How to Become a C.S.I.

Enterprise Forensics using a SIEM

Gary Freeman
HP ESP Pre-Sales Manager
Today’s agenda

Introduction
Typical Investigation Use Cases
Cyber Investigator Challenges
How HP ArcSight Assists
Integration Commands
Integration Commands In Action
Cyber Investigation Considerations
Appendix: Sample Investigation Commands
Introduction
Introduction

- C.S.I. = Collect, Store, Investigate
- Webster’s defines forensics as “the use of science and technology to investigate and establish facts in criminal or civil courts of law”
- Forensicswiki.org states that Network Forensics is “…is the process of capturing information that moves over a network and trying to make sense of it in some kind of forensics capacity.”
- Enterprise Forensics = new category that focuses on user activity and what drives the business (analytics + behavior)
- Investigators need to understand both synthesizing technical knowledge and human behaviors to better understand criminal behavior and motivation
- Data mining, profile analysis, user attribution and integration between SIEM and Enterprise Directories assist investigators
Typical Investigation Use Cases
Typical Investigation Use Cases

Classification of Corporate Investigations:

- **External Attacks (EA)** – Malware, Phishing, DDoS, XSS, SQL Injection
- **Compliance Violations (CV)** – Attacks against regulated systems
- **Employment Fraud (EF)** – Hours of work
- **Resource Misconduct (RM)** – Excessive printing, email
- **Policy Violations (PV)** – Acceptable usage
- **Anonymous Electronic Abuse (AEA)** – threatening emails
- **Counter-Surveillance (CS)** – Inappropriate snooping
- **Employee Sabotage (ES)** – Logic bombs
- **Property Theft (PT)** – After hours, video surveillance
- **Data Leakage (DL)** – Exfiltrating sensitive data
- **Network Behavior Anomaly (NBA)** – Abnormal activity
- **Lawful Intercept (LI)** – CALEA / Intercept traffic from MSSP/ISP without warrant
Cyber Investigator Challenges
Cyber Investigator Challenges

- Islands of defense / silo jurisdiction
- Large volumes of data
- Preserving evidence
- Many disparate tools used during investigation
- No workflow
- Admissibility
- Centralized collection and reporting
- Determining the who, what, when, where and why
- Interception “Safe Havens”
- Privacy Concerns
- Laws / Legislation
How SIEM Tools Assist
How SIEM Tools Assist

- Centralized data collection with a single “pane-of-glass”
- Terabytes/Petabytes of log storage for forensic analysis with integrity
- Integration with third-party tools for automated acquisition
- Integrated case management to establish chain-of-custody
- Threat response can be invoked to quarantine and contain threats during an investigation
- Lists allow “watched” activity for attackers and employees
- Identity correlation provides monitoring and reporting for employee activity by attributing name to the IP/MAC address
- Pattern Mining establishes baselines for employee activity and any deviations
- Reputation feeds provide real-time input from open-source threat intelligence to identify and mitigate malware, APT, botnets, etc.
Typical C.S.I. Architecture
Typical C.S.I. Architecture

- SIEM provides central location for case management, data acquisition, analysis, reporting, payload analysis and correlates identities and user behaviour.

- Distributed components could include Packet Capture, Flow Analysis, Firewall / IPS blocking.
Cyber Investigator Tools
**Cyber Investigator Tools**

### Collect
- Log Events (Connectors)
- Perimeter / Intranet Devices
- Authentication Data
- DB / Application
- Packet Capture (TCPdump, Snort, Wireshark, NIKSUN, NetWitness)
- Wireless Forensics
- VoIP
- Real-time integration (CMDB, IPS, scanners, malware lists, fingerprinting)

### Store
- Log Storage (Logger)
- Database (ACID, Base, MySQL, etc)
- Payload Data
- Session Traces
- Hadoop
- Vertica
- Autonomy

### Investigate
- Event Normalization
- Identity Correlation / User Monitoring
- Session Re-Assembly
- Case Management
- Workflow Integration
- Reporting
- Chain-of-Custody / Integrity
- On-demand Tools
- Geo-location mapping
Investigation Tools Integration

- Integration Tools introduced in ESM 4.5
- A lightweight means to link information between the SIEM and third-party tools
- Command execution mechanisms
  - URI (HTTP)
  - Local script/executable ("tool")
  - CounterAct Connector (TRM)
- Result rendering
  - Internal web browser/external web browser
  - Script/executable output
  - CounterAct structured result
  - Attach to case
  - Save to a file
Cyber Investigation Integration Commands

