Agenda

» Who I am, Who we are, What we do, and Why Foresite is different

» Developing a Security Program without a Fortune 500 Budget
  » Coming Together
  » Carbon Based Hacking
  » Passwords
  » Where’s my data?
  » Segmentation
  » DNS
  » Patching
  » Logging, Alerting, and Responding
  » Incident Response Management

» In Summary

» Q&A
Presenter – About Me

John Wolf

- Senior Security Consultant with Foresite for the last year
- Foresite’s Assessment Services and Incident Response/Digital Forensic Lead
- Almost 10 years in Information Security and Information Technology for almost 18 years.
- Has worked with small to large enterprise organizations within every industry vertical including Education
- Driven professional that looks to provide a sharing of knowledge with all clients on security processes that work and those that do not
- Has held numerous industry certifications from general (ie. CISSP) to network security testing (CSTA), wireless network assessment (CWNA), PCI (QSA, PA-QSA), and digital forensics (Ence) amongst those
Who we are
The Foresite Difference

**Security Testing and Assessments**
- Vulnerability and penetration testing
- Web application penetration testing
- Social engineering
- Enterprise risk assessment
- Third-Party risk assessment (vendor management)

**Compliance Solutions**
- Gap assessment
- Certified Audits/Attestations (PCI, HIPPA, SOX, NIST, etc.)
- Remediation

**Security Monitoring and Alerting**
- Proactive Log Analysis

**Device Management**
- Turnkey Solutions

**Incident Response**
- Response Communication and Planning
- Forensics
- Eradication Assistance

VISIONARY IT SERVICES
Developing a Security Program without a Fortune 500 Budget
Coming Together

» Working together to accomplish more.
   » Share knowledge and experience
   » Share wins and losses
   » We’re in the perfect environment to build/start building the relationships needed.

» Finding locals
   » http://information-security.meetup.com/
   » http://computer-security.meetup.com/
   » Google!
Carbon Based Hacking

“Hi! My name is ...”

- Phone
  - http://www.social-engineer.org/

- Phishing (ie. email)
  - http://www.phishingfrenzy.com/

- Physical
  - Walk in the door!

Foresite has had 100% results of either gaining access (physical), getting an individual to provide sensitive information (phone), or open, click on a link, and submit sensitive information (phishing) over the last 12+ months.
Here a password. There a password. ...

- Easy to remember, used everywhere...not good
  - https://haveibeenpwned.com/

- Password Management
  - LastPass
  - KeePass
  - Password Safe

- Open Source Intelligence (OSINT)
  - Maltego
  - Shodan
Knowing where your data is
- It isn’t as simple as it sounds
- Who has access?
- Is encryption being used?
  - If so, who’s in charge?

Backing up your data
- Ransomware (can you say CryptoLocker!)
- The Cloud!
Segment, Segment, Segment!!!

Access controls – Do all individuals have the correct privileges

Don’t forget the front door.
- You can go through both directions, same with network traffic. Protect both directions.
How do I spell that?

- DNS and filtering

Why?
- #1 - Malicious sites
- Protect against malicious communications (such as CryptoLocker)

Mistyping of a URL is more common than you think.
Patching, its not just for breakfast!

- Patching and Updates
  - If you were not expecting this, we need to talk!

- Its not just for the OS anymore.
  - Java, Flash, Apache, WordPress, etc.

- Legacy should not prevent

- Don’t forget to check that updates have been applied
  - http://www.ossec.net/
A complex 4 Letter Word

- **SIEM**
  - [https://www.alienvault.com/](https://www.alienvault.com/)

- **Log aggregation**
  - [https://syslog-ng.org/](https://syslog-ng.org/)

- These are not set and forget solutions.

- Collection of logs needed for disaster/incident response.
Plans that come together

Planning for Disaster

- What happens when you get notified by an outside agency that your sensitive data is out there for all to see?
- What happens if?

NIST SP800-61 R2 (Incident Response)

- [http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)

- Preparation
- Detection and Analysis
- Containment, Eradication, Recovery
- Post-Incident
In Summary

- Nothing in life is free!
- Know yourself, your friends, and your enemies.
- Plan, not just for disaster, but where you are going!
- Start!!!
Foresite Contact Details

Lorissa Rapp
Director of Sales
Lorissa.Rapp@foresite.com

John Wolf
Senior Security Consultant
john.wolf@foresite.com

www.foresite.com