

SIEM Overview with OSSIM Case Study

Mohammad Husain, PhD

Cal Poly Pomona

SIEM

- SIEM = Security Information and Event Management
- Collects security information from multiple sources; internal and external to an organization
- Detects **anomalies** in the collected security information and tries to **correlate** multiple anomalies to interpret whether a particular incident is related to a potential attack
- An organization can use the information within the SIEM to **effectively** respond and detect security incidents

But skeptics say ...



Image Courtesy: [3]

Once upon a time ...

Intrusion Detection System (IDS): **report** intrusions by out of band detection

Intrusion Prevention System (IPS): **block** intrusions by in band filtering

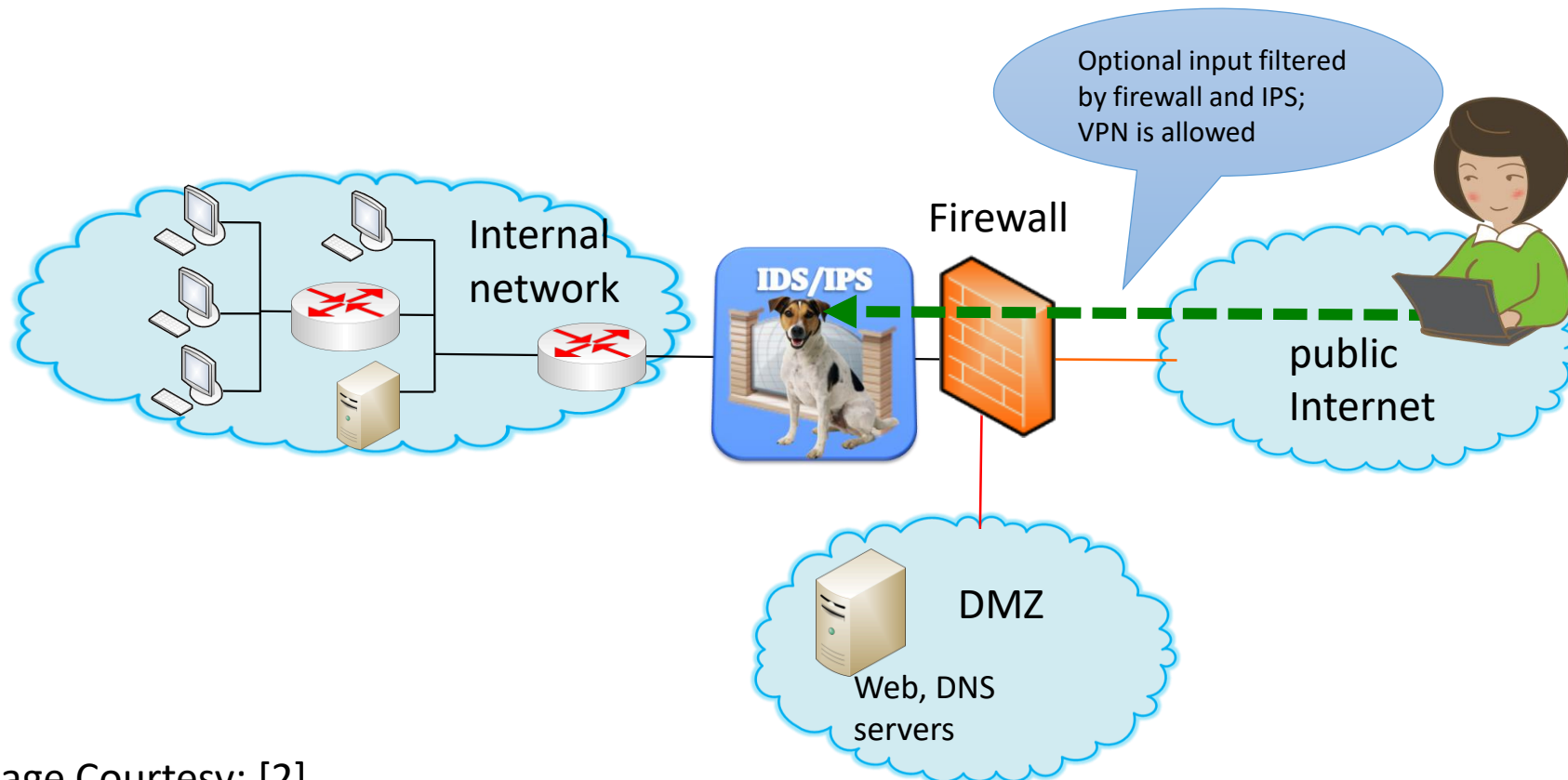
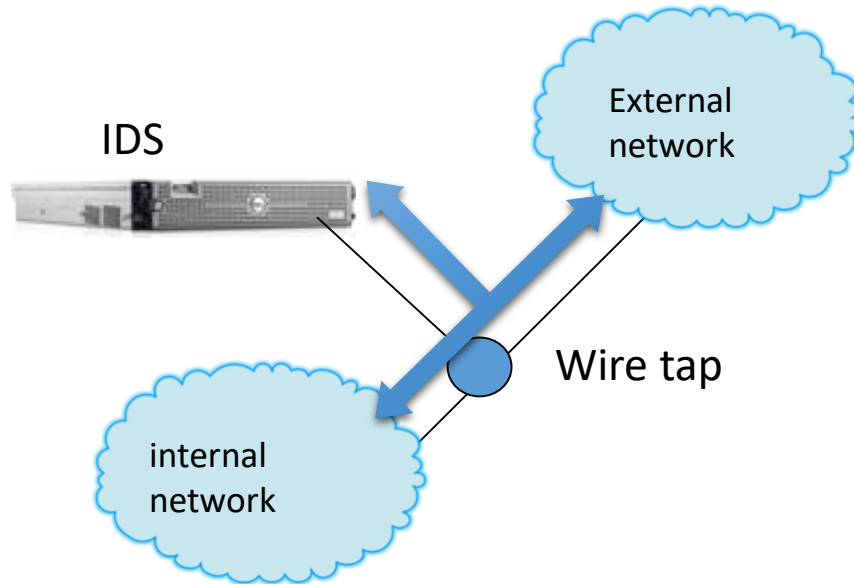