- Investigate: Blacklisted Sites (URL)
- Investigate: DNS Lookup: `%arcsight%\tools\dig.exe`
- Investigate: Internet Port Scan (URL)
- Investigate: Malware Protection Center (URL)
- Investigate: NBTstat: `%system32%\nbtstat.exe`
- Investigate: NetWitness Integration (local image)
- Investigate: NMAP (TCP): `%program files%\nmap\nmap.exe`
- Investigate: NMAP (UDP): `%program files%\nmap\nmap.exe`
- Investigate: Open Shares: `%arcsight%\tools\netview.cmd`
- Investigate: OS Fingerprint: `%program files%\nmap\nmap.exe`
- Investigate: Packet Capture: `%arcsight%\tools\windump.exe`
- Investigate: PathPing: `%system32%\pathping.exe`
- Investigate: RFC Ignorant: (URL)
- Investigate: SMTP Check: (URL)
- Investigate: Suspected Malware (URL)
- Investigate: Threat Expert (URL)
- Investigate: Vulnerability Scan: `%program files%\tenable\nessus\nessuscmd`
- Investigate: Windows Event (URL)
Integration Commands In Action
Integration Commands In Action #1

- Security triages a request to investigate everyone going to badguy.net
- First step is to create a case.
- Next, locate events with a destination DNS domain that contains “badguy.net”
- Run “dig” against domain to find out all DNS info related to “badguy.net”
Integration Commands In Action #2

- Next, add the output to the case already created
- Conduct an nmap TCP scan against target to discover open ports
- Continue running tools and adding the output to the case
- The tool output is added to the “Notes” section of the case along with audit trail items
Integration Commands In Action #3

• For long-term investigations, ESM allows integration with HP ArcSight Logger and can pass search parameters as well as usernames and passwords to the Logger appliance.

• Results can be exported to CSV and imported to the case as an attachment.
Integration Commands In Action #4

- Finally, case notes are required to describe what actions were taken, what tools were used and prepare the results of the investigation.
- Final reports can be generated to show all activity
Cyber Investigation Considerations
Integration Tools

- Choose Windows versions of common tools since the commands are run locally in most cases and most SOC consoles are running on Windows.
- On-demand packet capture tools would be scripted and would be invoked on remote systems connected to span ports on switches.
- Real-time packet capture can be done with integration with tools such as TippingPoint, NetWitness or Niksun NetTrident.
ArcSight Threat Detector (formerly Pattern Discovery) allows an investigator to build logical relationships from events and model baselines.

- Automatically identifies patterns that occur in the event flow that you don't know about or suspect.
- Network activity, application usage, user behaviours and heuristic deviations can be detected and added as baselines to Active Lists.
- Rules can then be created from the detected patterns and the investigations can be automated.
- Detected patterns can be attached to cases as well.
HP ArcSight IdentityView

Streamlined investigations via detective user activity reports:

- **Privileged User and Privileged Account Monitoring**: actively monitor the actions of privileged users for risky or unusual activity
- **Shared Account Tracking**: attribute use of a shared account or service accounts to a single individual
- **Terminated Employee/Contractor Access Detection**: correlates network or system activity to user status in directory
- **Multi-Account Correlation**: tie multiple user accounts to a single identity and then correlate activity across those accounts
- **IP Address to User Mapping**: correlate data between addressing systems (i.e. DHCP) and all log sources that use IP addresses) to attribute unauthenticated activity to individual users
- **Separation of Duties Violation Detection**: correlate and alert when a user performs actions that no single user should be able to perform
Other Tools

- CEF Integration with Deep Packet Inspection tools such as nPulse HammerHead, Qosmos, AccessData, Solera, Narus, NetWitness, NIKSUN, FireEye, etc
- Integration with EnCase using Response Automation Connector (RAC)
  - forensic auto-capture of live system memory
  - capturing Internet history, artifacts and cache files
  - Incident response automation
  - conduct forensic audits against white or blacklists
- Integration with Threat Response Manager (TRM) or TippingPoint SMS allows investigators to investigate a node and even quarantine a user that is in violation of corporate policies
- Integration with other HP products such as RepSM, TippingPoint, Fortify, EnterpriseView, NNMi, OMi, CMDB allows for additional enterprise intelligence regarding attacks or targeted assets
- Integration with applications allows ESM to keep a baseline of “normal” employee behavior and can raise an alarm when applications are being misused
What’s HP doing in the space?

HAVEn—Big Data platform

**Hadoop/HDFS**
Catalog massive volumes of distributed data

**Autonomy IDOL**
Process and index all information

**Vertica**
Analyze at extreme scale in real-time

**Enterprise Security**
Collect and unify machine data

**nApps**
Powering HP Software and your apps
Sample Investigation Commands
Appendix: Sample Investigation Commands

Investigate: Blacklisted Sites
- Command Type: URL
- Configuration Name: Investigate: Blacklisted Sites
- Configuration Attributes: Internal
- Configuration Context: Viewer | All Views | All Selections | IP Address, String

Investigate: DNS Lookup
- Command Type: Script
- Command Syntax: %arcsight%\tools\dig.exe -t ANY $selectedItem
- Configuration Name: Investigate: DNS Lookup
- Configuration Attributes: Text Renderer
- Configuration Context: Viewer, Resource, Editor | All Views, Assets, All Editors | Selected Cell, All Selection

