Bringing a Knife to a Gun Fight: The Arsenal Required for Modern Forensic Combat!

Andrew Hay
Senior Analyst, Enterprise Security
The 451 Group
Introduction

- Andrew Hay
- Senior Analyst, The 451 Group
- CCNA, CCSE NGX, Security+, GSEC, GCIA, GCIH, GCFA, RHCE, and CISSP
- Author, blogger, speaker, and lifetime security practitioner
Overview

• Current State of Forensics
• Security Management Acronym Hell (SMAH)
• The Future
• Summary
• Questions
Current State of Forensics

• Primarily host-centric focus
• IR and forensic response
• Ancillary network-centric helpers
• packet analysis, log inspection, IDS, etc.
• Combined forensic/IR workbench?

‘This is what the SIEM sales guy told me their product was for!*!'
Leaning-Forward
Leaning-Forward Forensics

Forensics & IR ‘Sweet Spot’

Leaning-Backwards Forensics
‘Sweet Spot’???

NIDS/NIPS Logs

Packet Captures

Proxy Logs

Host Logs

Firewall Logs

Network Flows

VPN Logs

HIDS/HIPS Logs

Access Logs

Behavior & Anomaly Detection

Application Logs
Where SIEM was Supposed to Help
Security Management Acronym Hell (SMAH)

- SIM?
- LM?
- SEM?
- SIEM?
- ESIM?
SIM & SEM?

- **Security Information Management (SIM)**
  - Log collection, access monitoring, reporting, etc.
  - Some collection from security and network devices

- **Security Event Management (SEM)**
  - Data from network, security, and applications
  - Event correlation and incident response
OK, What’s SIEM?

- Security Information & Event Management (SIEM)
- SIM + SEM = SIEM
- Compliance, security, and operational monitoring and reporting
- Correlation and normalization of logs, events, and network traffic related information
How About ESIM?

- ESIM is the next evolution in SIEM
- Combines traditional SIEM with Log Management, Vulnerability Management, Patch Management, DAM, White listing, WAF, IT GRC, and more!
- Forms basis for a true Forensic and Incident Response ‘workbench’
- No SIEM or LM vendor is here yet
The Future

• The future is ESIM!
• SIEM talks about ‘helping’ with forensics but doesn’t help enough to provide a useable forensics and IR workbench
• Let’s look at a typical incident response scenario
Plan comes together
What Does Each Gain with ESIM?

- Captain H.M. "Howling Mad" Murdock
  - Detect incident precursors and alert on, or potentially prevent, the breach before it occurred
  - Build a complete story of the incident based on logs, flows, packet captures, etc.
  - Inform Hannibal of similarly exploitable systems based on incident timeline and VM/PM
What Does Each Gain with ESIM?

- First Lieutenant Templeton "Faceman" Peck
- Draw from centralized investigatory notes from other team members during interviews (as they make them)
- Easily corroborate story on-the-fly (e.g. ‘I didn’t log into that machine on that day’)
What Does Each Gain with ESIM?

- Master Sergeant Bosco Albert ("B.A. Baracus"
- Could right-click on asset and kick-off remote forensic image acquisition
- Automated analysis searching for evidence already identified by team
- Downside: Less driving around in the cool van
What Does Each Gain with ESIM?

- Colonel John "Hannibal" Smith
- Can easily determine value of assets and redirect team as needed
- Achieves complete situational awareness of all aspects of the investigation from a central location - easy coordination of team
- Able to create incident walkthrough for management team and make recommendations on how to prevent in the future
Summary (Conclusions?)

• ESIM is not yet here and SIEM just isn’t cutting it from a forensic and IR perspective

• Vendors must strive to “play together” for ESIM to become the forensic and IR workbench that WE need it to be

• Some vendors are starting down the path but the ESIM goal is still out of reach

• WE need to teach SIEM vendors forensics!