PROTECT 2011

POWERED BY HP ENTERPRISE SECURITY

CSN33: ArcSight ESM Reports: It Pays to Know Your Audience

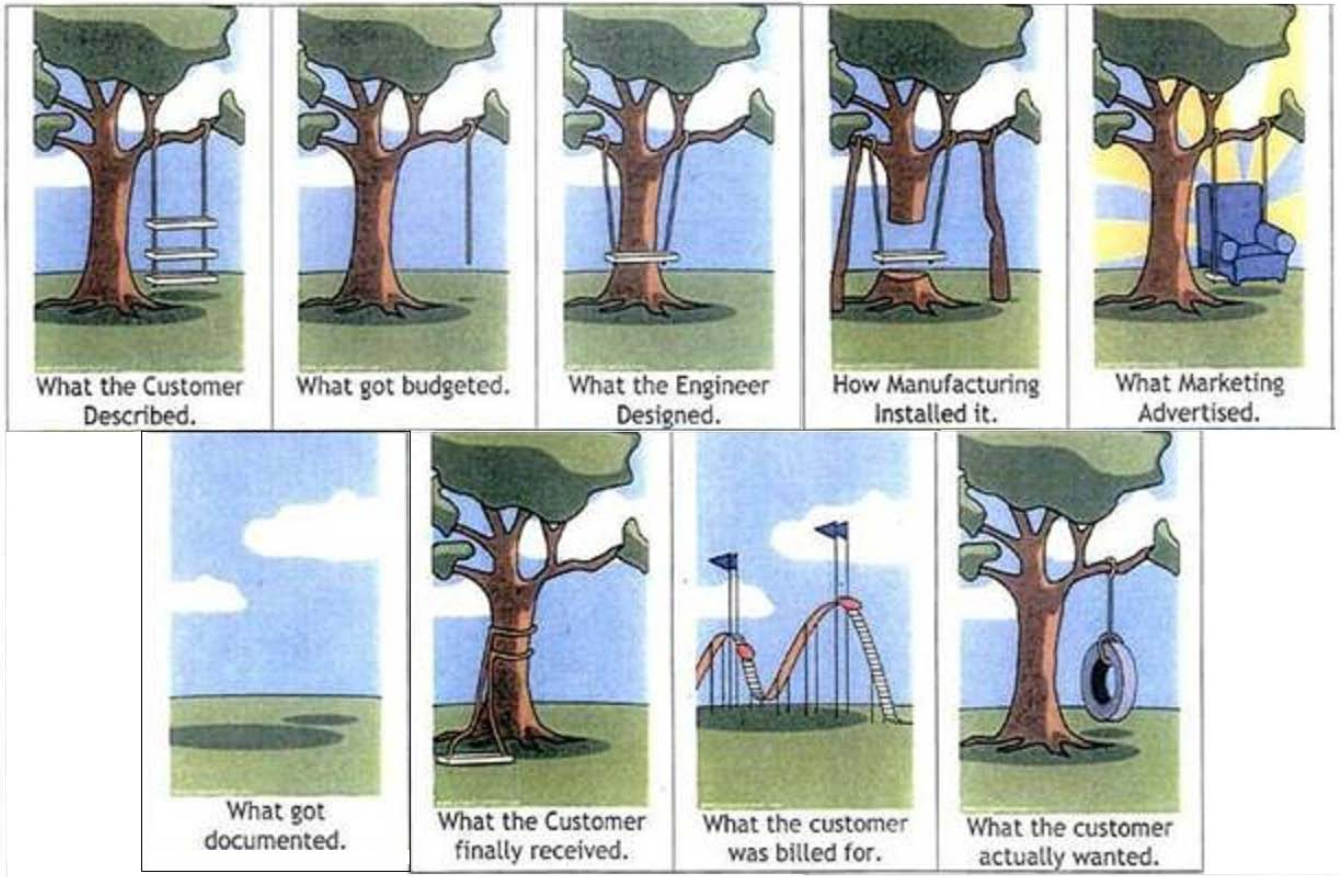
Heike Herpich
VP of Information Security, Forbes Top 5 Financial Organization
Scott Parkinson
Principal Consultant, HP ArcSight

With increasing cyberthreats, compliance regulations and management oversight, the demand for security event reporting has grown.

What is Reporting?

I define reporting as the regular provision of information and data to a selected audience within an organization to support them in their work. These reports can take the form of graphs, text and tables and, typically, are disseminated through e-mail.