Investigate: Internet Port Scan
- Command Type: URL
- Configuration Name: Investigate: Internet Port Scan
- Configuration Attributes: Internal
- Configuration Context: Viewer | All Views | All Selections | IP Address, Strings | IP Address, String, All Data Types

Investigate: Malware Protection Center (Target Address)
- Command Type: URL
- Configuration Name: Investigate: Malware Protection Center
- Configuration Attributes: Internal
- Configuration Context: Viewer | All Views | All Selections | IP Address, Strings | IP Address, String, All Data Types
- Context: Viewer | All Views | All Selections | IP Address, Strings | IP Address, String, All Data Types
Appendix: Sample Investigation Commands

**Investigate: NBTstat**
- Command Type: Script
- Command Syntax: %system32%\nbtstat.exe -a $selectedItem
- Configuration Name: Investigate: NBTstat
- Configuration Attributes: Text Renderer
- Configuration Context: Viewer, Resource, Editor | All Views, Assets, All Editors | Selected Cell, All Selections | IP Address, String, All Data Types

**Investigate: NMAP (UDP)**
- Command Type: Script
- Command Syntax: %program files%\nmap\nmap.exe -vv -sU -p0 $selectedItem
- Configuration Name: Investigate: NMAP (UDP)
- Configuration Attributes: Text Renderer
- Configuration Context: Viewer, Resource, Editor | All Views, Assets, All Editors | Selected Cell, All Selections | IP Address, String, All Data Types

**Investigate: Open Shares**
- Command Type: Script
- Command Syntax: %arcsight%\tools\netview.cmd $selectedItem
- Configuration Name: Investigate: Open Shares
- Configuration Attributes: Text Renderer
- Configuration Context: Viewer, Resource, Editor | All Views, Assets, All Editors | Selected Cell, All Selections | IP Address, String, All Data Types
Appendix: Sample Investigation Commands

**Investigate: OS Fingerprint**
- Command Type: Script
- Command Syntax: %program files%\nmap\nmap.exe -vvv -A -O -PN $selectedItem
- Configuration Name: Investigate: OS Fingerprint
- Configuration Attributes: Text Renderer
- Configuration Context: Viewer | All Views | All Selections | IP Address, String

**Investigate: Packet Capture**
- Command Type: Script
- Command Syntax: %arcsight%\tools\windump.exe -i 3 -l -x -n host $selectedItem
- Configuration Name: Investigate: Packet Capture
- Configuration Attributes: Text Renderer
- Configuration Context: Viewer | All Views | All Selections | IP Address, String

**Investigate: PathPing**
- Command Type: Script
- Command Syntax: %system32%\pathping.exe $selectedItem
- Configuration Name: Investigate: PathPing
- Configuration Attributes: Text Renderer
- Configuration Context: Viewer | All Views | All Selections | IP Address, String

**Investigate: RFC Ignorant**
- Command Type: URL
- Configuration Name: Investigate: RFC Ignorant
- Configuration Attributes: Internal
- Configuration Context: Viewer, Resource, Editor | All Views, Assets, All Editors | Selected Cell, All Selections | IP Address, String, All Data Types
Appendix: Sample Investigation Commands

**Investigate: SMTP Check**
- Command Type: URL
- Configuration Name: Investigate: SMTP Check
- Configuration Attributes: Internal
- Configuration Context: Viewer, Resource, Editor | All Views, Assets, All Editors | Selected Cell,
  All Selections | IP Address, String, All Data Types

**Investigate: Suspected Malware (Target Address)**
- Command Type: URL
- Configuration Name: Investigate: Suspected Malware
- Configuration Attributes: Internal
- Configuration Context: Viewer, Resource, Editor | All Views, Assets, All Editors | Selected Cell,
  All Selections | IP Address, String, All Data Types

**Investigate: Threat Expert (link – no integration)**
- Command Type: URL
- Configuration Name: Investigate: Threat Expert
- Configuration Attributes: Internal
- Configuration Context: Viewer, Resource, Editor | All Views, Assets, All Editors | Selected Cell,
  All Selections | IP Address, String, All Data Types
Appendix: Sample Investigation Commands

Investigate: Vulnerability Scan
- Command Type: Script
- Command Syntax: %program files%\tenable\nessus\nessus\nessuscmd -U -p139,445 -V -i 10150,34477 $selectedItem
- Configuration Name: Investigate: Vulnerability Scan
- Configuration Attributes: Text Renderer
- Configuration Context: Viewer, Resource, Editor | All Views, Assets, All Editors | Selected Cell, All Selections | IP Address, String, All Data Types

Investigate: Windows Event
- Command Type: URL
- Configuration Name: Investigate: Windows Event
- Configuration Attributes: Internal
- Configuration Context: Viewer, Resource, Editor | All Views, Assets, All Editors | Selected Cell, All Selections | IP Address, String, All Data Types
Summary
Why HP Enterprise Security

Harden the attack surface
improve and reduce the vulnerability profile of applications and systems

Increase threat intelligence
see, find and stop known and unknown threats

Proactively protect information
find and protect sensitive information across the enterprise
Thank you