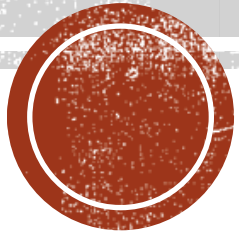
SIEM – KEY PERFORMANCE INDICATOR

Paulus Tamba



ABOUT ME

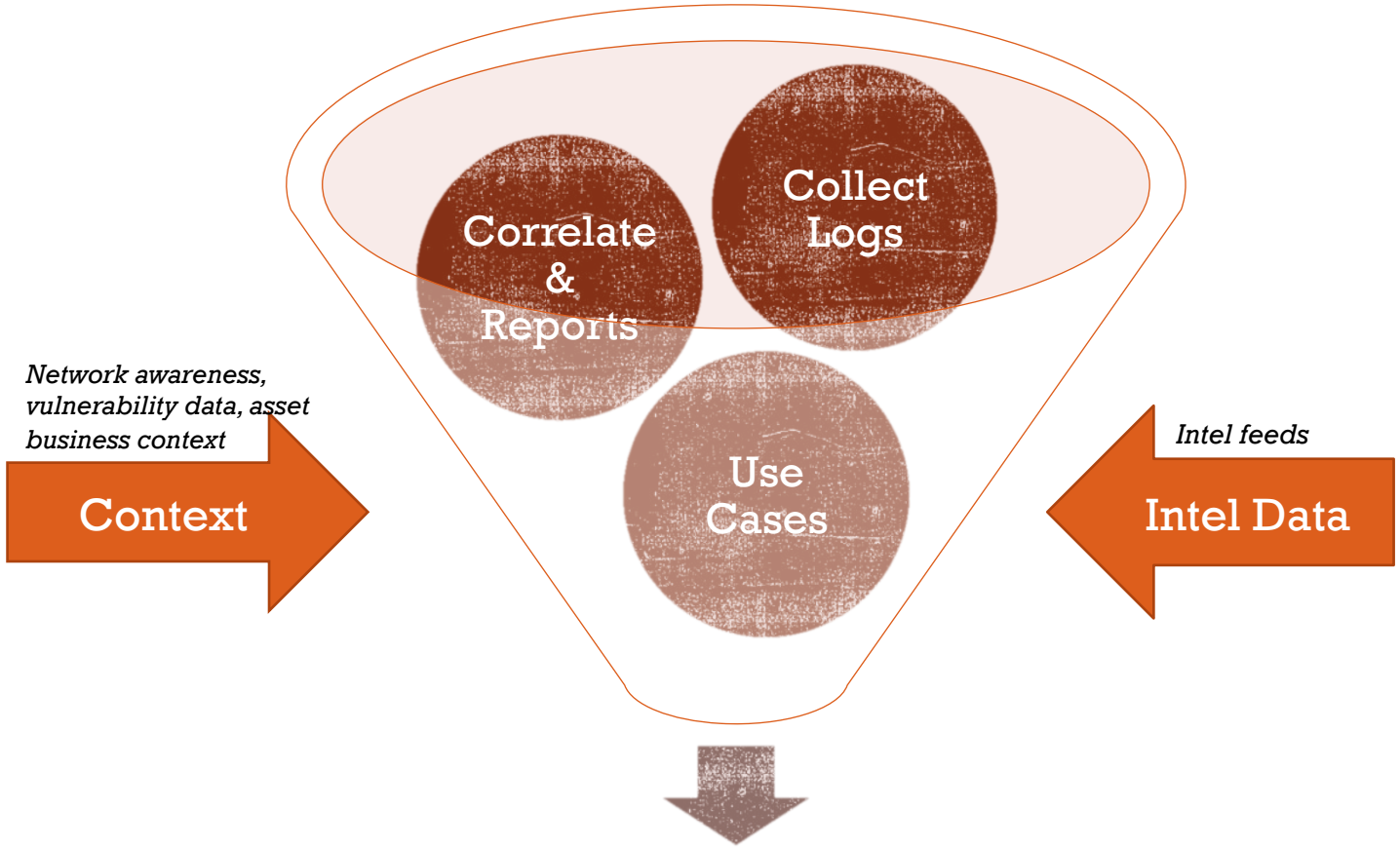
- Analyst in training
- 12 years in infosec and counting
- Interested in T&VM, Security Operations, Risk and Compliance
- Was with Verizon-Cybertrust, BT, & FireEye
- Founded KPI on 2014
- https://www.linkedin.com/in/paulustamba/

