Process, normalize, categorize, and search forensic evidence within PCAP files

The Challenge

- **Ever-growing zero-day and hard-to-detect memory-based attacks are evading detection for an average of 140 days**
- **High operational cost of solution deployment, management, and monitoring**
- **Lack of sufficient forensic data to piece together critical attack evidence**

Integrated Solution

- **Leverages analysis of internet based artifacts such as webmail, instant messaging, browser history, and more**
- **Identifies delivery mechanisms and payloads to paint a more complete picture of the attack**
- **Ensures email, attachments, instant messages, and other data can be accurately reconstructed and visualized for cyber investigations**

Once a data breach is detected, analysts in an organization's security operations center (SOC) or managed security services provider (MSSP) have limited time to investigate and determine what happened, when and how it happened, and who was involved.

This sense of urgency multiplies each day the incident has gone undetected and for each day the problems remain unremediated. Do multiple attackers have a foothold; is more than one insider responsible for data exfiltration?

Understanding the flow of data in and out of a network is crucial to the identification of unauthorized, illicit, or criminal activity by both insider and outsider threats. Traditionally, packet capture (PCAP) analysis has been a separate discipline from digital forensics. However, with data breaches now an endemic part of doing business, SOCs and MSSPs need a way to merge the two, using PCAP analysis' proactivity to speed up digital forensics' most reactive aspects.

The AXIOM and SentryWire Joint Solution

By combining the forces of Magnet AXIOM with SentryWire, incident responders now have a way to complete in-depth post-mortem and root cause analysis in a fraction of the time it might once have taken them.

Incident responders can use SentryWire with AXIOM to identify attack vector artifacts such as delivery mechanisms and payloads, parsing emails, logs that reflect the use of removable media, and network services to paint a more complete picture of what happened.

Because AXIOM analyzes a breadth of digital data from host systems, responders can conduct more thorough investigations by combining timelines from both affected hosts and PCAPs. A more complete timeline enables the search for events in close temporal proximity to attack vectors.

The SentryWire-AXIOM integration leverages AXIOM's foundation analyzing internet-based artifacts such as webmail, instant messaging, browser history, and more. It also brings AXIOM's powerful reporting and collaboration capabilities to bear, enabling responders to communicate clearly and effectively with key stakeholders at any level.

Key Benefits

- **Complete, in-depth post-mortem and root cause analysis in a fraction of the time**
- **Granular precision on location and nature of an attack**
- **More focused incident response around data transfers or exfiltration attempts**

Alliance Technology Group Security Solutions

- **Risk & Compliance**
- **Vulnerability Assessments**
- **Information Assurance**
- **Product implementations**
- **Independent Verification & Validation (IV&V)**
- **SentryWire - Packet Capture Solutions**

SentryWire

- **Next Generation Packet Capture**
- **Data Driven Security**
- **Managed Security Service**
- **Highly Granular Forensics**
- **Extreme Ingest & Scalability**
- **Major cost reduction in Packet Storage**

How AXIOM Works Together with SentryWire

Process

SentryWire captures the PCAP files and reassembles them for ingestion into AXIOM.

Normalize

PCAPs' unstructured data makes it difficult to perform forensic analysis. By structuring the reassembled data, AXIOM ensures that the email, attachments, instant messages, and other data can be visualized in the same way as data at rest.

Categorize

AXIOM categorizes the newly structured data into recognizable identifying fields including time and date stamps, body content, attachments, and so forth.

Search

Once categorized, the reassembled PCAP data can be searched for keywords. Its time and date metadata can be used to construct timelines.

When to deploy AXIOM with SentryWire

IDS alerts on a suspicious IP address that has been associated with a command and control server.

- SIEM alerts on an unusual logon event pattern that could indicate a brute-force attack.
- Threat hunters reveal a logon pattern consistent with lateral movement.
- A routine audit shows host journal entries from the system of a departed employee that suggest sensitive data exfiltration.

About SentryWire

SentryWire, a Division of Alliance Technology Group, is engineered and architected to be the most efficient packet capture solution on the planet. The system supports capture rates up to 100Gbps and retains network traffic for months and even years at 20% the cost of other systems.
Learn more at www.sentrywire.com

About Magnet Forensics

AXIOM now brings Magnet.AI for automated contextual content analysis, full disk decryption, and more. Get to the data faster with seamless integration of extraction, carving and indexing. Find evidence that others miss. Use multiple data visualization tools for in-depth analysis. Collaborate quickly with stakeholders at all levels.
Learn more at www.magnetforensics.com