IT Security Mentored Workshops

Vulnerability Assessments

Regulatory requirements as well as the desire to maintain a secure environment are driving the need for regularly scheduled vulnerability assessments. These assessments are a powerful way to analyze your environment and identify weaknesses within the network. The Sage Group mentors on a variety of assessment methods to provide you with a comprehensive overview of your company's technology risk profile.

Penetration Testing

Penetration Testing is an integral part of any information security program and should be conducted on a periodic basis to comply with regulatory requirements such as Sarbanes-Oxley. Penetration testing is the live testing of a computing environment to assess the defenses on the network and to identify areas for security improvement. The Sage Group has expert level experience conducting penetration tests at many of the Fortune 500. This knowledge will passed on to the client via our mentoring solution framework.

Application Security Analysis

Application security is a much needed layer of defense against attack. Applications and the ways they function are often neglected during the risk management process. In particular, web applications are avenues of attack which firewalls cannot protect against. The Sage Group has the resources and experience to mentor our clients to identify application weaknesses and develope remediation plans before they become a risk to the company.

Digital Forensics

With a team of expert level resources, The Sage Group has the ability to provide thorough electronic discovery and litigation mentoring for all computer-related activities. Digital evidence is becoming even more crucial and indispensable to legal cases. Our computer forensic specialists will mentor on the process of conducting investigations that will uncover various artifacts such as:

- Email data
- Internet usage
- Deleted files and directories
- Data and file fragments

Security Audits

The Sage Group's Mentoring/Training follows the NSA- Infosec Assessment Methodology (IAM) process for doing security audits. All of our experts are certified in this process. The IAM is a detailed and systematic way of examining cyber vulnerabilities and was developed by experienced NSA and Commercial INFOSEC assessors. NSA is providing the IAM to assist both INFOSEC assessment suppliers and consumers requiring assessments.

This market was originally created by the PDD-63 requirement for vulnerability assessments of automated information systems that support the U.S. infrastructure. In addition to assisting the governmental and private sectors, an important result of supplying baseline standards for INFOSEC assessments is fostering a commitment to improve organizations' security posture.

Since the IAM is a baseline methodology, the final results of the assessment service are highly dependent on the INFOSEC and analytic skills of the assessors.

The NSA's INFOSEC assessment process, is a high-level, non-intrusive process for identifying and correcting security weaknesses in information systems and networks.

Cyber Security

Cyber attackers exploit vulnerabilities or blind spots in your web apps, systems, networks, mobile apps, your suppliers and your people through phishing, malware, SQL injection, XSS, CSRF and other attack vectors. The Sage Group's cyber threat monitoring & response Mentoring solution works towards helping your staff obtain the skills necessary to help your organization stay cyber resilient. Our mentoring solutions are focused around SIEM Monitoring and Management, Application Security Monitoring, Perimeter Security Monitoring & Management, and Website Malware & Phishing Monitoring.

Active Defense for Enterprise Networks

The Corporate Mission

- What is being done to avoid jeopardizing the corporate integrity of the network systems?
- What mission critical network systems are vulnerable to corporate invasions?
- What network systems rely on supporting web based applications?
- What network system applications, that may or may not be web based, are exposed to either an internal or external invasion?
- What are the network system applications and corporate business functions? Human resources? Sales? Stocking inventory? Medical? Proprietary corporate and industry analysis? Competitive business data?

The Corporate Methodology

- What system tools are available to determine new Trojan horses, Viruses, and Worms?
- What system tools can intercept password cracking, DOS attacks, internally from employees and externally?
- What system tools can determine the invasions and then search, identify and locate the source of the invasions?

THE SAGE GROUP

Phil Costanzo
Phone 877-697-2434 x746
fax 877-697-2434
philc@thesagegrp.com

IT Security Mentored Workshops

The Program (5 Days)

Our workshop series is directed towards IT Professionals and business management leaders responsible for the security of computer networks. This five-day hands-on workshop will provide you with the knowledge and skills necessary to secure networks and systems in an enterprise environment. All tools are provided free with the conclusion of the practical security exchange during the interactive training course procedures.