Your standard reporting request…



“If you want a wise answer, ask a reasonable question.”

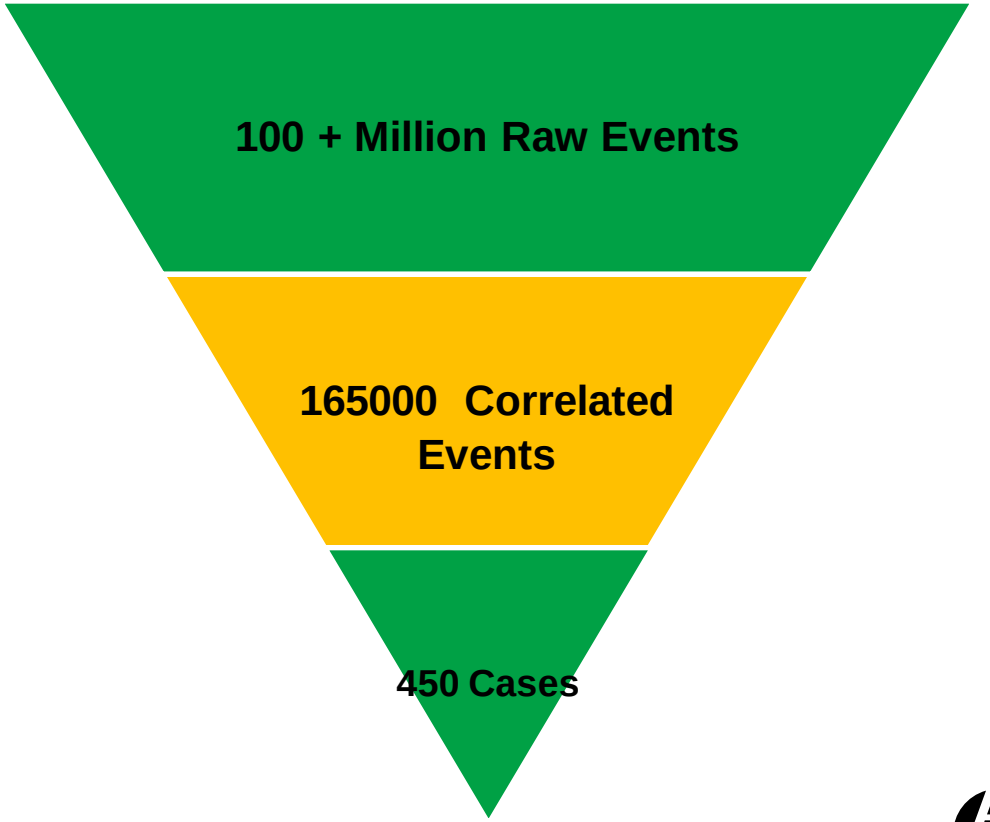
-Johann Wolfgang Von Goethe

Your Audience

- Who are they?
  - Your direct management
  - Your executive management – including the CTO
  - Your peers
  - Information Security teams outside your immediate organization
  - Audit
  - Compliance
  - Different LOBs within your organization

Data Sources

- 100+ million events a day, where do I start?
- Events ?
  - Base events
  - Correlated events
- Active Lists ?
- Cases ?
- Assets ?



What “Flavor”….?