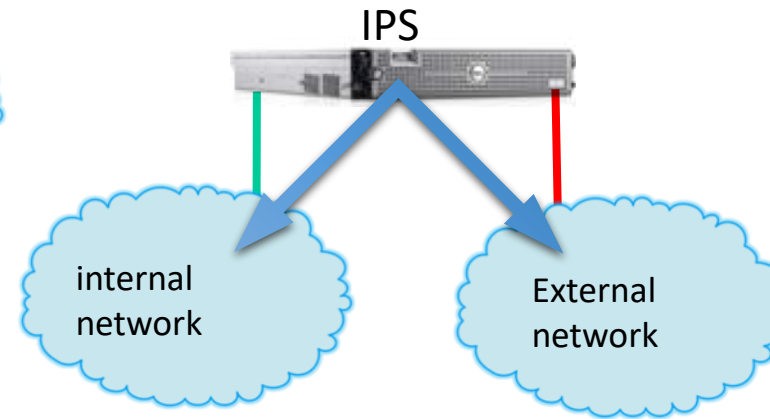
Image Courtesy: [2]

IDS vs. IPS

IDS: out of band



IPS: in line



The Bigger Picture

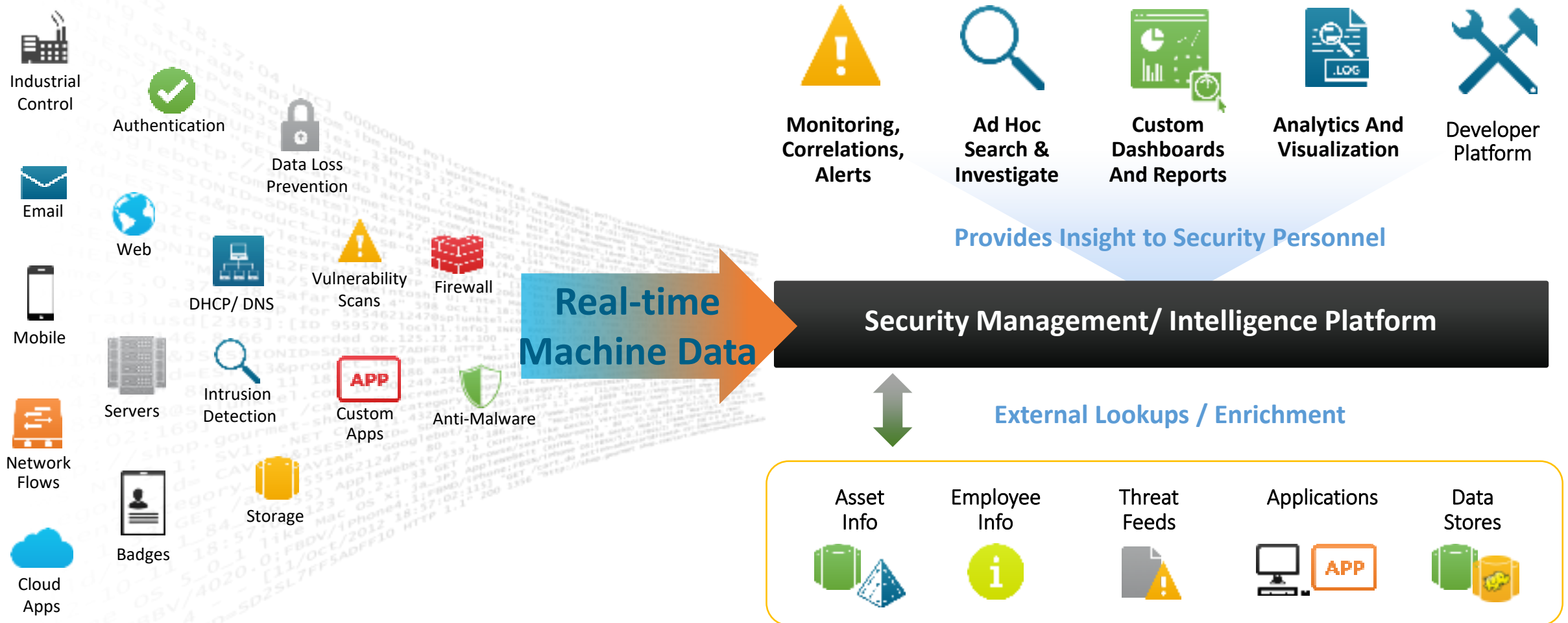


Image Courtesy: Splunk

Host-Based IDS/IPS (HIDS/HIPS)

- Protects against:
 - local attacks from a user, and codes/scripts from removable devices
 - attacks from the same subnet/VLAN
- Con:
 - if an attacker takes over a host, then one can tamper with IDS/agent binaries and modify audit logs
 - only local view of the attack
- Analyzing, and comparing with the database for
 - system calls, sequence of system calls
 - logs/ file-system modification
 - integrity of system binaries
 - password files
 - access control and privilege escalation

Network-based IDS/IPS (NIDS/NIPS)

- Deploying sensors at strategic locations with a central monitor in the network
 - E.G., Packet sniffing via *tcpdump* at routers
 - watch for violations of protocols and unusual connection patterns
- Protects against
 - network-oriented attacks such as DDoS
 - monitoring user activities by looking into the data portions of the packets for malicious command sequences
- Con:
 - may not detect encrypted traffic, as data portions and some header information can be encrypted
 - cannot detect some attacks in the host

