Security Operations and Monitoring

Domain 2.0

Data Analysis in Security Monitoring Activities

Chapter 11

Episode 11.01

Data Analytics

Objective 3.1 Given a scenario, analyze data as part of security monitoring activities.

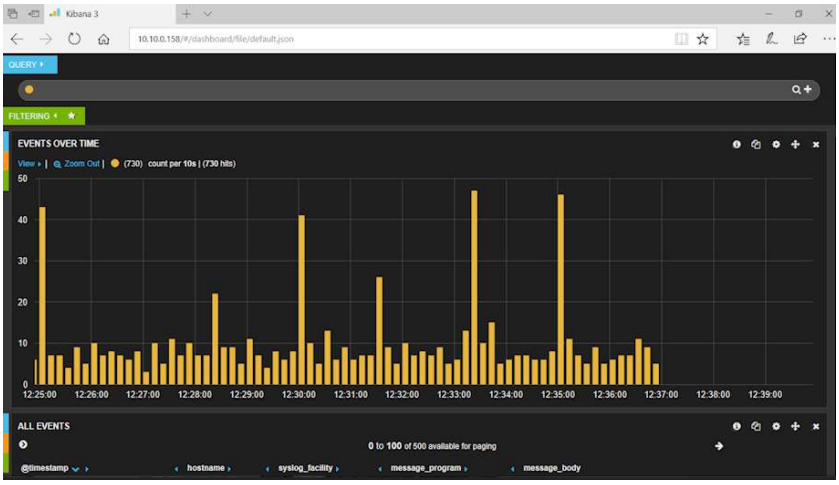
- Trend analysis
- Log review
  - Event logs
  - Syslog
  - Firewall logs
  - Web application firewall (WAF)

Overview

Aggregation

- Sources
- Log managers

Kibana Demo


Kibana 3
10.10.0.158/#/dashboard/file/default.json
QUERY
FILTERING
EVENTS OVER TIME
View | Zoom Out | (730) count per 10s | (730 hits)
50
40
30
20
10
0
12:25:00
12:26:00
12:27:00
12:28:00
12:29:00
12:30:00
12:31:00
12:32:00
12:33:00
12:34:00
12:35:00
12:36:00
12:37:00
12:38:00
12:39:00
ALL EVENTS
0 to 100 of 500 available for paging
@timestamp
hostname
syslog_facility
message_program
message_body

Analytics

- Trend analysis
  - Baseline required
  - Looking for deviations from baselines
- Historical analysis
  - Past behavior used to gain perspective
  - Make informed decisions for defense

Manual Review

- Firewall logs
- Authentication logs
- Event logs
- Syslogs

Syslog

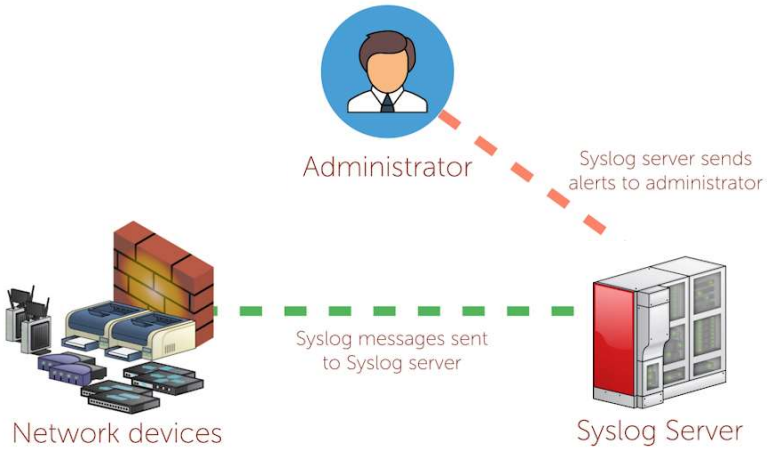
Value	Severity	Keyword	Deprecated keywords	Description
0	Emergency	`emerg`	`panic` [7]	System is unusable. A panic condition.[8]
1	Alert	`alert`		Action must be taken immediately. A condition that should be corrected immediately, such as a corrupted system database.[8]
2	Critical	`crit`		Critical conditions, such as hard device errors.[8]
3	Error	`err`	`error` [7]	Error conditions.
4	Warning	`warning`	`warn` [7]	Warning conditions.
5	Notice	`notice`		Normal but significant conditions. Conditions that are not error conditions, but that may require special handling.[8]
6	Informational	`info`		Informational messages.
7	Debug	`debug`		Debug-level messages. Messages that contain information normally of use only when debugging a program.[8]

https://en.wikipedia.org/wiki/Syslog

Syslogd

- Daemon (service) in Linux
- Collects & records messages from the machine
- Also found in embedded systems
  - Routers, switches, access points, firewalls
- Windows has other options
- Collect logs in one place, can also point to central server for aggregation & analysis

Syslog


Administrator
Syslog server sends alerts to administrator
Syslog messages sent to Syslog server
Network devices
Syslog Server

Episode 11.02

Endpoint Security

Objective 3.1 Given a scenario, analyze data as part of security monitoring activities.