CREDITS

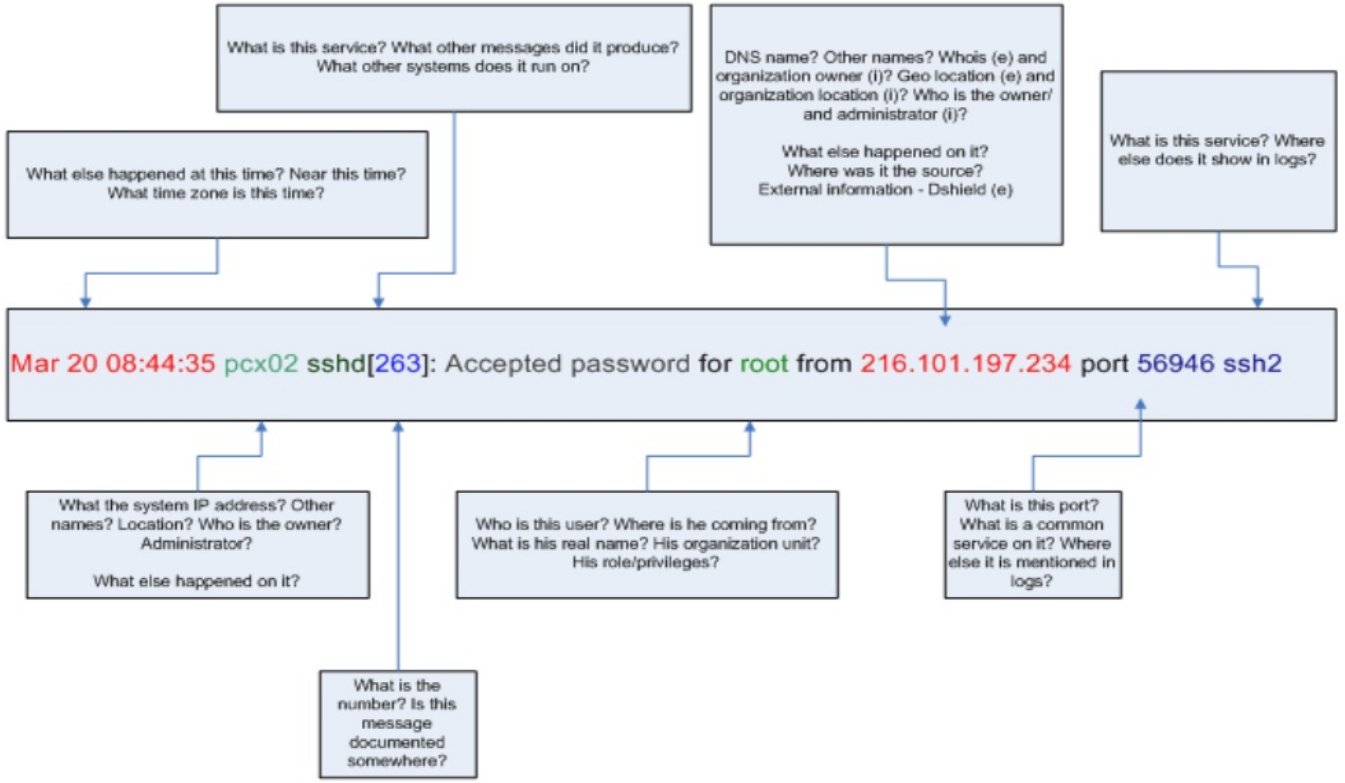
- Lots and lots of Anton Chuvakin thoughts on SIEM
  - https://blogs.gartner.com/anton-chuvakin/
  - http://www.securitywarrior.org/
- Arcsight Whitepaper
  - Security Operations Metrics Definitions and Operations Team
- Various publications on the internet

LETS TALK SIEM

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?