The genesis of SIEM

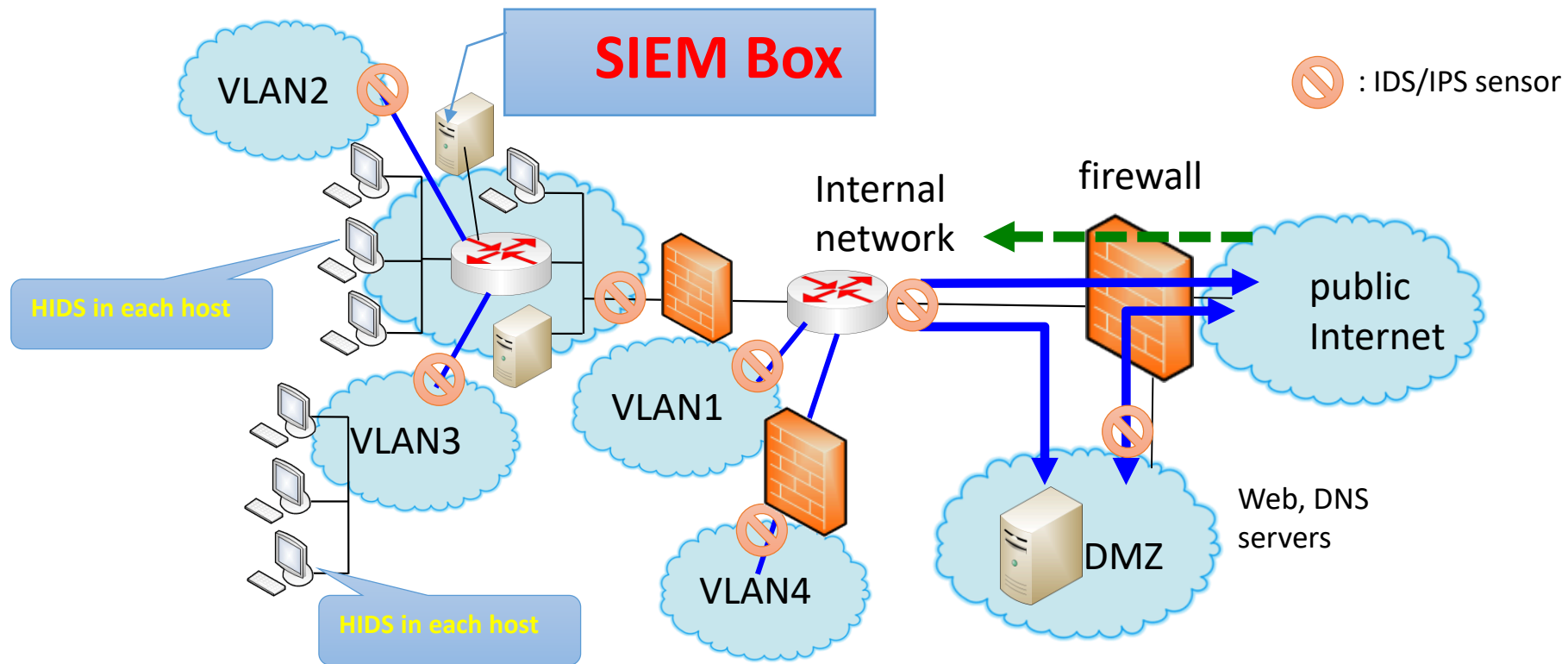