The Business Managers Workshop (3 Days)

This workshop will help the department heads and division leaders to understand how IT develops prevention, procedures and set standards. It will teach managers how they can develop support for their IT staff, and how necessary it becomes to have a security process in place to prevent corporate business model security disparities.

The IT Workshop (5 Days)

This workshop provides both practical and technical expertise required to implement enterprise security utilizing defense security processes. The atypical 'hacker' intrusion techniques and the development of a business case for enterprise security will be addressed. Trial-ware, standard domain software, security white papers and guides, used as part of the class series will be given to students for use in their work environment. Finally all documentation, software, and security materials become the possession of the participants as well as certification, upon completion of an "interactive and practical" hands-on workshop experience.

Active Defense for Managers (2 Days)

Section 1 - Human Factors of Security

The human factors that make implementing security difficult; primary personality types encountered and their motivations for (or against) security initiatives; how social awareness can help corporate security efforts succeed.

Section 2 - Objectives of Security

The Active Defense approach to security; "Defense in Depth" model; interaction between written and electronic policy; layered approach to security including Perimeter Security, Network Security, Host Based Security, and Human Awareness.

Section 3 - What The Hackers Know

Information on some of the quick and easy tools available for finding information that can be used in a more coordinated attack by hackers; some common tools that identify network assets; how to show both technical and business managers the amount of information that is exposed via the network.

Section 4 - Enemies and Their Motivation

The most common hacker personality types; the reasons they participate in these activities; common targets for these individuals.

Section 5 - Objectives of Risk Management

Identifying specific areas where safeguards are needed to prevent deliberate or inadvertent unauthorized disclosure, modification, or unauthorized use of information, and denial of service.

Section 6 - Defining Security Policy

Developing computer security policies and procedures for corporations that have systems connected to the Internet; providing practical guidance to administrators trying to secure their information and services.

Section 7 - Developing Electronic Policy

Security tools by and large require that you create electronic policies from the written security policy in order to enforce compliance on the network. We examine e-policies, often referred to as electronic or enforceable policies, and how they are used.

Section 8 - Justifying the Cost of Security

A business case is made for Return of Security Investment by showing some areas where security saves money on labor and other items.

Section 9 - Incident Investigation Methods

Incident investigation: the process, tools, and methods

- Avoiding "contaminating" evidence
- Definitions of common response terms
- Identification of business and legal considerations
- Understanding of the time sensitivity of response

Section 10 - Security Planning for Electronic Business

Overview of the considerations necessary to securely and successfully implement electronic business over the Internet; identifying the business structure required for conducting electronic business; identifying and minimizing the threats to electronic commerce, including threats that may involve electronic commerce 'partners.'

Advanced Intrusion & Response

Is your IDS a process that includes technology, people, and tools?

Disaster recovery, network intrusion, internal threat ... What will you do?

Develop a clear understanding and take a practical and systematic approach towardintrusion detection and response.

Advanced Intrusion Detection and Response gives you the BIG PICTURE.

Overview

In this 5 day workshop participants will learn the steps of the incident handling process, the factors that influence incident response, and a "pre-incident" response strategy.

Completely customized based upon client specifications

This workshop covers the typical flow of an attack and teaches students to recognize steps normally seen in attack signatures and prior to a successful compromise of a system. The following topics will give participants the knowledge necessary to effectively detect incidents.

- Functional components of CIDF
- intrusion signature categories
- hackers response to IDS

This workshop will teach & demonstrate how to reduce false positives from damage assessment and identify the perpetrator during the response phase of investigations. Maintaining integrity of incident response is essential. Participants learn forensic policy and procedures that are critical to real world security.

Active Defense Advanced Tools

Our Active Defense system is a proven approach that reaches all depths of security. We keep it simple, just like learning the ABC's, and focus on the business needs and tasks required so the participants can solve real world security problems they will encounter when back in the work place.

