New York/New Jersey Intergovernmental Audit Forum Meeting

Cyber Investigations: Audits (Shadow)

EY
Building a better working world

Timothy P. Ryan

- US Cyber Investigations leader, Partner, Ernst and Young, LLP
- Cyber Investigations leader, Managing Director, Kroll
- Supervisory Special Agent, Federal Bureau of Investigation
- Acting Director, New Jersey Regional Computer Forensics Laboratory
- Practiced law in Arizona
- JD Rutgers
- MS IT/IA University Maryland
- FBI CART
- SANS GCIH

What happens when an audit client suffers a cyber incident?

The better the question. The better the answer.
The better the world works.

Building a better working world

Hypothetical Fact Pattern: Breach at Sure Shot Diagnostics

Sure Shot Diagnostics is a medical testing facility that allows consumers to perform blood tests and receive expert analysis. Sure Shot is a publicly traded company with labs in every US state. Consumers pay for their blood tests using credit or debit cards. Consumers fill out a medical history form prior to the test. Consumer also have the right to opt out of the sharing of their information with Sure Shot affiliated companies. These companies market a variety of medical devices and pharmaceuticals.

Sure Shot was notified by the FBI that one of their machines was communicating with a foreign IP address associated with a state sponsored hacker.

Different purpose and focus of various cyber investigations

- **PII** State Breach laws-Notification requirements. Focus on personally identifiable information.
  - http://www.mass.gov/ago/doing-business-in-massachusetts/privacy-and-data-security/security-breaches.html#
- **PCI** Payment Card Industry- PCI-DSS. Review of the PCI architecture using a PCI Forensic Investigator (PFI). Focus on credit cards and card processing machines.
  - https://www.pcisecuritystandards.org/about_us/
- **PHI** Health and Human Services, Office of Civil Rights-HIPAA Privacy and security rules
  - https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