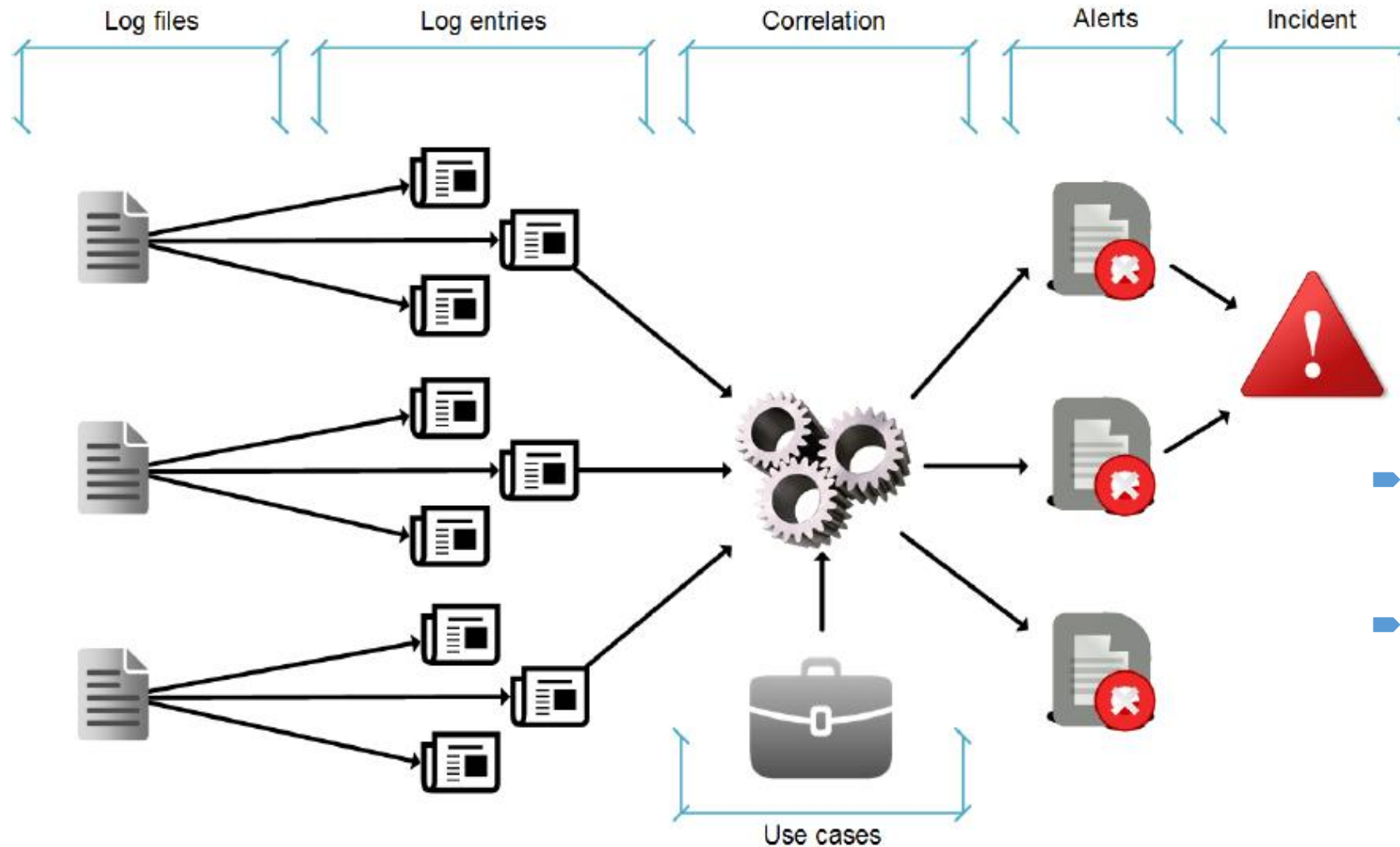