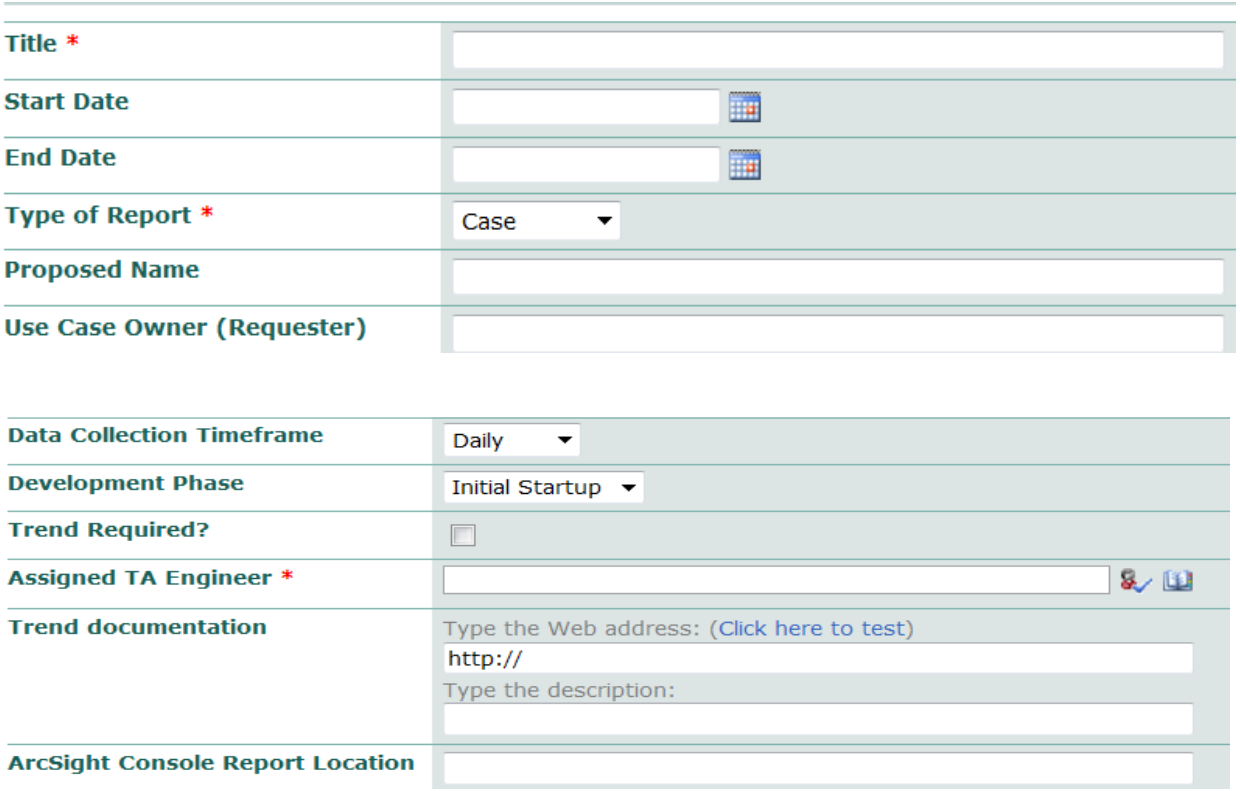
- Format - .pdf, .csv, xls ?
- Summary or detailed reports?
- Monthly trend on Arcsight cases to establish a workload baseline?
- Custom icons and templates required?
- Ad Hoc, Daily, Monthly, Yearly reports?

Business Requirement Document

Because you just cannot remember all the details

- Make it a template!
  - The file extension is up to you
  - Create a standard about the template, post it, communicate it – Make it a repeatable process
- Define the required, critical fields that cannot be blank
  - Data Source
  - File format
  - Report delivery
  - Requester information
  - Sign off

Business Requirement Document



Breaking Down the Requests

Executive Management

- State of the Security
- Complete Summarized Report request
- Various charts
- Customized templates
- Multiple pages

Third Party Reporting Tools

- Specific data
- Simple data format for import into third party Enterprise level reporting tool

