews

Mobile App Security

Covers all major categories

- ✔ Security verification and validation includes authentication, session management, access control, malicious input handling, cryptography at rest, error handling and logging, data protection, communications security, HTTP security, malicious controls, business logic, file and resource, and other mobile controls.

Static & Dynamic Analysis

- ➢ Our security engineers will verify code at rest and at run-time using both static and dynamic analysis to identify and assess vulnerabilities within your mobile apps and their supporting infrastructure. A whitebox testing approach will benefit from access to developers, documentation, and code.

Comprehensive Security Analysis

- Shadows Government takes a holistic approach to security testing for modern day mobile applications. On top of covering all major security control categories, Shadows Government identifies today's most prevalent and critical vulnerabilities found in the OWASP Mobile Top 10 and SANS 25.

Static & Dynamic Analysis

- Our security engineers will verify code at rest and at run-time using both static and dynamic analysis to identify and assess vulnerabilities within your mobile apps and their supporting infrastructure. A whitebox testing approach will benefit from access to developers, documentation, and code.

On-Device & Off-Device Testing

- Shadows Government mobile security assessments take into account all components that drive today's modern mobile applications. Shadows Government's mobile security testing offers assessments of both the local mobile app running on-device and the back-end web services that the mobile app communicates with off-device.

Cloud Security Assessment

Cloud Application Assessments

- The overall goal of an application security assessment is to uncover software vulnerabilities, demonstrate the impact of weaknesses, and provide recommendations for mitigation. Our security engineers will provide a detailed and in-depth security analysis of your organization's critical applications.

Cloud Infrastructure Assessments

- Shadows Government engineers will remotely identify the networks, hosts, and services that comprise your cloud's external and internal environments. Vulnerabilities are identified and if desired, exploited during a penetration test.

Host/OS Configuration Reviews

- Host reviews comprehensively identify security issues within your cloud environment. Shadows Government engineers remotely review the configuration of key applications, servers, databases, and network components to identify vulnerabilities that may go unnoticed during network testing.

Cloud Architecture Reviews

- A network architecture review will evaluate the function, placement, and gaps of existing security controls and compare their alignment with the organization's security goals and objectives.

VPN Security Reviews

- The VPN review compares your current configuration against recommended best practices and identifies any areas of concern. The assessment includes a remote configuration review as well as an architecture review.

Host-Based Firewall Reviews

- Analyze both the configuration of the host-based firewalls (accounts, logging, patch management, etc.) as well as the implementation of network security controls (ACLs) via the firewall.

Internet of Things Security

- In today's connected world, the perception of security risk alone, even if not realized, can still negatively impact consumer confidence necessary for new technologies to meet their full market potential. Recent, high-profile data breaches have heightened consumers' awareness of data security and privacy issues. As a result, consumer adoption may suffer until vendors can adequately address security and privacy concerns.

  Shadows Government's Internet of Things assurance services take a holistic approach to security testing by reviewing the entire product

ecosystem, from chip to code, while prioritizing vulnerabilities so you can successfully balance risk with time-to-market pressures.

Security Benchmark

NIST Cybersecurity Framework Benchmark

- Shadows Government will benchmark your organization's current cybersecurity posture to the NIST Cybersecurity Framework, and identify an appropriate target state based on the organization's threat and vulnerability profile. By combining the NIST Framework and CCS's Top 20 Critical Security Controls a useful current/target state analysis can be performed and then utilized as a driver for prioritized activities to improve an organization's security posture.

  We use data gained during the various phases of a security audit to identify the current state. Working closely with your organization we will identify a target state based on the threats to your particular organization, your business needs, technology profile, and overall risk approach. Shadows Government utilizes the results of technical security assessments, interviews, and documentation review to complete this service.

- The National Institute of Standards released Version 1.0 of the NIST Cybersecurity FrameworkFeb 12, 2014. The Framework provides a common taxonomy and mechanism for organizations to describe current and target state cybersecurity postures, identify and prioritize opportunities for improvement, and communicate cybersecurity risk.

  The Framework Core consists of five concurrent and continuous Functions – Identify, Protect, Detect, Respond, Recover. Each of these Functions is further subdivided into several Categories that describe functions within an organization's security program. The Categories

are further divided into Subcategories which are tied to specific technical or management activities.

Incident Response

Incident Response Services

- Incident response is a distinctly unsatisfying activity for most organizations. Adversaries, usually foreign, are rarely prosecuted or deterred. Ad hoc remediation is trial and error, devolving into a game of attacker whack-a-mole that drags on for months. Mid six figure response bills are common. Shadows Government offers a pragmatic, goal based approach to incident response. Our goal is to identify the extent of the breach, clean up it as quickly as possible, and prevent re-entry by the attacker.
- While prevention efforts should not be ignored, a true measure of an organization's resilience is found in its ability to quickly detect security intrusions, thoroughly uncover the extent and impact of those intrusions, and recover.

Remote Network Monitoring

- Shadows Government will ship you a network monitoring device which is remotely administer to capture and analyze network traffic. The device is configured based on your incident type to optimize results. Shadows Government security engineers conduct daily data analysis to identify suspicious activity and determine Indicators of Compromises (IOCs), such as command and control (C2) channels used by attackers to access compromised systems.

Malware Analysis

- Shadows Government engineers will investigate discovered malware to determine impact, functionality, attribution, and/or specific Indicators of Compromise (IOCs). Our process includes both static and dynamic analysis. Static analysis will identify file type, strings, debugger unpacking, and checksum comparisons. Dynamic analysis is performed in a sandboxed testing environment to monitor process, memory, and filesystem activity.