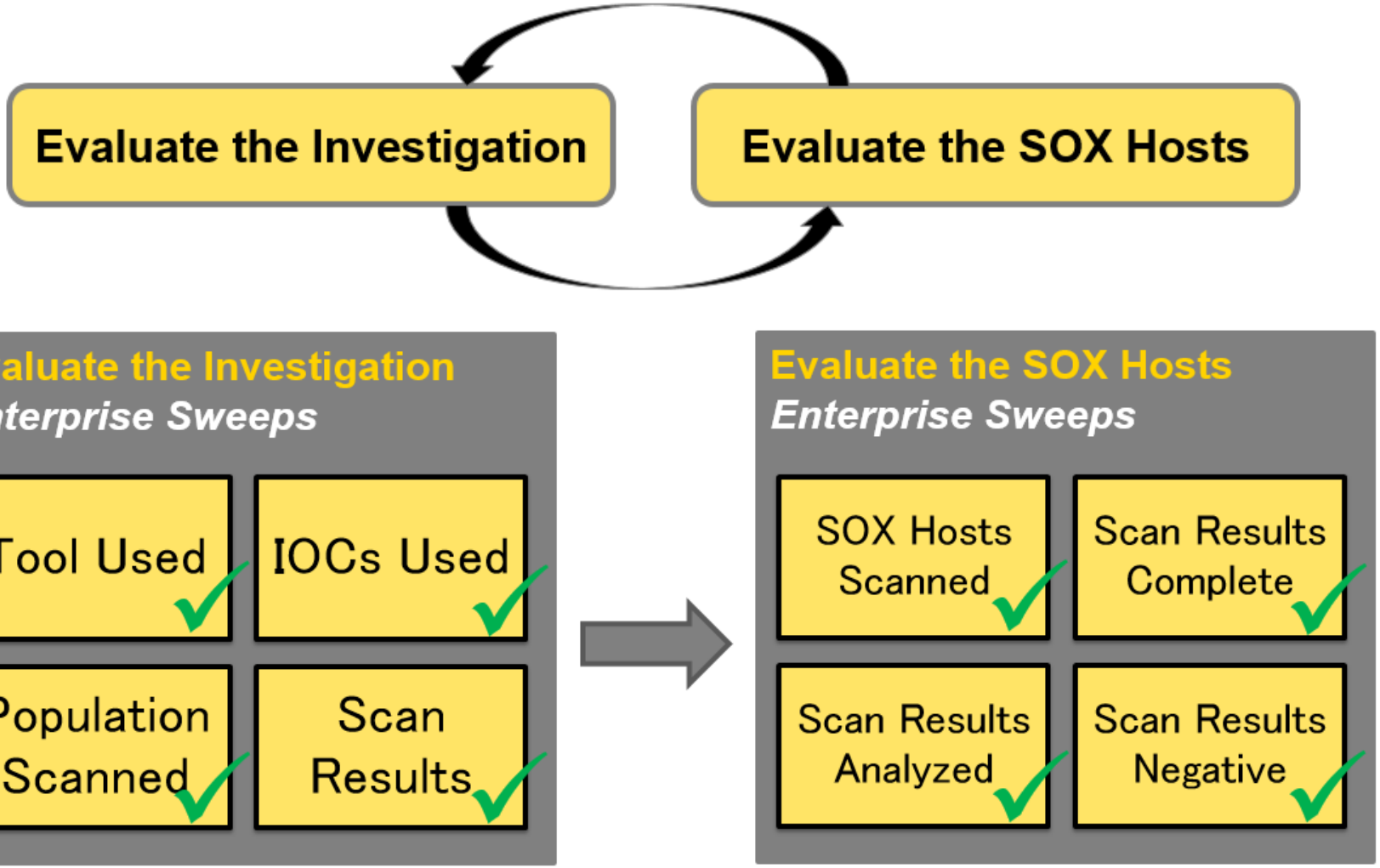
Cyber Audit Investigations: Shadows

- Pertains to audit clients who have suffered an incident where we rely on the client's information systems to produce audit findings.
- Shadow investigation is designed to determine whether the incident impacted the financial systems that the auditor relies upon when issuing its audit reports.
- Inaccurate financial reporting could impact the client and their auditor.
- Cyber investigators work with the audit team as part of the audit team.

Potential Triggers for a Cyber Shadow Investigation

- Compromise of enterprise access controls that would provide the intruder access to the financial application or the system hosting that financial application.
  - Malware
  - Compromised credentials, or
  - Exploited vulnerabilities
- Compromise of enterprise access controls where there is evidence or a reasonable likelihood that the intruder compromised a windows domain administrator account.
- Misuse by a user, internal or external, of credentials permitted to access relevant financial systems.
- Any unauthorized activity related to a relevant financial system.

Methodology

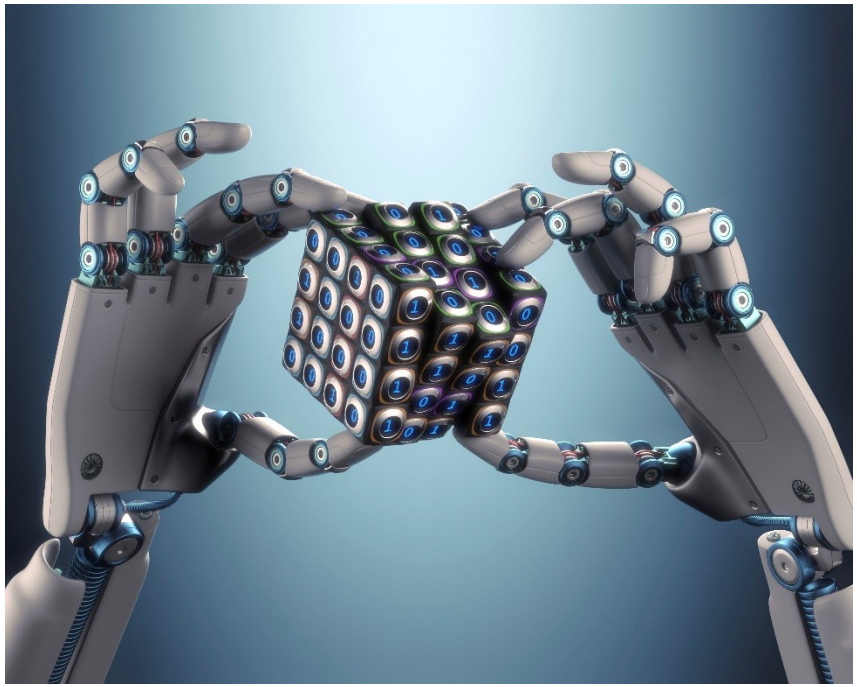


Pertinent Questions

- Who did the primary investigation?
- What level of visibility did they have into the adversary's activity:
  - Antivirus
  - Endpoint detection
  - Network logs
  - Duration of the logs
  - Host forensics
  - Backgrounds of the investigators
- What malware was used
- What credentials were used

Elements of Proof

- Different from the primary investigation.
- Investigators saying “we didn’t find anything” may not be sufficient.
- Sometimes raw log data or screenshots are required that demonstrate nothing was found.



Hypothetical Fact Pattern: Breach at Sure Shot Diagnostics

Sure Shot Diagnostics is a medical testing facility that allows consumers to perform blood tests and receive expert analysis. Sure Shot is **a publicly traded company** with **labs in every US state**. Consumers pay for their blood tests using **credit or debit cards**. Consumers fill out a **medical history form** prior to the test. Consumer also have the right to opt out of the **sharing of their information with SureShot affiliated companies**. These companies market a variety of medical devices and pharmaceuticals.

Sure Shot was notified by the FBI that one of their machines was communicating with a foreign IP address associated with a state sponsored hacker.

The Sure Shot Diagnostics Investigations

- Primary (privileged): Internal and forensic firm retained to understand the scope of the breach and ensure it is contained. Often done under privilege at the direction of counsel.
- PFI: Card brands may require a PFI if there has been a loss of credit card information. The PFI will be focused on the PCI processing infrastructure only.
- Non-privileged: Sometimes conducted to assist with PHI, PII, Audit inquiries from State Attorneys General, OCR, Auditor.
- Shadow: Audit firm will review the foregoing investigations to determine if the incident impacted the financial systems.

Questions