Practical Network Defense

Master's degree in Cybersecurity 2020-21

SIEM

Angelo Spognardi
spognardi@di.uniroma1.it
Dipartimento di Informatica
Sapienza Università di Roma

Security Information and Event Management (SIEM)

- An approach to cybersecurity combining:
  - Security information management (SIM)
    - Collects log data for analysis, alerting responsible individuals of security threats and events
  - Security event management (SEM)
    - Conducts real-time system monitoring, notifies network admins of important issues, and establishes event correlations
- Generally made of multiple monitoring and analysis components meant to help organizations detect and mitigate threats
  - Not a single tool or application, but a set of different building blocks that all constitute part of a system

No SIEM standard

- There is no standard SIEM protocol or established methodology, but most SIEM systems know how to:
  - automatically collect and process information from distributed sources
  - store it in one centralized location
  - correlate between different events
  - produce alerts and reports based on this information
  - help for compliance and security incident management (digital forensics)
- They can be agent-based or agentless

Security Information and Event Management (SIEM)

- Then, it should be providing the following collection of services:
  - Log management
  - IT regulatory compliance
  - Event correlation
  - Active response
  - Endpoint security
- Log != Event
  - but we talk about "event logging"

Log management

- Nodes in an IT system, particularly the more important or critical nodes, send relevant system and application events (logs) to a centralized database that is managed by the SIEM application
- This SIEM database application first parses and normalizes the data sent by the numerous and very different types of nodes on an IT system
- Then the SIEM typically provides **log storage, organization, retrieval, and archival service**s to satisfy the log management requirements that businesses may have

Logs enable analysis

- The SIEM system lends itself to the additional use of near real-time analysis and data mining on the health and security status of all the IT systems feeding their data into the SIEM system
- The more nodes that feed into your SIEM system, the more **complete** and **accurate** your vision is of the IT system as a whole

IT Regulatory Compliance

- Once logs are stored, you can build filters or rules and timers to **audit** (monitor against a standard) and validate **compliance**, or to identify violations of compliance requirements imposed upon the organization
  - Examples: monitoring the frequency of password changes, identifying operating system (OS) or application patches that fail to install, and the auditing frequency of antivirus, antispyware, and IDS updates for compliance purposes…
- SIEM generally can produce **reports** often needed by businesses to provide evidence of self-auditing and to validate their level of compliance

Event Correlation

- Consider various conditions before triggering an alarm
- The correlation engine on a SIEM can investigate and consider (**correlate**) other events that are not necessarily homogeneous
- It can provide a more complete picture of the health status of the system to rule out specific theories on the cause of given events

Active response

- Activate procedures after the identification of given (security) events
  - Automatic response
  - Manual response
- The SIEM triggered, automated, and active response to the perceived threat would probably occur much faster
  - Like: adding IP and port filters on the access control list (ACL) on a router or firewall

Endpoint Security

- Most SIEM systems can monitor endpoint security to centrally validate the security "health" of a system
- Some SIEM systems can even manage endpoint security, actually making adjustments and improvements to the node's security on the remote system
  - Ex: configuring firewalls and updating and monitoring AV, antispyware, and antispam
- Some SIEM systems can push down and install the updates, or in Active Response mode, adjust the ACL on a misconfigured personal firewall

Logs are fundamental

- Logs are the events that your network produces
- Needed to extract information about the events
- Without them, it is impossible to achieve any security management
- Typical questions:
  - How long must you retain the logs?
    - Data retention and data destruction
  - How much log information will you be required to retain?
  - What kind of information system logs are you required to retain (and eventually analyze)?

Log sources

- Log management apparently easy
- Complicated task as varied sources of information are included and higher levels of functionality, such as filtering, correlating, and reporting, are enabled
- Examples:
  - Syslog of servers and end-user computers
  - Alerts from IDS/IPS and antivirus
  - Flow data
  - Domain controllers
  - Databases
  - Switches and routers
  - VPN gateways
  - Firewalls
  - Web filters and proxies
  - ...

