VERSPRITE

Why Traditional SIEMs Are Falling Short

Absent Threat Models Impact SIEM Effectiveness

VERSPRITE

1 Security Operation Centers do not leverage threat models to contextualize SIEM alerts

2 Signature based alerts may extend focus to triaging more false positives or extraneous alerts

PASTA Threat Model

Data Overload Fatigues Detection

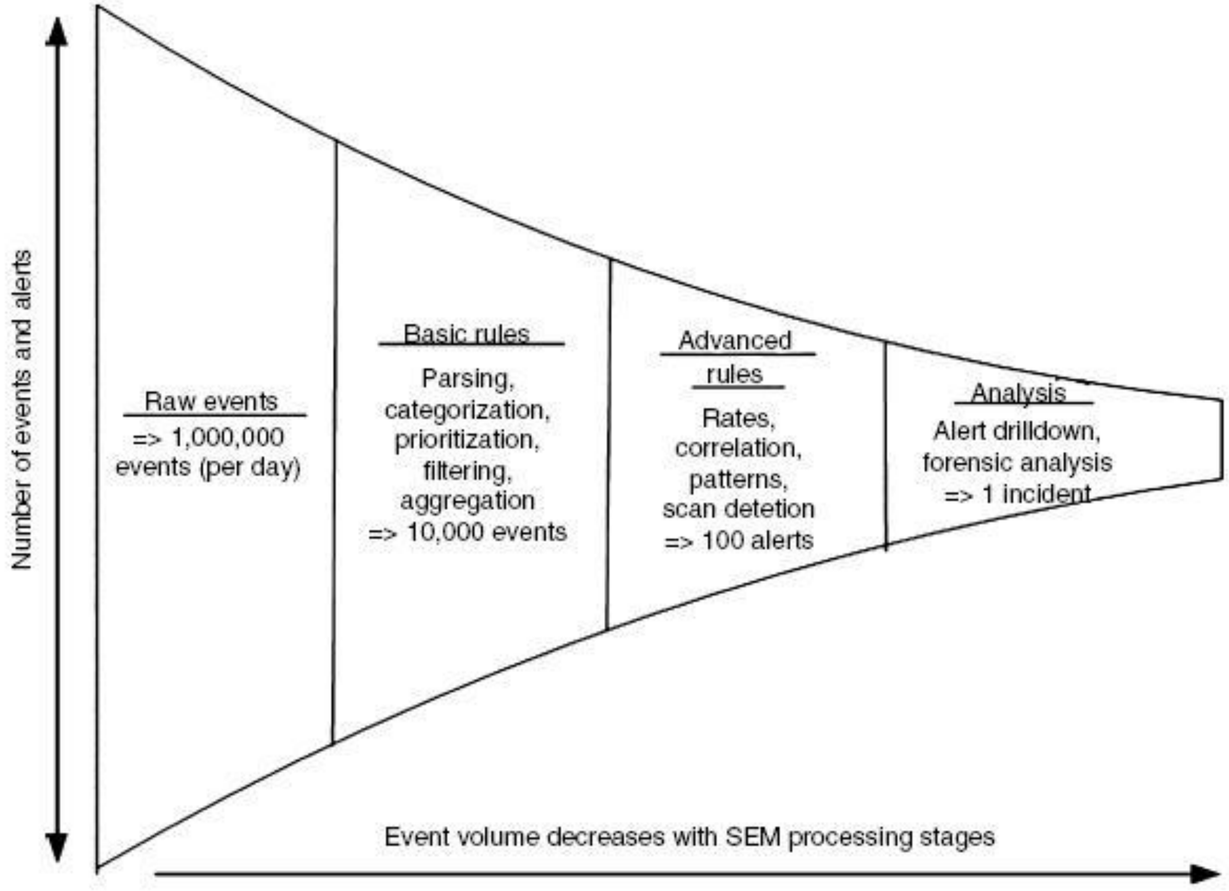
1 SIEMs often represent an endless, list of alerts which may correlate to likely threats for the organization.

