filename:comptia-secplussy0601-9-8-1-investigational-data-sources
Topic:Operational Security and Incident Response
Episode:

"*Given an incident, utilize appropriate data sources to support an investigation*"

In this episode, the viewer will identify the appropriate data sources to support an investigation such as SIEM dashboards, log files, logging utilities such as syslog, rsyslog and journalctl as well as metadata netflow and bandwidth monitors following and incident.

---

- SIEM dashboards
- Netflow - Cisco Propriatary
- IPfix - IETF protocol (RFC 7011/5101 )
- Protocol analyzers
    - tcpdump
    - Wireshark

- Log files (Windows)

    - Event viewer
        - Application
        - System
        - Security (Authentication)
        - Dump files (Local machine Preview)

- Log files (Linux)

    - Network logs

```
journalctl -u NetworkManager
```

```
journalctl -u NetworkManager |grep dns
```

- System Logs

```
journalctl| grep systemd
journalctl| grep systemd |tail -n 50
```

- Authentication

```
less auth.log.1
grep session auth.log.1
```

- Centralized Logging is the reality
  - syslog/rsyslog/syslog-ng
  - nxlog

- Metadata
  Email, files, mobile

```
Open gmail click email in question, look for the ellipses at the right of email > Show original
```