Other points for log

- Which devices will you collect events from?
  - Critical servers, devices providing access to critical servers, IDS
  - Optional: network endpoints (maybe only aggregated via other services)
- Which events will you collect?
  - Debug info, log-in records, configuration changes, alerts...
- How long will you keep the logs?
  - Balance between needs and desires
  - Usually, agree on the regulatory
- Where will you store the logs?
  - Local storage, cloud, hybrid solutions

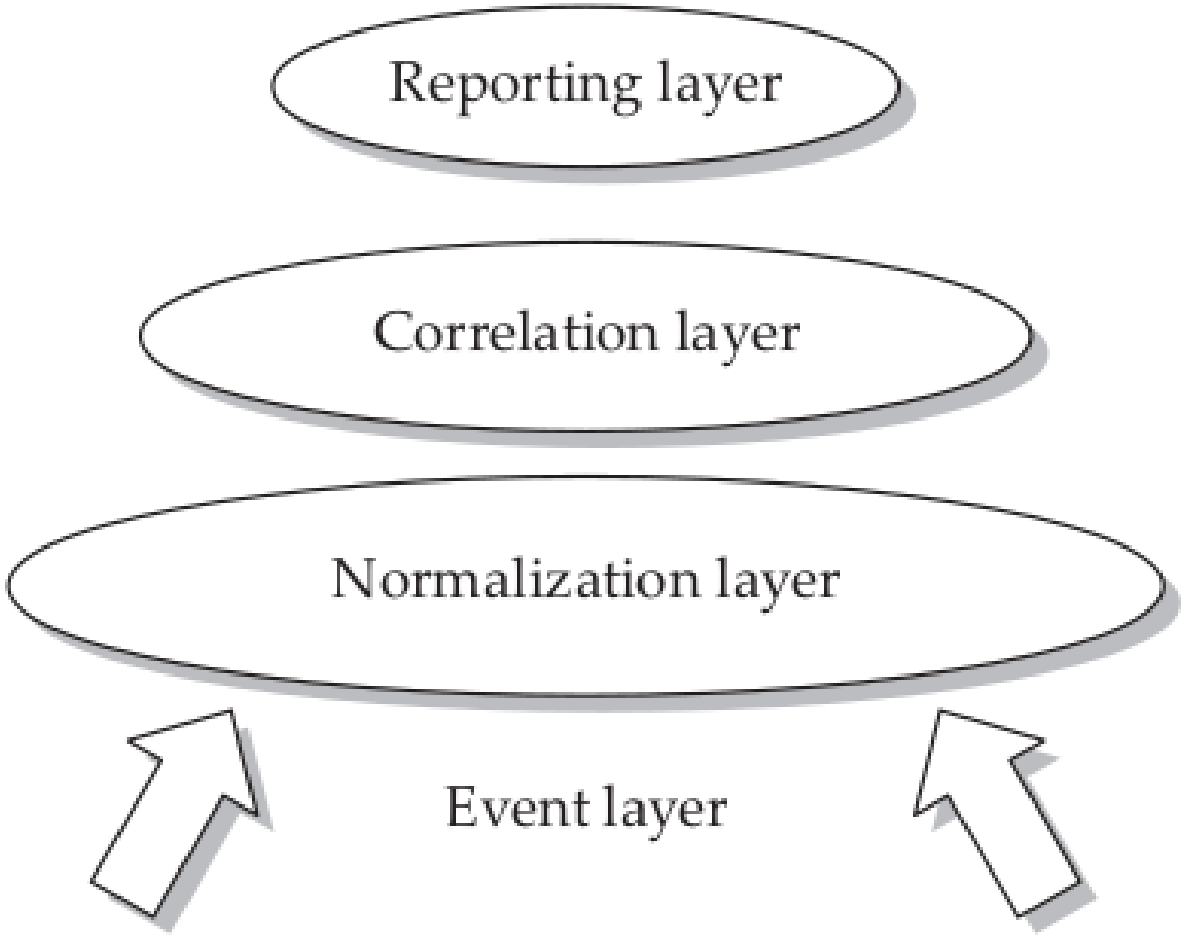
Event data vs state data

- Event data (logs) provide you with an exact list of all events that occurred on your server, network, or website
  - Managing logs tells what happened and when
- State data gives you the view of the overall state of the system
  - Configurations
  - Current applications
  - Active users
  - Processes
  - Registry settings
  - Vulnerabilities