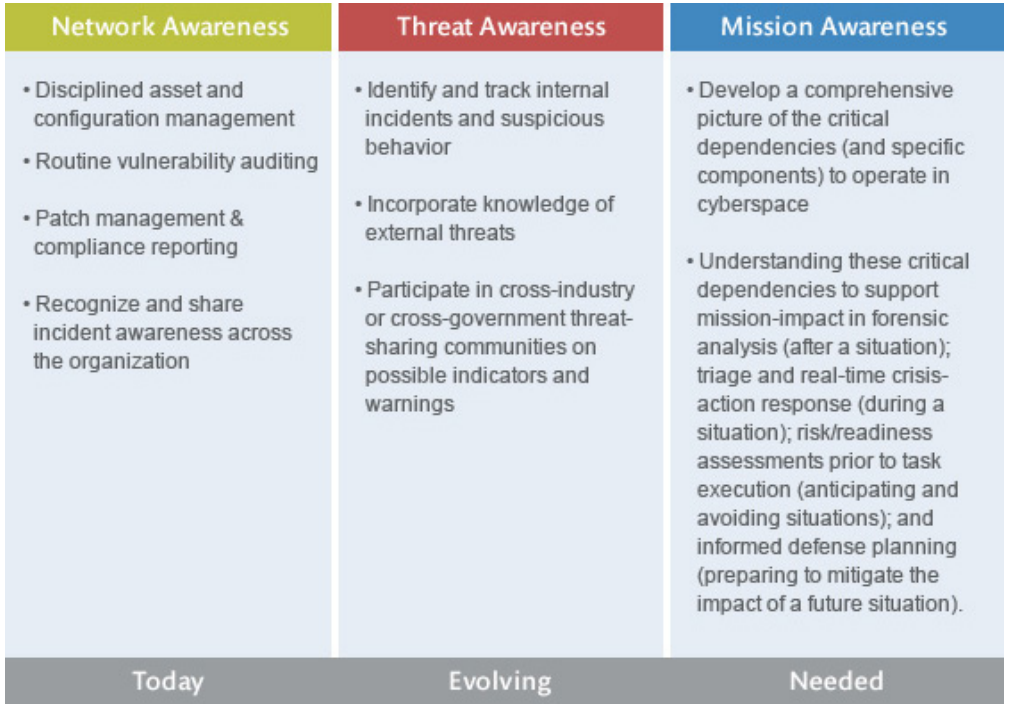
SIEM KPI

- 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



- 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

SIEM – KEY PERFORMANCE INDICATORS

Log Collection

Data Completeness	Data Quality	Error monitoring
• Are all collectors sending events? • Are all events processed by collectors? • Are there any unprocessed logs?	• Are all events parsed properly? • Any unparsed events? • Parser errors ?	• Collector errors • Parser error • Error monitoring dashboard

SIEM – KEY PERFORMANCE INDICATORS

Correlation

Network awareness	Vulnerability Data	Business Context
• Your SIEM should be aware of your network zoning • Dashboard to monitor "unzoned events" • Use IP geolocation	• Add scanning result to your SIEM	• Asset Criticality • Asset Location • Asset Owner

SIEM – KEY PERFORMANCE INDICATORS

Use Cases

Compliance Status	Watchlists	Activities
• AV Compliance Status • Configuration Compliance Status • Patch Compliance Status	• Infected Assets • Devices with Open Vulnerabilities	• High Privileged Users Activity • Asset Location • Asset Owner

SIEM – KEY PERFORMANCE INDICATORS

SIEM Operations

Case Management	Event Statistics	Operational Statistics
• Case / Analyst • Average Case Duration • General Case Statistics (Open, In Progress, Closed)	• Average EPS, Per Collectors, Per Zone, etc • Alerts / Analysts • Raw , Correlated, Annotated Events • Indicates SIEM efficiency	• SIEM component health • Quiet Feeds • Number of Assets tracked • Number of Devices monitored

SIEM – KEY PERFORMANCE INDICATORS

Base Statistics

Activity Monitoring	Dashboards	Situational Awareness
• Firewall Activities • IPS / IDS Activities	• Top Ingress/ Egress • Top Events • Top Foreign Countries • Top Malware	• High Critical Zones activities • Zones with highest critical events

DISCUSSIONS