THE SAGE GROUP

Mentoring Solutions for Law Enforcement

"Solutions that Empower your Workforce"

IT & Cyber Security

Overview and Solutions

Technology systems have contributed significantly to the operational effectiveness and efficiency of law enforcement agencies of all types.

As the ability to collect, share, and use information continues to gain momentum in modern policing, technology tools that offer agencies the chance to develop this ability are omnipresent.

Yet, as much as we rely on technology for some of our most sensitive and necessary activities, securing that technology is often an afterthought to system deployment rather than being an integrated part of the strategic implementation process.

The Sage Group's Information Technology & Cyber Security Mentoring Solutions division was created to provide the law enforcement community with strategies, best practices, recommendations, and ideas for developing and implementing information technology security policies. We have helped our clients identify and assess information technology security risks within their agencies and provide ideas for mitigating them. Moreover, we encourage clients to view security policies and practices as an ongoing process of assessment, modification, and measurement.

Expertise & Experience

- Incident Response
- Penetration Testing
- VOIP and Wireless Penetration Testing
- Data Correlation & Analysis
- Security Auditing Policies and Guidelines
- Digital Forensics and Court Preparation
- Digital Forensics for Mobile Devices
- Risk Assessments
- Cyber Security and Social Media
- Intrusion Detection
- Active Defense
- Cyber Range Capability

GSA Schedule 70 Contract GS-35F-174DA

Incident Response

On April 17, 2011 77 million user accounts were compromised within the Sony PlayStation Network. On May 30th, 2011 PBS.Org was hacked, malicious users were able to compromise a number of internal hosts and data bases. One June 15, 2011 the CIA website was compromised, malicious users took control of the website.

More than 30% of all hacks originate in the US, more than 80% of consumers do not use a different email address for their online purchases. Nearly 75% of all Americans have fallen victim to some form of cyber-crime. Hacking has led to over a trillion dollars in losses to businesses around the world. In almost all cases the hackers stole sensitive personal identifiable information, left backdoors into your network and created zombies of your computer system so they can be used to launch attacks at staged events.

- Incident Response Policy Core Elements
- Incident Response Policy Ancillary Elements
- Establishing annual reviews of the CIR Policy
- Third Party Certifications
- Incident Response Team Roles and Responsibilities
- Incident Response Awareness
- Tuning the infrastructure
- Steps to incident validation
- Developing an incident escalation and contact matrix
- System Access / Physical Access
- Selecting a recent breach / incident and dissecting the failures
- Vendor and Consultant Partnerships
- Responsive Action
- Containment
- DR / BCS
- Remediation
- Ensuring you have an established Digital Forensics Program
- Establishing a toolkit set for your digital forensics program
- Preservation
- Developing an Incident Response Assessment Program
- Staging a production incident

Digital Forensics & Court Preparation

What is Forensics?

- How Digital Forensics is the same as traditional forensics
- How Digital Forensics is different
  - Volatility of evidence
  - Ease of copy
  - Ease of Transportation
- Recreate a timeline of events
- Integration and tension with Incident Response

The Forensic Investigation Process

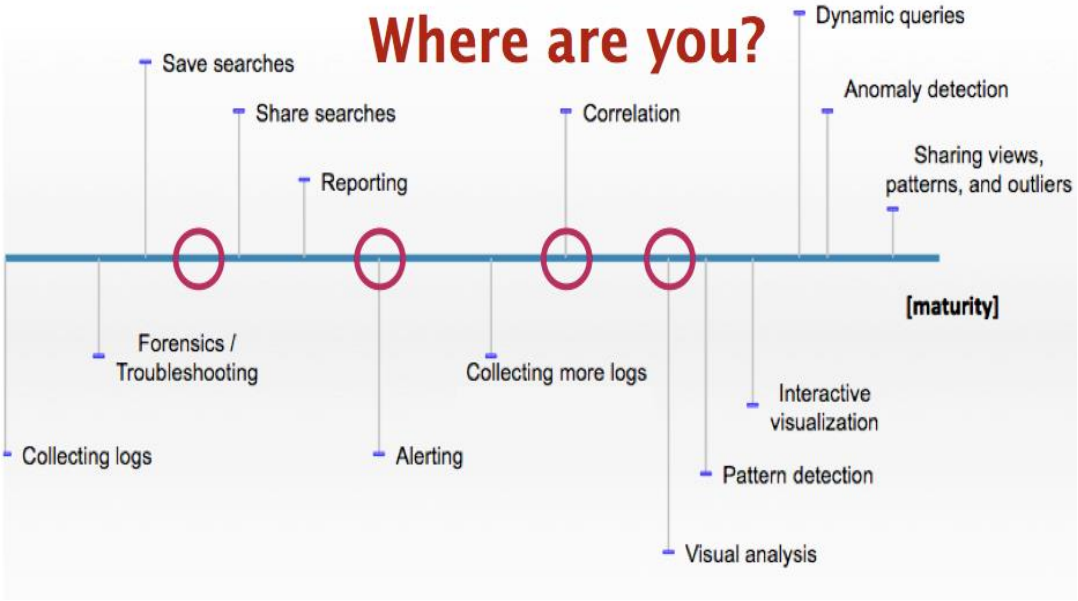
Preparation

- Assemble a forensics team
- Training
  - How computers work
  - How the Internet Work
  - Encryption (Cryptographic hashes)
- Software Principles
- Relevant forensic tools

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

The Forensic Investigation Process



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 Presentation Simulation

Cyber Security & Social Media

- Background and the Dangers of Social Media
- Exercise – Google Yourself
- Social Media Sites
- Reading the Fine Print – Privacy Policies
- Once on the Internet, Always on the Internet
- Protect Yourself – Discretion is the Better Part of Valor
- Exercise – Creating a Safe Profile
- Social Media Threat Vectors
- Monitor Your Brand
- Control Who Updates the Site – Check for Quality
- Developing Internal Policies
- Training Your Employees
- Loose Lips Sink Ships
- Protection Tools & Techniques
- Encoding and Decoding URL's
- Is Your "Friend" Acting Strange?
- Keep Your Circle Close
- Free Software? Cool!
- Keeping Applications Updated

- Patching Systems
- The Clickjack Attack
- Are Your Mobile Devices Protected?
- Malvertising
- Twitter as a Means of Control
- Skepticism – Your Best Friend
- Survey says…It's a Scam!
- Option Profiles
- Engaging Human Resources