Revitalizing the Security Operations Center

Simon Brydone, Marcus Elson & Rob Knoblauch

SecTor
October 9th 2019

Data.

All the Logs.

Challenges related to using logs as a source of detection

- Log transport (global log gathering)
- Log Storage / Capacity Planning
- Log Syntax standardization
- Log Use Cases / Rules and Alerting
- Integration into automated security controls
- Log Analytics
  - Machine Based Learning
  - Boolean Based Approaches
  - Artificial Intelligence

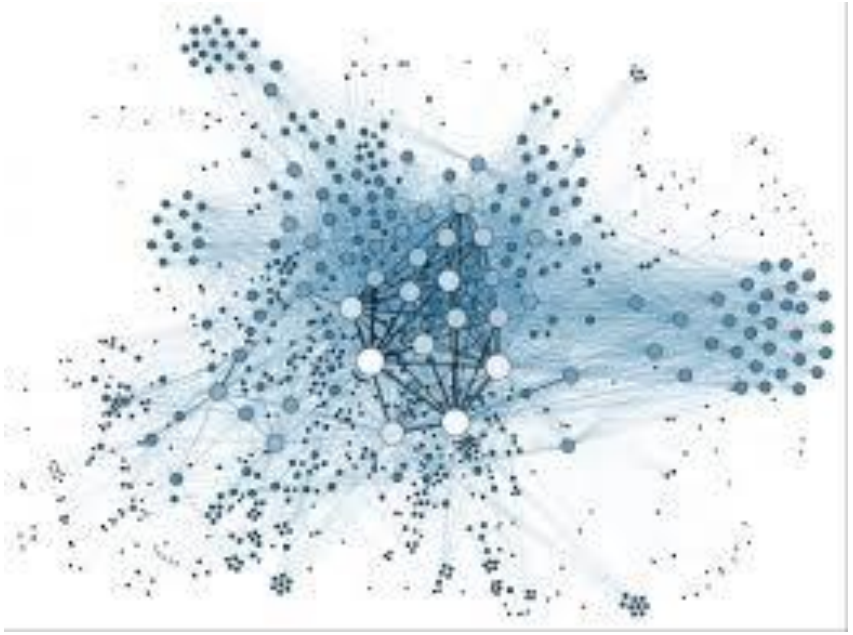
Considerations

- Cost and scalability
- Manual response & process
- False Positives
- Large amount alerts the SOC can’t handle
- Limited search ability
- Asset Inventory
- Case Management / Organizational Processes

Challenges present Opportunity

Innovation.

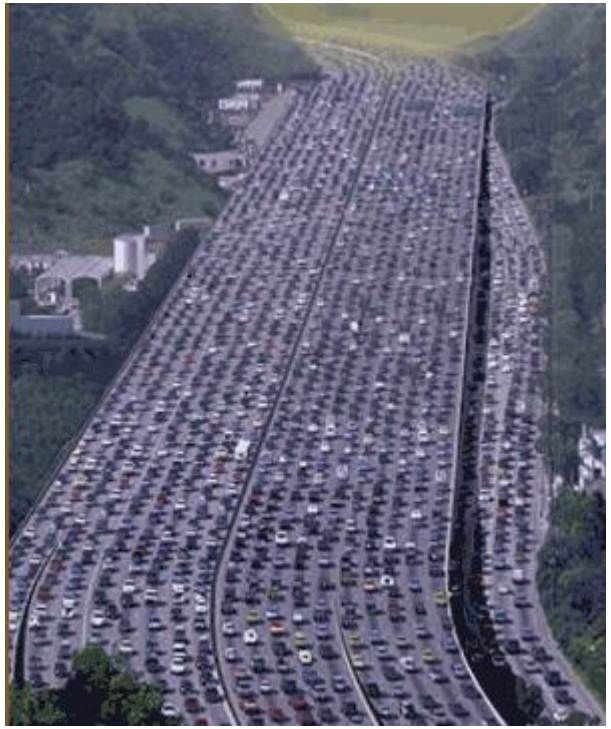
- Detecting the needle, in a haystack of needles.
- Not depending on security controls as a primary source of detection.
- **Financial Crimes** approach to Log Analytics.
  - **Enabling Fraud Analytics**
  - **Enabling Decision Making Sciences**
  - **Enabling User Behavior Analytics**



The Data Highway

The Plumbing.

- Cloud vs On Premises
- Log Aggregation Methodology
- Logs Transportation/Network Impact/QoS
- Log storage & retention requirements
- Log syntax standardization
- Protocol Compatibility
- Data at Rest/Data in Transit (Encryption)



Big Data Analytics for Hunting

Logging Data

The most effective source for detecting, or investigating a potential security event are logs.

- Application Logs
- Infrastructure Logs
- Networking Logs
- Utility Logs
- Identity Access Management Systems
- Security Controls Logs

Issues/Limitations for the hunt team

- Companies do not have a big data platform
- Leveraging SIEM to do big data queries
- Understanding what is normal for an organization

Big Data Analytics for Hunting

- Leveraging unsupervised machine learning
- Leveraging automation in order to identify patterns
- Leveraging existing architecture and database technologies to build baselines around endpoint configurations and processes
- Leveraging machine learning to identify attack patterns based on network traffic
- Interrelationship between different data

Key Messages / FAQs

- Measure twice cut once (determining data requirements and networking impact)
- Be prepared for the onslaught of false positives
- Process behind alerts (Case Management)
- Threat Intelligence

Thank you!