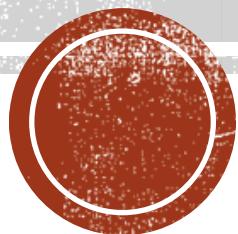


SIEM - KEY PERFORMANCE INDICATOR

Paulus Tamba



ABOUT ME

- Analyst in training
- 12 years in infosec and counting
- Interested in T&VM, Security Operations, Risk and Compliance
- Was with Verizon-Cybertrust, BT, & FireEye
- Founded KPI on 2014
- <https://www.linkedin.com/in/paulustamba/>



CREDITS

- Lots and lots of Anton Chuvakin thoughts on SIEM
 - <https://blogs.gartner.com/anton-chuvakin/>
 - <http://www.securitywarrior.org/>
- Arcsight Whitepaper
 - Security Operations Metrics Definitions and Operations Team
- Various publications on the internet



LETS TALK SIEM

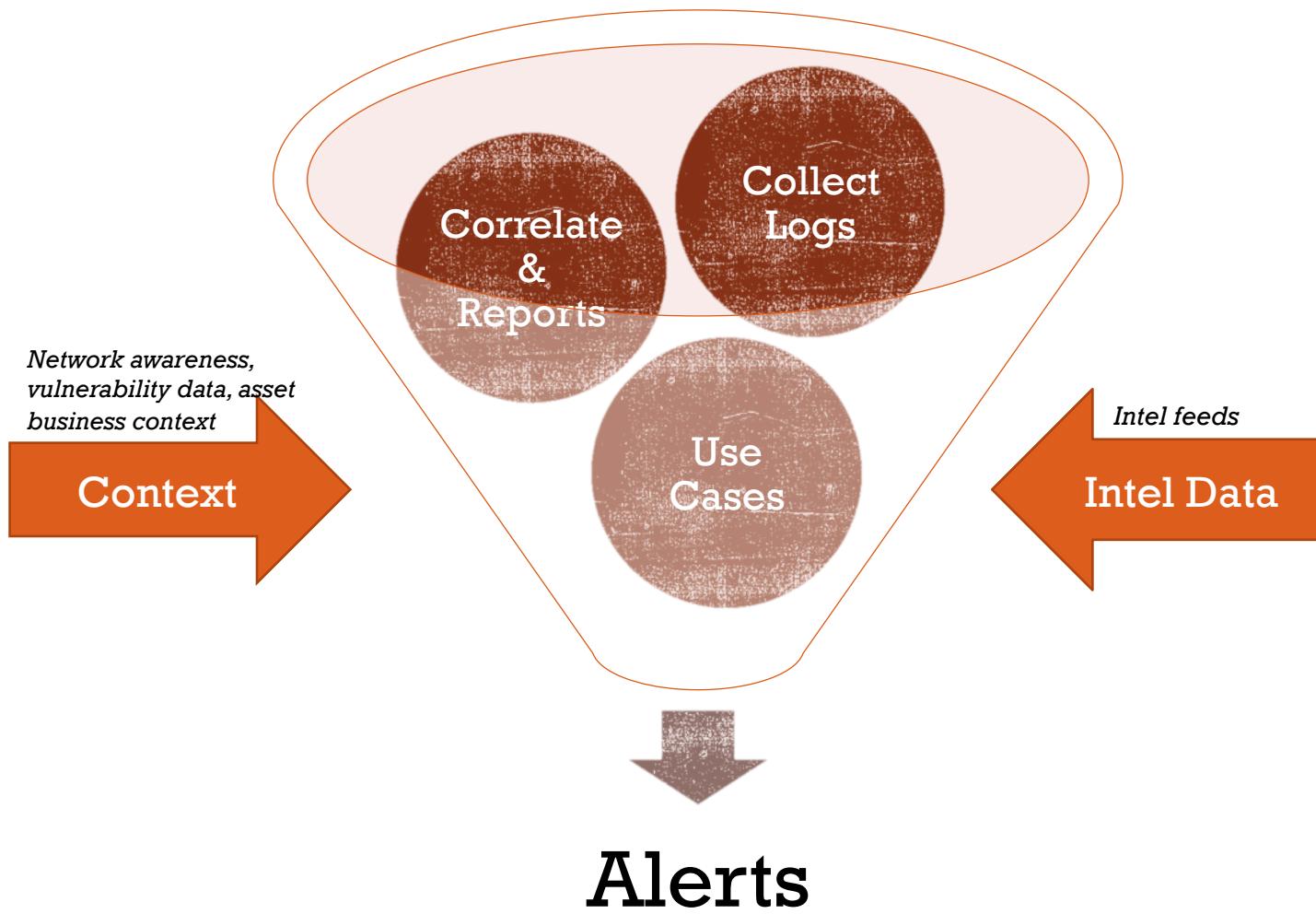
You Just Don't Get IT



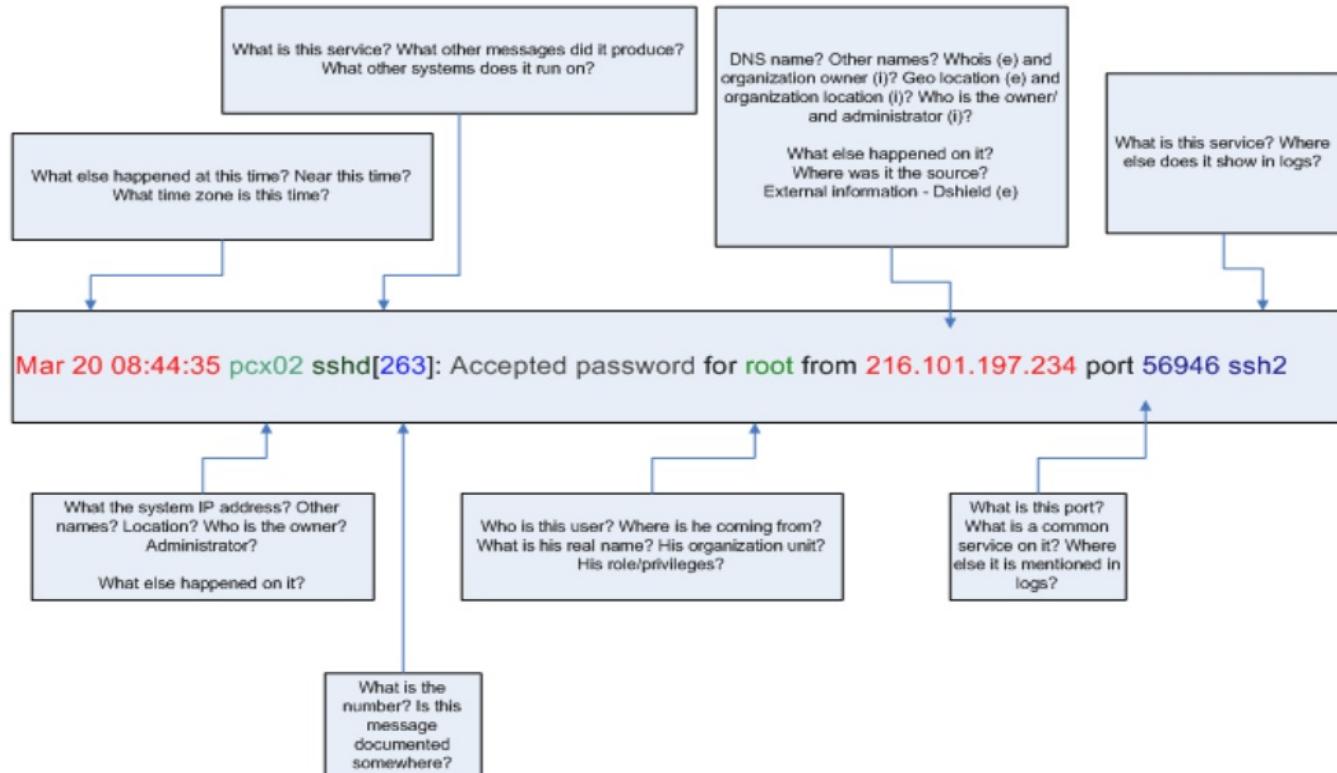
youjustdontget.it



WHAT DEFINES A SIEM?