• Endpoint
- Malware
- Reverse engineering
- Memory
- System and application behavior
- Known-good behavior
- Anomalous behavior
- Exploit techniques
- File system
- User and entity behavior analytics (UEBA)

Endpoint Security

- Malware
  - Fingerprinting/hashing
  - Decompose (reverse engineering)
  - Protect against it by detecting and blocking
  - Fileless (in-memory) malware
    - Loads into memory but not stored in the file system
    - Example: rootkits (in part)
  - Test via sandbox

Endpoint Security

- User and entity behavior analytics (UEBA)
  - Create baseline of normal behavior
    - Known-good behavior
  - Makes anomalous/ abnormal behavior easier to detect

Episode 11.03

Recon Results: Part 1

Objective 3.1 Given a scenario, analyze data as part of security monitoring activities.

- Network
  - Flow analysis
  - Packet and protocol analysis
    - Malware
- Log review
  - Intrusion detection system (IDS)/Intrusion prevention system (IPS)
- Security information and event management (SIEM) review
  - Dashboard

Sources of Data

- No shortage of sources
  - IDS (Intrusion detection system) logs
  - IPS (Intrusion prevention system) logs
  - Router & switch logs
  - Firewall logs
  - Packet captures
  - Endpoint logs

Point-in-Time Analysis

- Best for single events
- Tools
  - Packet capture
  - Protocol analysis
  - Network analysis
  - Wireless analysis

Correlation Analysis

- Larger volumes of data
- Looks at trends across a network

Wireshark

- Point-in-time analysis
- Packet & protocol analysis tool
- Connection-oriented
- Cross-platform
- TCP/IP packet sniffer
- Captures & analyzes packets
- Reconstructs network traffic
- Reports statistics

Protocol Analysis

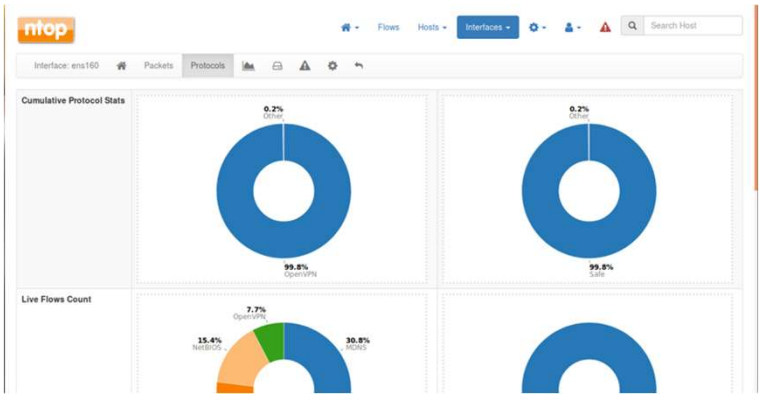
- Know what to expect
- Know what looks ‘off’

Traffic Analysis

- Netflow
  - Cisco developed system
  - Track source & destination events
  - Groups packets into “flows”
- ntop
  - Utility to view the flows

ntop Demo

- Walkthrough
  - Dashboard
  - Packets
  - Protocols

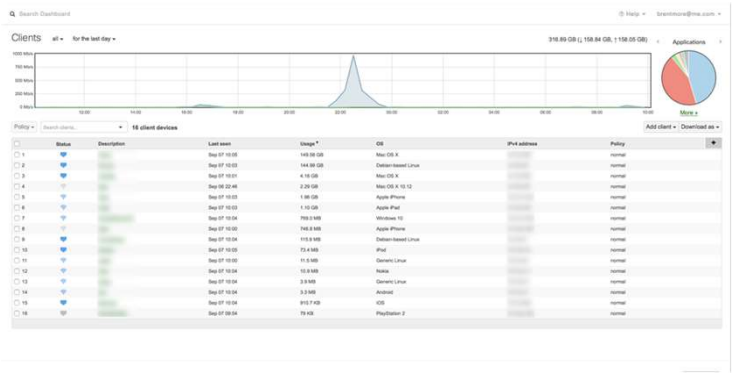


Traffic Analysis

- The challenge with 'real-time'
  - Metadata
  - Computation & storage
  - Sensing
- False positives
- Not always user-friendly interface
- The solution: SIEMs (security information and event management)