2 Correlation capabilities are still primitive & devoid of **threat | impact | target** context

Broken Event Correlations

1 Overly simple correlation rules from SIEM products

2 SIEM products can ‘box’ analysts to only considering events correlated at a more generic level.



Poor Integrity of Threat Intel

1. Rise of ‘fake’ intel tainting SIEM events

2. Gap exists between threat related information & observed attack patterns

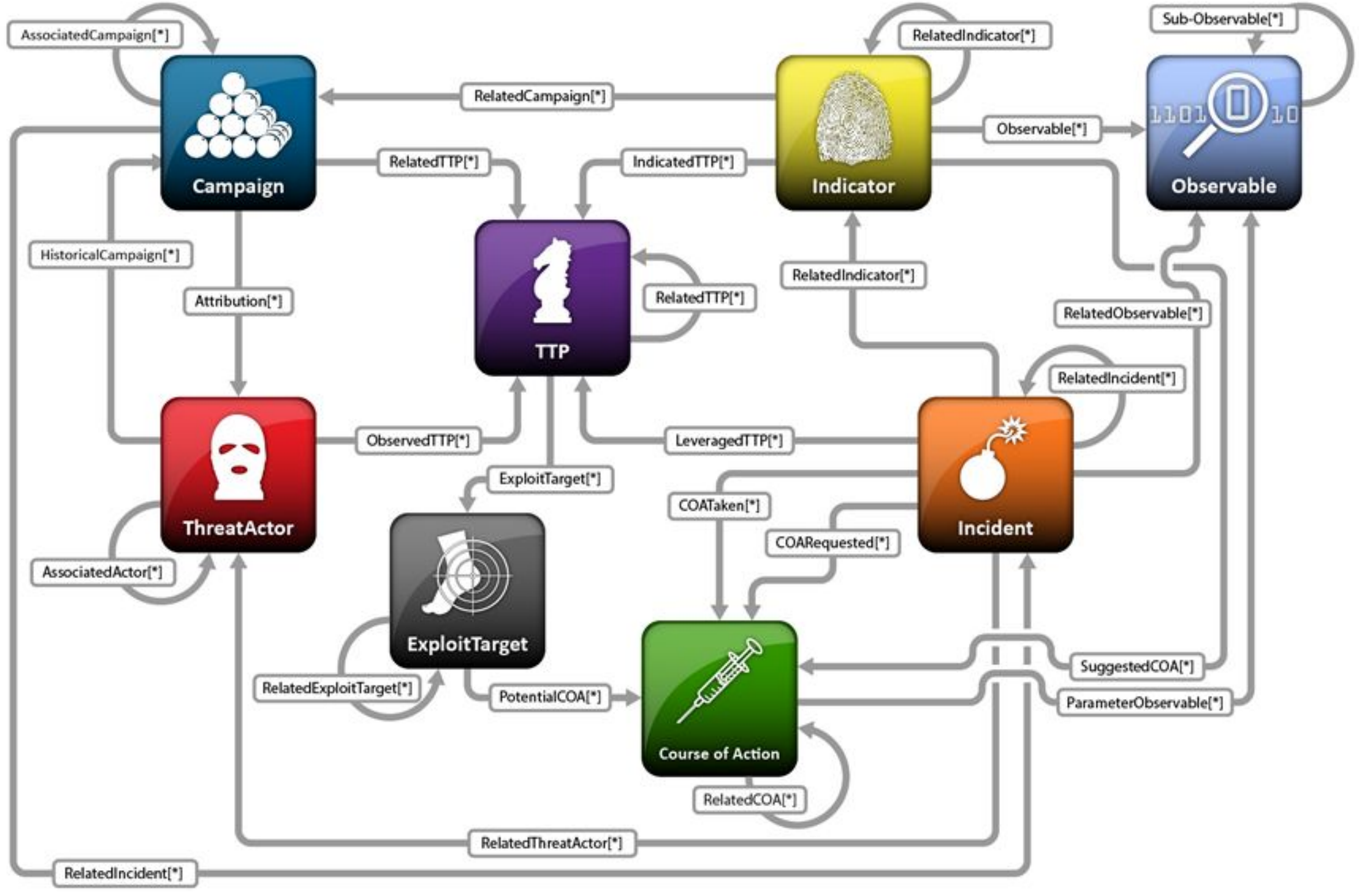
Understanding Emerging Threats for Improved SIEMs

VERSPRITE

1 Gaps exist between threat related information & observed attack patterns

2 Conceptualizing threat patterns to attack patterns to targets helps configure SIEMs for focused security operations

3 Threat models help greatly to contextualize & interlink threat information to emerging attack patterns.



VERSPRITE

Tony UcedaVélez

CEO & Founder, VerSprite

VerSprite.com - Global Security Firm

- OWASP Atlanta Chapter Leader (past 10 years)
- Author, "*Risk Centric Threat Modeling – Process for Attack Simulation & Threat Analysis,*" Wiley June 2015
- Passionate global, threat modeling evangelist
- Dreams of bankrupting #infosec with intelligent, threat inspired DevSecOps automation

LinkedIn.com/tonyuv **@t0nyuv**