Logging solutions

- Syslog, syslog-NG
- Splunk
- LogStash
- Graylog

SIEM stack


Reporting layer
Correlation layer
Normalization layer
Event layer

Log correlation means

- Monitoring the incoming logs for
  - Logical sequences
  - Patterns
  - Relationships
  - Values
- The ultimate goal is to analyze and identify events invisible to individual systems
- Generally make use of "supporting data"

SIEM supporting data

- Data collected by other sources that can be imported into the SIEM to make comparative determinations
- Example: asset management data
  - Names, IP addresses, operating systems, software versions
  - Geo-location information
- They can be used as weights to prioritize and escalate alerts

Event correlation

- Correlation engines usually are the most distinguishing feature of SIEM
  - And also what the vendors want to sell…
  - Mainly closed source
- Before they have to perform event normalization
  - Message logs are in standard formats, but are not homogeneous
    - "drop" from one vendor firewall, "block" from another
  - Define a common syntax to represent events in the SIEM and apply it to the logs
- Make use of correlation rules
  - Rules that can trigger alerts or actions
    - Example: Perl SEC (Simple Event Correlator), SolarWinds
  - Machine Learning

Endpoint security

- Patching the operating system and major applications
- Antivirus and antispyware updates
- Firewalls—making sure they are on and configured properly
- Host Intrusion Detection Systems (HIDS) and Host Intrusion Protection Systems (HIPS)
- Configuration management
- Management of removable media, such as USB drives and CD and DVD burners
- Network Access Control (NAC)
- Network Intrusion Detection Systems (NIDS) and Network Intrusion Protection Systems (NIPS)

IT regulatory compliance

- All forms of compliance ask the fundamental question related to diligence:
  - Have you taken the steps to perform your responsibilities to securely manage the information in your control—which a reasonable person would expect of someone in your position?
- In other words, if you had to defend your actions in this regard in front of a jury of your peers, would you be comfortable stating that you had used available best practices and sufficient effort to perform your duties?
  - Think about GDPR

Provide evidences of best practices

- Implementing technologies to protect and detect intrusions is not enough
- This should be **provable**
- The log server has to be reliable. For example
  - Use TCP transport
  - Use encrypted storage
- Moreover, it could be important to also sign the logs
  - Authentication and integrity

Compliance tools

- SIEM can also include compliance checklists
  - Ex: SPLUNK
- The reports that SIEM can generate can be used as evidences for the IT regulatory compliance
  - Example: https://gdpr.eu/checklist/
- Proper configuration can be quite complex → professionals of regulatory compliance

Additional features

- Support for open-source threat intelligence feeds
- Real-time analysis and alert (IDS-like)
- Optionally, automated response (IPS-like)
- Advanced search capabilities
  - Elasticsearch
- Historical and forensic analysis

Threat intelligence

- Threat intelligence feeds and reports help security officers in making decisions concerning organizational security
- Threat intelligence is the analysis of data using tools and techniques to generate meaningful information about existing or emerging threats targeting the organization that helps mitigate risks
- Threat Intelligence helps organizations make faster, more informed security decisions and change their behavior from reactive to proactive to combat the attacks