Meraki Demo

- Meraki is a SIEM
- Walkthrough
  - Dashboard
    - Spikes correlate with traffic
  - Traffic analytics
  - Event logs



Wireless Analysis

- Wireless modes
  - Managed
  - Ad-hoc
  - Promiscuous
  - Monitor
- Airmon-ng & Airodump demos

Episode 11.03b

Recon Results: Part 2

Objective 3.1 Given a scenario, analyze data as part of security monitoring activities.
• Heuristics
• Security information and event management (SIEM) review
- Rule writing
- Known-bad Internet protocol (IP)
- Dashboard

Heuristic Analysis

- Uses experience over fixed models
- Imperfect craft
- Constantly evolving field
- Best for malware detection
  - Detects suspicious traffic
  - Detects suspicious file changes

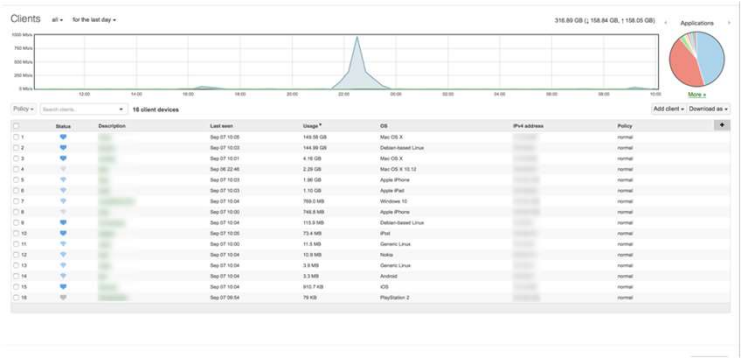
Analyzing the Data

- Security Information and Event Management (SIEM)
  - ELK
  - Splunk
- Analyses
  - Anomaly
  - Behavioral
  - Trend
  - Availability
  - Heuristic

Anomalies

- Visual indicators for traffic
- Baselines
- Spikes and valleys

Meraki Demo



Episode 11.04

Impact Analysis

Objective 3.1 Given a scenario, analyze data as part of security monitoring activities.
• Impact analysis
- Organization impact vs. localized impact
- Immediate vs. total

Impact Analysis

- Pre-emptive
  - Estimates possible impact of any future successful attack
- Post-mortem
  - Determines immediate and ongoing impact of a threat that has already been realized
- Immediate (localized) impact
- Long-term impact
- What's the total impact to the organization?

Impact Analysis

- Availability
  - Tends to have immediate impact
  - Secure systems guarantee confidentiality, integrity, and availability
  - Use resource monitoring tools to analyze
    - Early indicator of an attack

Episode 11.05

Collective Tools

Objective 3.1 Given a scenario, analyze data as part of security monitoring activities.
• Security information and event management (SIEM) review
- Rule writing
- Known-bad Internet protocol (IP)
- Dashboard

SIEMs

- Security information & event management systems
- Collect, store, analyze, & report data
- Normalize data from various logs & compare
- Examples:
  - ArcSight
  - QRadar
  - Splunk
  - Alienvault
  - OSSIMKiwi Syslog
  - ELK

Episode 11.06

Query Writing

Objective 3.1 Given a scenario, analyze data as part of security monitoring activities.

- Query writing
  - String search
  - Script
  - Piping

Query Writing

- SQL (Structured Query Language)
  - Most common
  - Splunk Search Processing Language (SPL)
  - Kibana Query Language (KQL)
  - Apache Lucene

Query Writing

- Simple queries
  - grep
    - Stands for get regular expression
    - Search text files (string search), fetch data, pipe out data however you want
  - Write scripts
    - Useful for avoiding excessive typing

Episode 11.07

Email Analysis, Part 1

Objective 3.1 Given a scenario, analyze data as part of security monitoring activities.
• E-mail analysis
- Malicious payload
- Domain Keys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting, and Conformance (DMARC)
- Sender Policy Framework (SPF)

E-mail Analysis

- Malicious payload
- DomainKeys Identified Mail (DKIM)
- Sender Policy Framework (SPF)
- Domain-Based Message Authentication, Reporting, and Conformance (DMARC)
- Header

Episode 11.08

Email Analysis, Part 2

Objective 3.1 Given a scenario, analyze data as part of security monitoring activities.

- E-mail analysis
  - Phishing
  - Forwarding
  - Digital signature
  - E-mail signature block
  - Embedded links
  - Impersonation
  - Header

E-mail Analysis

- Phishing
- Forwarding
- Digital signatures and encryption
- Embedded links
- Impersonation
- E-mail signature block
  - A digital signature is not the same as the signature block