Server/Host Data Analysis

- Following initial network monitoring Shadows Government engineers will gather data from key systems that appear to be affected. Live data is collected to retrieve and analyze relevant memory and filesystem attributes, logs, and artifacts. When necessary, forensic duplication can be conducted to retrieve and preserve a complete computer image. Log data is collected and analyzed from relevant network devices such as IDS, IPS, log servers, or similar.

Remediation Planning & Assistance

- Using the results of investigative phases, Shadows Government engineers will design a coordinated remediation plan specific to your incident. Configuration recommendations and assistance are provided for host and network based security countermeasures. Assistance coordinating the remediation event ensures actions are taken to simultaneously remove the attacker and prevent re-entry, while accounting for IT dependencies and operations.

Web Development

- ✔ Web Design
- ✔ Wordpress Development
- ✔ Joomla Development
- ✔ SugarCRM Development
- ✔ Magento Development
- ✔ e-Commerce Setup/Development
- ✔ Shopping Cart Setup
- ✔ SEO
- ✔ SEL
- ✔ Google Analytics
- ✔ Google AdSense
- ✔ Remote Assistance

Programming/Application Development

Available Languages

- ➔ C
- ➔ C++
- ➔ Python
- ➔ Assembly
- ➔ PHP
- ➔ PERL
- ➔ Ruby on Rails
- ➔ Cold Fusion
- ➔ Linux Shell Scripting

System Administration

- ➔ Server Setup/Configuration
- ➔ Wiring & Network Setup
- ➔ Reverse Engineering

Training Programs & Classes

Shadows Government offers all types of computer, server, programming, web design, web development and security training to interested clients.

Payment Options

Shadows Governments' business model mandates that on a per project basis, 50% of the total cost of the project is due upon the clients' acceptance of our services. Upon completion of the project, the remaining balance is due. We spell this out in black & white without any legalese jargon.

Supplementary Information

Our expertise includes but is not limited to Image Analysis, Audio Analysis & Reverse Engineering Malware, Viruses & Applications.

i. General Information Technology
ii. Information Security Consulting & Implementation
iii. Software & Network Penetration Testing & Security Auditing
iv. Digital Forensics
v. Online Psychological Criminal Profiling
vi. Cyber Criminal Investigation
vii. Encrypted Data Storage

Information Security Consulting & Implementation

Sometimes referred to as computer security, Information Technology security is information security applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems.

Software & Network Penetration Testing & Security Auditing

Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Digital Forensics

Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime.

Online Psychological Criminal Profiling

The analysis of a person's psychological and behavioral characteristics with respect to that individuals on-line psychopathology.

Cyber Criminal Investigation

Various terms are used (and misused) to define cybercrime. Here, we define cybercrime as, "A criminal offense that has been created or made possible by the advent of computer technology, or a traditional crime which has been so transformed by the use of a computer that law enforcement investigators need a basic understanding of computers in order to investigate the crime." Within that broad definition lie two distinct sub-categories:

Computer Crime and Computer-related Crime.

Computer Crime involves the use of a computer as the primary instrument to facilitate the crime and the target thereof . While state laws vary somewhat, these crimes usually include the unauthorized:

- •use, access or damage to a computer system;
- •taking, copying, altering, deleting, or destroying computer data, software or programs;
- •disrupting computer services or denying computer services to an authorized user;
- •introducing a computer contaminant (viruses) into any computer or system; or,
- •misuse of someone else's Internet domain name.

Computer-related Crime involves the use of a computer to commit a crime and/or as a repository of evidence related to the crime. Generally, this includes traditional crimes that have been
transformed by computer technology such as:

- •computer-generated counterfeit documents;
- •computer generated threats;
- •possession of computer-based child pornography images; or,
- •any crime in which documents or evidence is stored in a computer such as records of narcotic distribution,
- •gambling or embezzlement.

Computer-related crime can involve use of the Internet to facilitate crimes such as:

- •Internet auction fraud (primarily thefts);
- •criminal threats;
- •stalking (cyberstalking);
- •threatening or annoying electronic mail;
- •distribution of child pornography;
- •online gambling;
- •fraudulent credit card transactions;

- fraudulent application for goods or services; or,
- identity theft.

The importance of recognizing these two distinct categories is critical in that they require varying levels of investigative skill. Specifically, computer crimes require a much higher degree of technical knowledge than computer-related crimes. Throughout this paper, we will make specific observations regarding these two categories of cybercrimes.

Investigation of Cybercrime

Many law enforcement agencies define cybercrime very narrowly and think of it only in terms of complex, computer-specific issues like hacking or crimes that require a forensic computer examination. This is a fatal flaw in two respects. First, it oversimplifies what are in fact very complex crimes, and secondly it inflates the investigative difficulty of relatively simply crimes. On a national level, law enforcement must recognize that many forms of simple theft and fraud are in fact cybercrimes if a computer is used to commit the crime. What may appear to be a simple theft of small proportions--and may even go unreported in many cases--may actually be a major crime with a huge loss. In fact, computer thieves have recognized the almost infinite number of victims available to them on an international scale and the MO of "taking a little bit from a lot of places" to avoid the normal detection systems has become all too common.

Here we will discuss the most pressing problems in the area of cybercrimes. These issues are divided into the areas of organizational structure, sharing of information, resources, regulations and prevention. Obviously, these topics can only be addressed in a limited manner in this paper.

