ALIEN VAULT - OSSIM

By Arun

Date: 17 Oct 2019

- Open Source SIEM (OSSIM)
  - Commercial Version is called Unified Security Management (USM)
  - World’s most popular open source SIEM.
  - 5 in One product.
    - Asset Discovery & Inventory
    - Vulnerability Assessment
    - Intrusion Detection
    - Behaviour Monitoring
    - SIEM Event Correlation.

OSSIM vs USM

	AlienVault OSSIM™	USM Anywhere™
PRODUCT AVAILABILITY	Open Source Software Download	Cloud-Hosted Service
PRICING	Open Source	Annual Subscription Pricing VIEW PRICING OPTIONS ›
SECURITY MONITORING	On-premises Physical & Virtual Environments	AWS & Azure Cloud Environments Cloud Apps On-premises Physical & Virtual Environments
DEPLOYMENT ARCHITECTURE	Single Server Only	SaaS Delivery with sensors deployed in each monitored environment Federation-ready

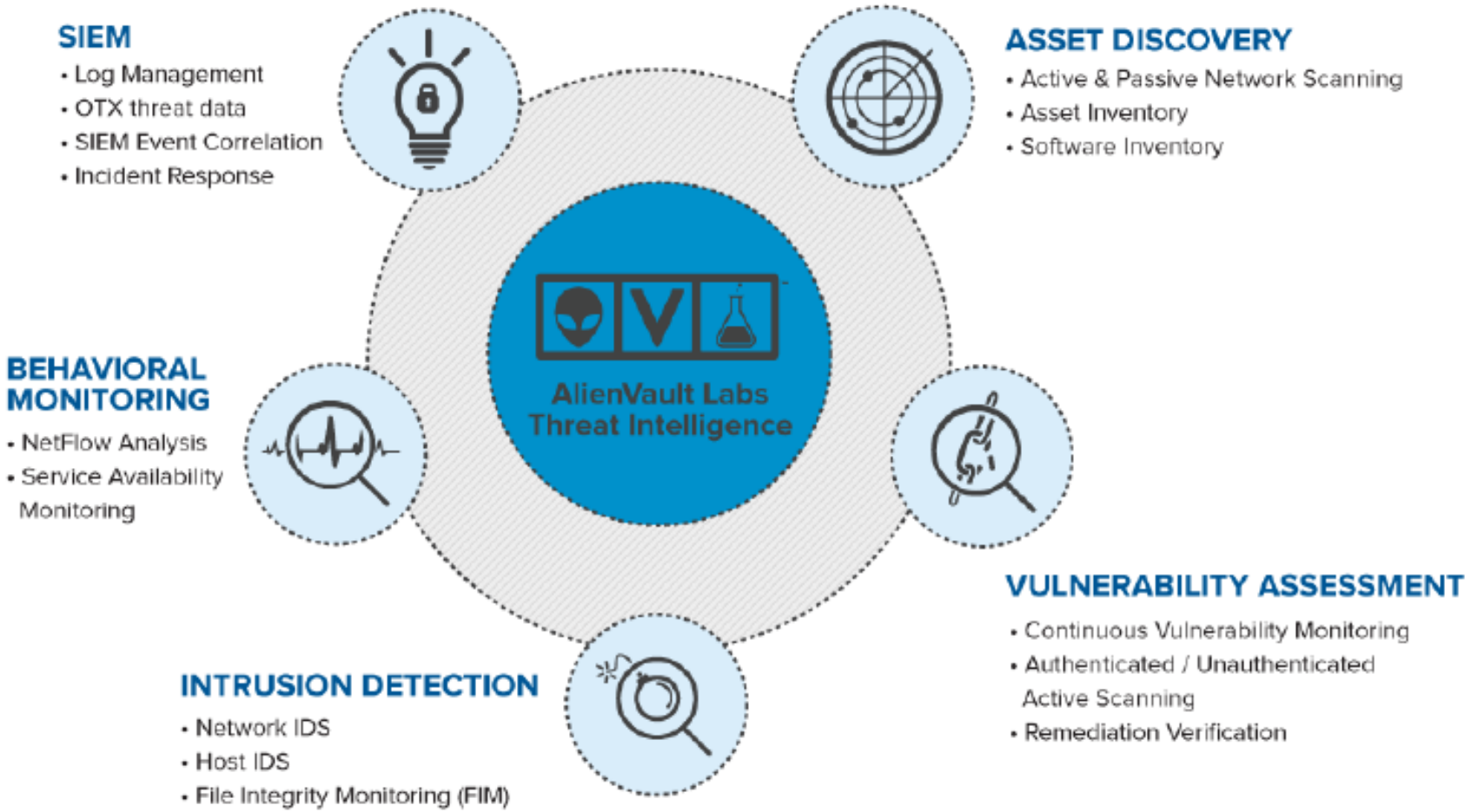
https://qostechnology.in/

OSSIM vs USM

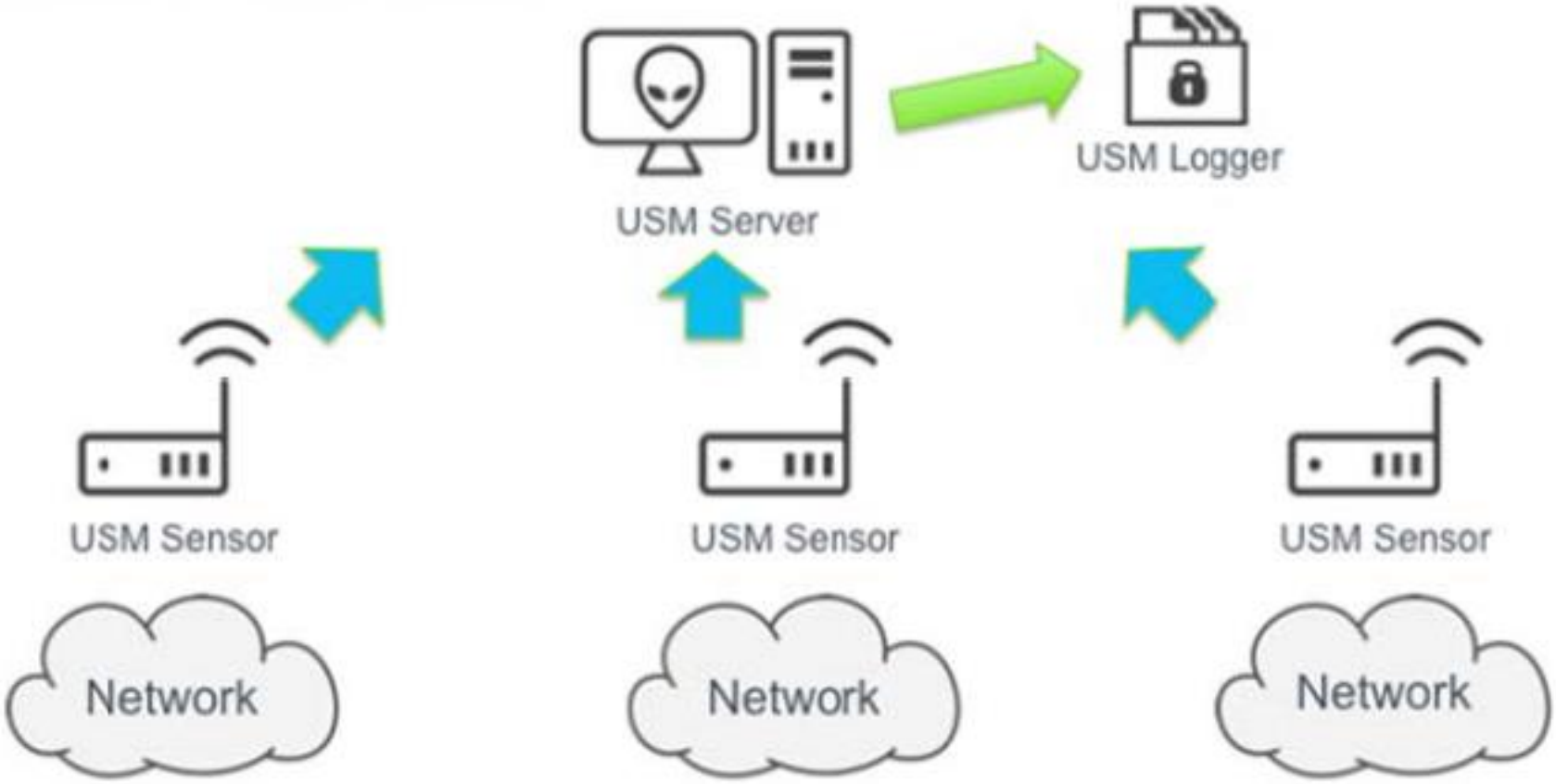
Security Capabilities:		
ASSET DISCOVERY & INVENTORY	✓	✓
VULNERABILITY ASSESSMENT	✓	✓
INTRUSION DETECTION	✓	✓
BEHAVIORAL MONITORING	✓	✓
SIEM EVENT CORRELATION	✓	✓
LOG MANAGEMENT	✗	✓
AWS & AZURE CLOUD MONITORING LEARN MORE ›	✗	✓
CLOUD APPS SECURITY MONITORING	✗	✓

