IR/Forensics Team Tactics Panel

Best Incident Response and Forensics Techniques

Eric Gentry
eric.gentry@verizonbusiness.com

Christopher J Novak
chris.novak@verizonbusiness.com

Quickly Determining What Type of Data Was Compromised

Know What/Where Sensitive Data Resides in Environment

- Network Diagram
- Map Data Flows

Forensic Analysis

Identify / Analyze Corroborating Sources

- Netflows, IDS and Firewall Logs, etc.
- Web Server Logs
- Database Content

Determining How a Breach Occurred

Malware Analysis

- Analysis in Sandbox Environment
- IP Addresses
- Filenames, Processes
- Hacker Handles

Leverage Other Intelligence Sources

- Underground Monitoring
- Coordination with Law Enforcement
  - e.g. Known Information Black Market forums

Circumstantial Evidence

- Overall Security Posture

Identify Malware on Hosts

Forensic Analysis

- Known Keywords
- Analysis of File Times/Dates
- Known “Bad” IP Addresses
- Known Malware Hash Values

Other Evidence Sources

- Web Server Logs
- Application Logs

Thank You

Eric Gentry
eric.gentry@verizonbusiness.com

Christopher J Novak
chris.novak@verizonbusiness.com