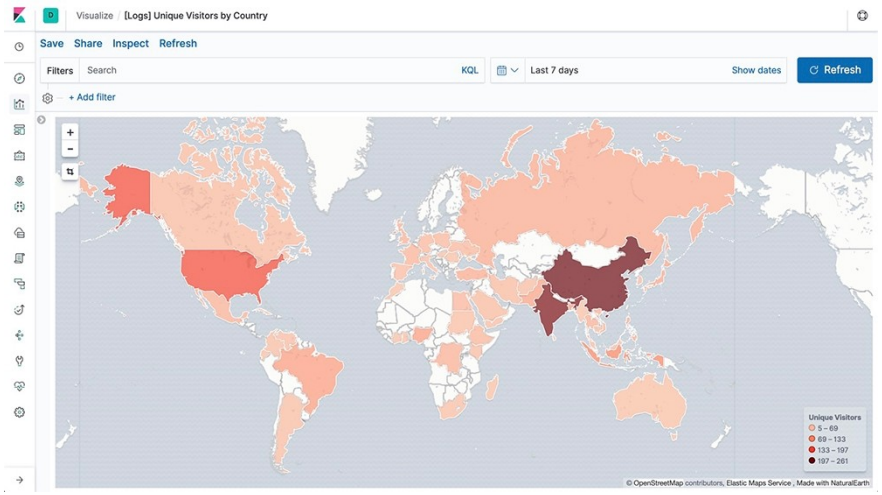
Digital forensics

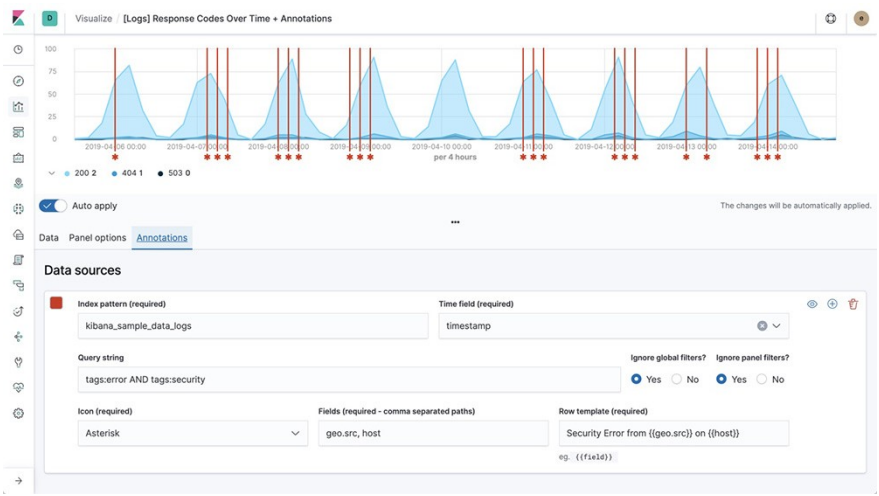
- Digital forensic science is a branch of forensic science focused on the recovery and investigation of material found in digital devices and cybercrimes
- Digital forensics was originally used as a synonym for computer forensics but has expanded to cover the investigation of all devices that store digital data
- Digital forensics is concerned with the identification, preservation, examination and analysis of digital evidence, using scientifically accepted and validated processes, to be used in and outside of a court of law

SIEM operational interfaces

- Dashboards and maps → pull of information
  - A way to present information in a way that administrators can understand at glance
  - It is a graphical and organized representation of alerts, event data, and statistical information
  - It allows administrators to see patterns, understand trends, identify unusual activity
  - Dashboards are also key differentiator among the different SIEM products on the market
- Alerts → push of information
  - Do not require human diligence to notice something important is happening