- Active Defense for Enterprise Networks Review
- The Objectives Of Security
- White Hat / Black Hat / Grey Hat
- The "Triad" CIA
- Confidentiality and Attacks
- Integrity and Attacks
- Availability and Attacks
- Understanding PKI
- Using and installing PGP
- Using PGP with e-mail
- Understanding different types of Certificate servers (self-signed and 3rd party)
- Using and installing Certificate services
- Install certificates on Web servers
- Using Biometrics
- Understating security issues with Wireless
- Different types of wireless (802.11, a, b, g, x)
- Configuring WEP and learning how to defeat it
- Configuring 802.11x
- Using the Active Defense Security Tool CD.
- Process of password cracking of operating systems
- And much more

Data Correlation & Analysis (Number of Days TBD by Client)

This workshop is completely customized and will give the client the ability to develop strategies for utilizing and analyzing their IT data as it relates to their Information Security Office.

The Mentored Workshop will cover data overview, data correlation and enrichment and response procedures. Technologies/Tools to support a client's security operations such as QRadar, Imperva and Websense while not the focus, will be considered and utilized during content development.

Topics Covered

Section 1

- Data Overview
- Current Alerting
- Data being collected
- Data not being collected
- Data parsing in QRadar
- Key QRadar features/limitations
- Threat Intelligence Feeds
- Future Plans

Section 2

- Data Correlation & Data Gaps
- Correlation Rules
- Data Baselining
- Activity Profiling
- Composite Events
- Risk Scoring

Section 3

- Event Investigation Life Cycle
- Event Triage
- Pivoting
- Documentation (Best Practices)
- Containment/Remediation
- Investigation Feedback & New Intelligence
- Alert Tuning
- Creating and Using Custom Attributes
- Generating Managed Code
- Versioning, Signing and Deploying Assemblies
- Project: Specifying the Data to Include in the Grades Report

Digital Forensics & Analysis

This workshop is completely customized and will give the client the ability to develop strategies for utilizing and analyzing the Digital Forensic process as it relates to their Information Security Office.

Section 1

What is Forensics?

- How Digital Forensics is the same as traditional forensics
- How Digital Forensics is different

  Volatility of evidence

IT Security Mentored Workshops

Ease of copy

Ease of Transportation

- Recreate a timeline of events
- Integration and tension with Incident Response

The Forensic Investigation ProcessPreparation

- Assemble a forensics team
- Training

How computers work

How the Internet Work

Encryption (Cryptographic hashes)

- Software Principles & Relevant Forensic Tools

Section 2

Supporting Policies for Forensics

- Establish a formal forensics team
- Documentation requirements
- Preservation of Chain of Custody
- Principles for storage of digital media
- Use established tools
- Isolate Analysis systems
- Analysis should be repeatable
- Privacy concerns
- Case Studies
- Crafting and documenting applicable policies and procedures

Section 3

The Forensic Investigation Process – With Tools

Collection

- Chain of custody in the digital world
- Live capture of evidence
- Capture after obtaining digital media
- Precedence of evidence

Most volatile to least

Preservation

- Digital Copies

Read-only Bitwise copy

Slack space

Unallocated sectors

- Number of Copies

Original safeguard

Control copy

At least one analysis copy

- Verification through Hashing

Analysis

- Network Analysis/Logs

Workstations, Servers, Firewalls, IDS/IPS

- Sniffer captures
- Memory Analysis

Signature for known malware

Custom of unknown malware

Presentation

- Internal reports
- Court presentations

Digital Forensic Tools Utilized (Subject to Client preferences)

Wireshark Sniffer – Collections and Analysis

- Demonstrations/Shadowing

Capturing data

Find malicious activity in a capture

WinHex – Collection, Preservation, and Analysis

- Demonstrations/Shadowing

Copy evidence

Look for evidence of malware

Log Analysis ToolAnalysis

- Demonstrations/Shadowing

Determine order of events

Other Important Forensic Tools (Some Free-Some Not)

- EnCase – Collection, Preservation, Analysis, and Presentation
- SafeBack (Preservation), DD (Preservation), SANS-SIFT (Preservation, Analysis, and Presentation)
- Software Analysis Tools and Scripts (Some Custom) (Requires some Perl/Python Scripting Experience)

THE SAGE GROUP

Phil Costanzo
Phone 877-697-2434 x746
fax 877-697-2434
philc@thesagegrp.com