Image Courtesy: [2]

SIEM Process



- Most alerts require manual analysis by a SOC analyst
- Experience gained from handling incidents or false-positives can serve as an input for a new use case or for fine-tuning

Image Courtesy: [1]

SIEM Comparison (Gartner, Aug 2016)

| Critical Capabilities | AlienVault | BlackStratus | EMC (RSA) | EventTracker | Fortinet (AccelOps) | HPE (ArcSight) | IBM Security | Intel Security | LogRhythm | Manage Engine | Micro Focus (NetIQ) | SolarWinds | Splunk | Trustwave |
|-------------------------------------|------------|--------------|-----------|--------------|---------------------|----------------|--------------|----------------|-----------|---------------|---------------------|------------|--------|-----------|
| Real-Time Monitoring | 2.7 | 1.8 | 3.3 | 2.2 | 2.8 | 3.3 | 4.1 | 3.7 | 4.5 | 2.0 | 2.8 | 2.1 | 4.3 | 2.0 |
| Incident Response and Management | 2.3 | 2.7 | 3.8 | 2.1 | 2.6 | 2.9 | 4.2 | 3.1 | 4.0 | 1.2 | 2.3 | 2.1 | 4.2 | 2.5 |
| Advanced Threat Defense | 2.5 | 1.4 | 3.8 | 1.8 | 1.7 | 2.7 | 3.5 | 3.0 | 4.1 | 1.0 | 1.7 | 1.1 | 4.0 | 1.4 |
| Business Context and Security Intel | 1.7 | 1.8 | 3.8 | 1.5 | 2.0 | 2.9 | 4.1 | 3.6 | 2.8 | 1.0 | 1.7 | 1.0 | 3.9 | 1.5 |
| User Monitoring | 2.3 | 2.0 | 3.5 | 2.3 | 2.5 | 3.1 | 3.7 | 3.5 | 4.1 | 2.0 | 3.5 | 2.3 | 4.3 | 2.5 |
| Data and Application Monitoring | 2.1 | 1.7 | 3.9 | 1.4 | 2.0 | 3.3 | 3.3 | 3.7 | 3.9 | 1.0 | 2.7 | 2.5 | 4.0 | 1.8 |
| Advanced Analytics | 1.5 | 1.9 | 3.7 | 1.4 | 1.7 | 3.0 | 4.0 | 2.7 | 3.9 | 1.0 | 1.2 | 1.0 | 4.5 | 1.0 |
| Deployment and Support Simplicity | 3.3 | 3.0 | 3.3 | 3.1 | 3.0 | 2.7 | 3.9 | 3.7 | 4.5 | 2.0 | 3.1 | 3.0 | 4.2 | 3.4 |
| As of August 2016 | | | | | | | | | | | | | | |

Table 2. Weighting for Critical Capabilities in Use Cases

But skeptics say ...



Image Courtesy: [3]

Hands-on: Alien Vault OSSIM

- Open Source
 - <https://www.alienvault.com/products/ossim>
- Download and installation
 - <https://youtu.be/Xfa-zlYhX3c>
- Configuration of OSSIM
 - <https://youtu.be/y2F3VqOXzus>
- Attack event scenarios
 - <https://youtu.be/WGNmIR8Lqgo>

Research Question

- What if the SIEM box is compromised?
 - Thoughts?
- How about using SIEM in a Software-as-a-Service scenario
 - Thoughts?

But skeptics say ...



Image Courtesy: [3]

References

[1] van de Moosdijk, Jarno, and Daan Wagenaar. "Addressing SIEM." (2015)

<http://www.vurore.nl/images/vurore/downloads/scripties/2030-Def-scriptie-Jarno-van-de-Moosdijk---daan-Wagenaar.pdf>

[2] Introduction to Computer Networks and Cybersecurity. Chwan-Hwa (John) Wu and J. David Irwin. CRC Press

[3] <http://www.curphey.com>