Dashboards and maps

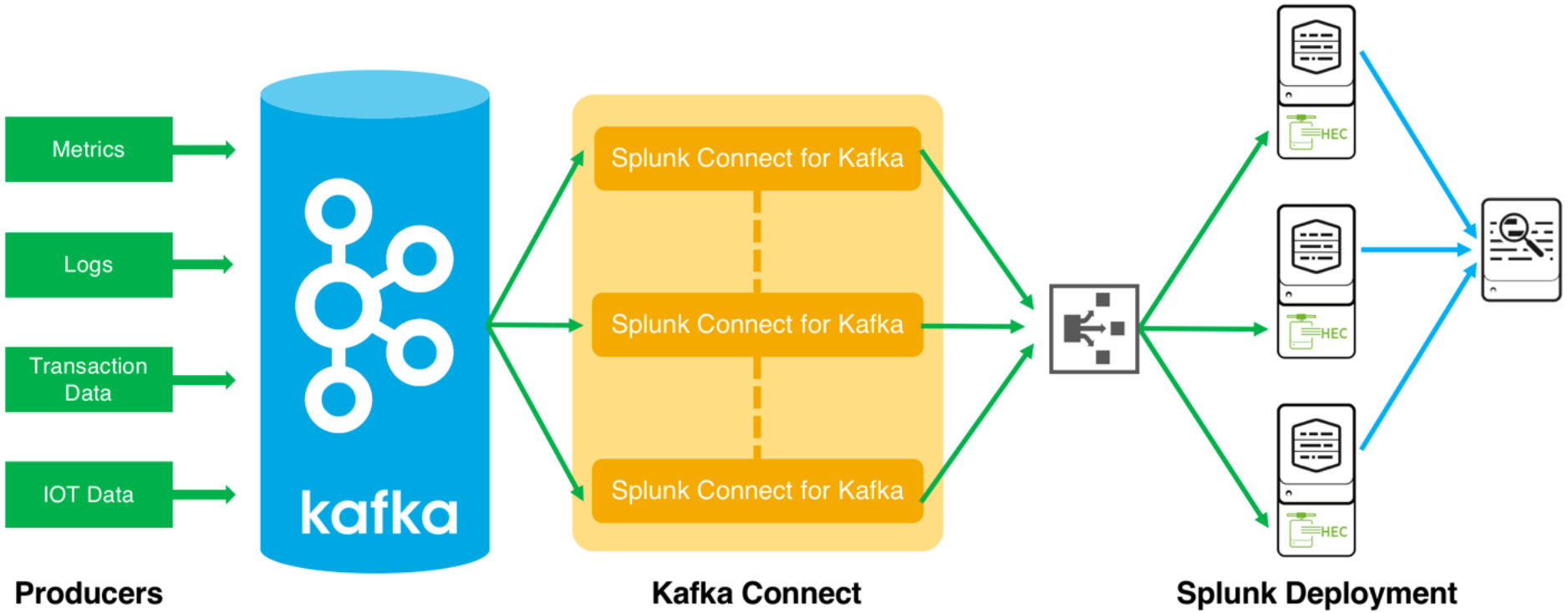




SIEM → complexity!

- A survey conducted in 2013 by elQnetworks revealed that:
  - "managing the complexity of the product is considered the biggest headache when using SIEM
  - followed by lack of trained personnel to manage the product
  - and lack of integration with other products"
  - 31 percent would prefer to replace their existing SIEM solution for better cost savings
  - 25 percent have invested more than month in professional services since the implementation of their current SIEM solution
  - 52 percent require two or more full-time employees to manage the chosen solution

SIEM complexity: clustered setting



https://www.splunk.com/blog/2018/04/25/unleashing-data-ingestion-from-apache-kafka.html

SIEM tools

- Splunk
- OSSIM – Alien Vault
- Security Event Manager (SEM) – SolarWinds
- AT&T Cybersecurity
- IBM QRadar
- RSA NetWitness Platform (RSA NWP) – Dell Technologies
- Security Management Platform (SMP) – Exabeam
- ArcSight ESM – Micro Focus
- LogRhythmNextGen SIEM Platform
- SELKS distribution
- Graylog
  - http://www.cryptos.com.mx/mx/sites/default/files/Gartner_MQ_SIEM_2020.pdf

That's all for today

- **Questions?**
- See you next lecture!
- Suggested reading: https://www.sans.org/reading-room/whitepapers/detection/paper/37477
- References:
  - Security Information and Event Management (SIEM) Implementation, D. Miller, S. Harris, A. Harper, S Vandyke, C. Blask, McGrawHill, 1st ed. 2011
  - Security Event Correlator: https://simple-evcorr.github.io/
  - SEC ruleset (check the thesis): https://github.com/markuskont/SagittariuSEC/
  - Kibana 5 introduction video, live demo
  - SELKS distribution: https://github.com/StamusNetworks/SELKS

Student's Opinions Questionnaires (OPIS)

- For the Practical Network Defense course
- Two options:
  - the infostud app (probably best option)
  - the infostud website
    - follow the following instructions https://www.uniroma1.it/sites/default/files/field_file_allegati/vadevecum_opis_eng_27_11_2018_002_modalita_compatibilita.pdf
    - use this course code **1Q85HJ66**
- **Be (pro-)positive!**