https://qostechnology.in/

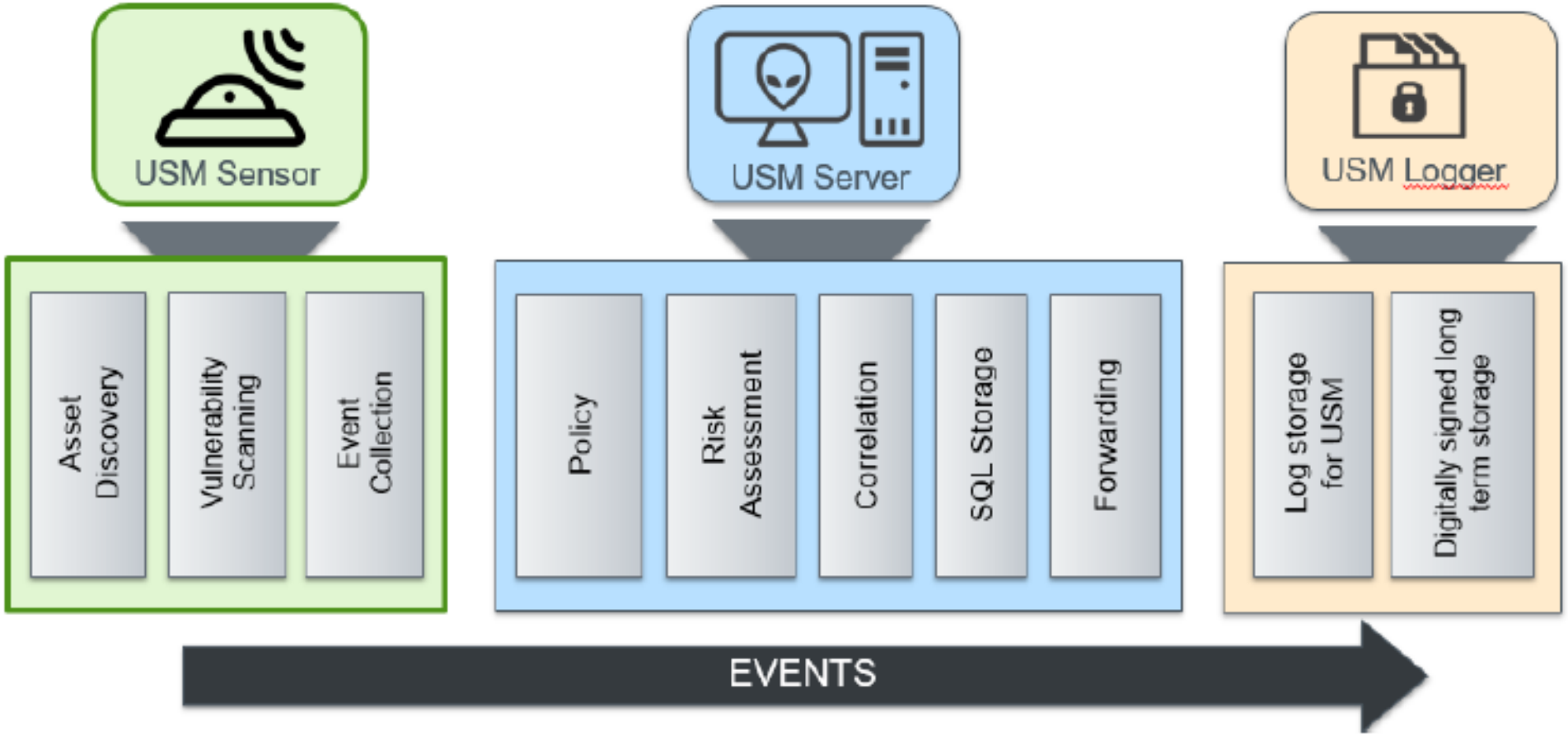
AlienVault USM



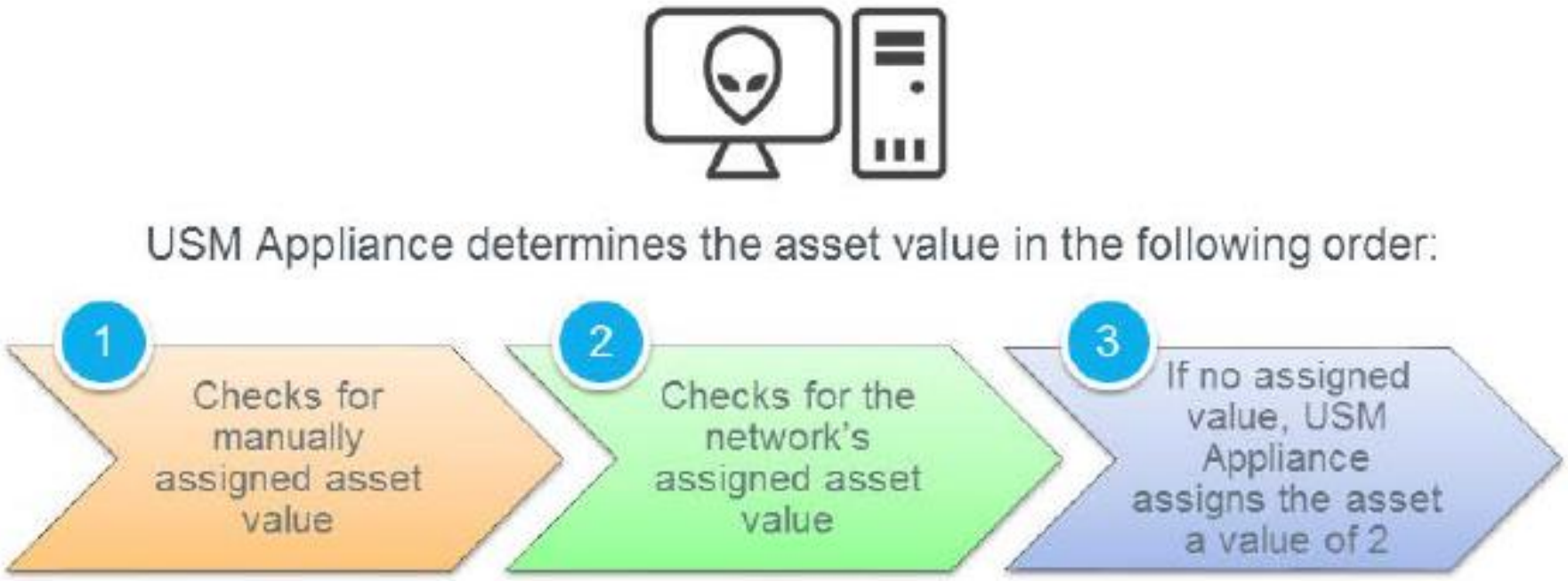
OSSIM/USM Architecture



OSSIM/USM WORK FLOW

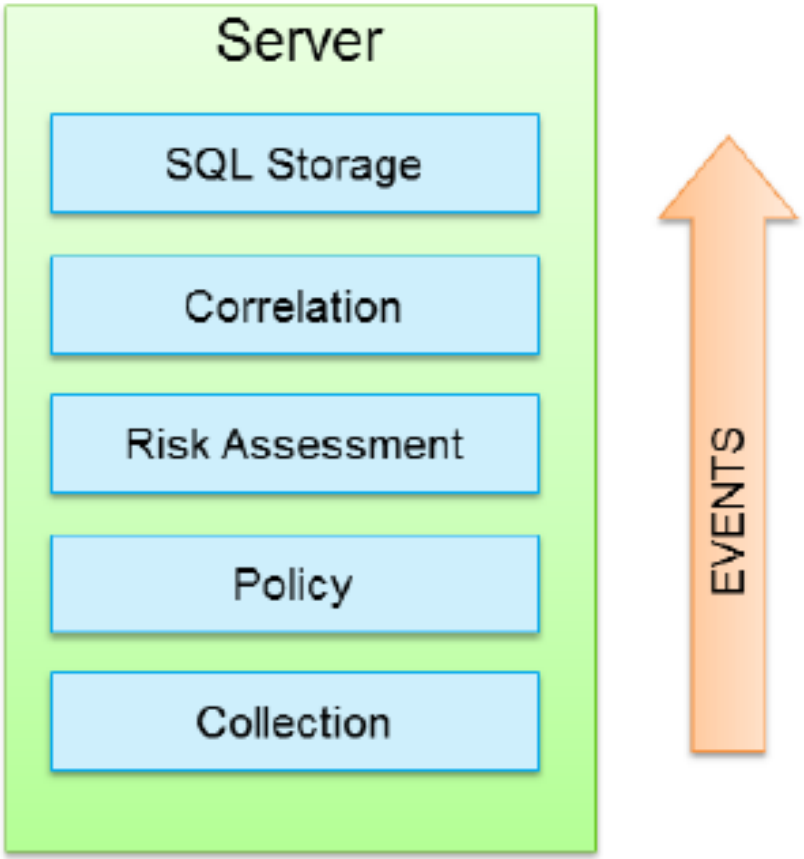


HOW ASSET VALUE IS CALCULATED



EVENTS

- Any log entry generated by any data source at application, system, or network level is an event
- It is important to know:
  - When was the event generated?