What SIEM Eats: Context



<http://chuvakin.blogspot.com/2010/01/on-log-context.html>



Dr. Anton Chuvakin

CONTEXT MATTERS

WHAT'S A SIEM KPI?

SIEM KPI

- Minimum criteria for an effective SIEM operation

Objectives

- Attempt to display effectiveness of SIEM investment
- Allow for creation of high quality use cases and alerts
- Allow for quick triage by analysts



THE ULTIMATE GOAL - SITUATIONAL AWARENESS

Network Awareness	Threat Awareness	Mission Awareness
<ul style="list-style-type: none">• Disciplined asset and configuration management• Routine vulnerability auditing• Patch management & compliance reporting• Recognize and share incident awareness across the organization	<ul style="list-style-type: none">• Identify and track internal incidents and suspicious behavior• Incorporate knowledge of external threats• Participate in cross-industry or cross-government threat-sharing communities on possible indicators and warnings	<ul style="list-style-type: none">• Develop a comprehensive picture of the critical dependencies (and specific components) to operate in cyberspace• Understanding these critical dependencies to support mission-impact in forensic analysis (after a situation); triage and real-time crisis-action response (during a situation); risk/readiness assessments prior to task execution (anticipating and avoiding situations); and informed defense planning (preparing to mitigate the impact of a future situation).
Today	Evolving	Needed

- **Authentic Single Real Time View of Network- What it should be, What it is – In business and physical context**
- **Past, Present and Possible Future States – Network, Business Risk, Threats**
- **React to events based on changeable business priorities, using captured knowledge gained from previous incidents**
- **Real time accreditation/audit dashboards and compliance**



Data Completeness

- Are all collectors sending events?
- Are all events processed by collectors?
- Are there any unprocessed logs?

Data Quality

- Are all events parsed properly?
- Any unparsed events?
- Parser errors ?

Error monitoring

- Collector errors
- Parser error
- Error monitoring dashboard

SIEM - KEY PERFORMANCE INDICATORS

Log Collection



Network awareness

- Your SIEM should be aware of your network zoning
- Dashboard to monitor “unzoned events”
- Use IP geolocation

Vulnerability Data

- Add scanning result to your SIEM

Business Context

- Asset Criticality
- Asset Location
- Asset Owner

SIEM - KEY PERFORMANCE INDICATORS

Correlation



SIEM - KEY PERFORMANCE INDICATORS

Use Cases

Compliance Status

- AV Compliance Status
- Configuration Compliance Status
- Patch Compliance Status

Watchlists

- Infected Assets
- Devices with Open Vulnerabilities

Activities

- High Privileged Users Activity
- Asset Location
- Asset Owner

Case Management

- Case / Analyst
- Average Case Duration
- General Case Statistics (Open, In Progress, Closed)

Event Statistics

- Average EPS, Per Collectors, Per Zone, etc
- Alerts / Analysts
- Raw , Correlated, Annotated Events
- Indicates SIEM efficiency

Operational Statistics

- SIEM component health
- Quiet Feeds
- Number of Assets tracked
- Number of Devices monitored

SIEM - KEY PERFORMANCE INDICATORS

SIEM Operations



Activity Monitoring

- Firewall Activities
- IPS / IDS Activities

Dashboards

- Top Ingress/Egress
- Top Events
- Top Foreign Countries
- Top Malware

Situational Awareness

- High Critical Zones activities
- Zones with highest critical events

SIEM - KEY PERFORMANCE INDICATORS

Base Statistics

DISCUSSIONS