  - What is involved? (systems, users)
  - Which data source generated the event?
  - What's the event type?
  - What is the event risk?

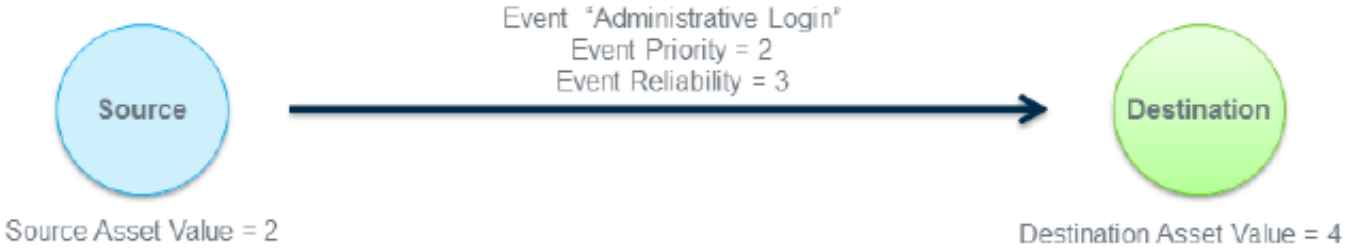


EVENT PRIORITY AND RELIABILITY

- PRIORTY [0-5] – 0 Means Not important; 5 Means very important.
- RELIABILITY [0-10] – 0 Means False Positive; 10 Means Real Attack.

CALCULATING RISK SCORE

- The Server calculates a risk for each processed event.
- The event risk is an integer (0-10).



Risk ≈ (*Asset Value* * *Event Priority* * *Event Reliability*) / 25

For the Risk calculation the higher asset value will have preference

Risk ≈ (*4* * *2* * *3*) / 25

- Higher of Src or Dst Asset value will be selected.
- The Final Integer Risk value [0-10] will be rounded down.
  - 0.95 => 0
  - 1.33 => 1
- Risk of 1 or more will be considered as an Alarm.

Thank You

https://qostechnology.in/