Event Analysis

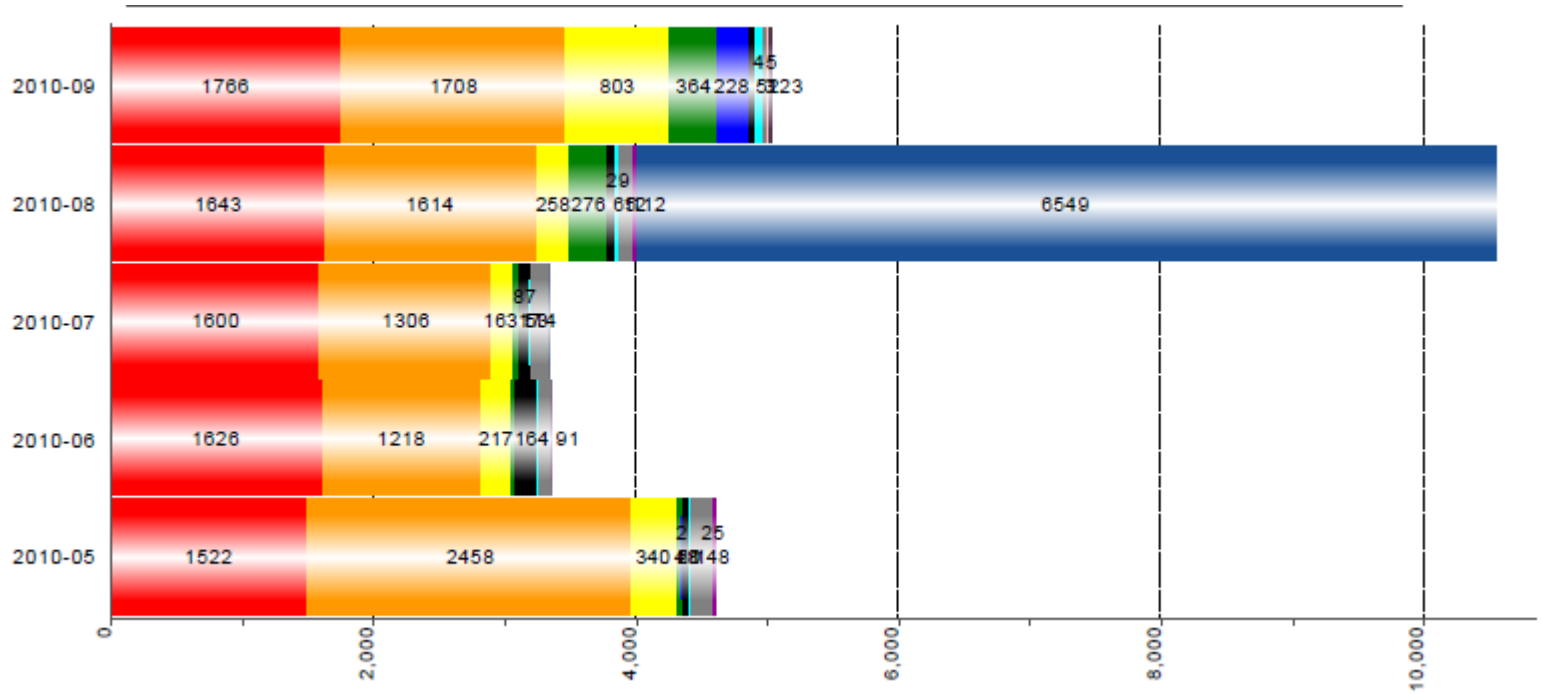
- Total count of cases created by month
- Trending of total count for workflow over 12 months

Use Case Administrators

- Case reports specific to Stage disposition
- Summarized Daily Event flow data by Connector

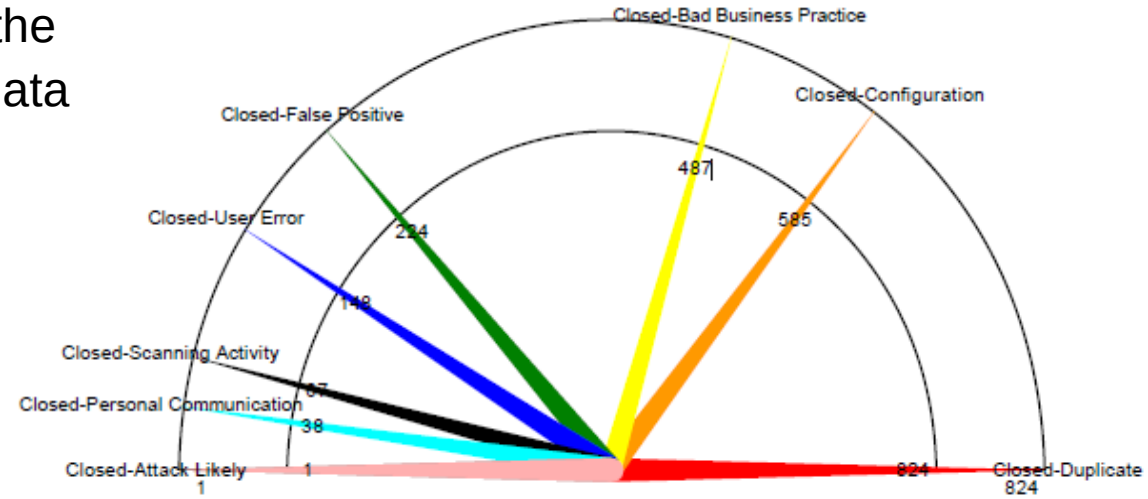
Event Analysis Trend Report

Trending ArcSight Cases can aid defining workload baseline



Cases Processed by Stage

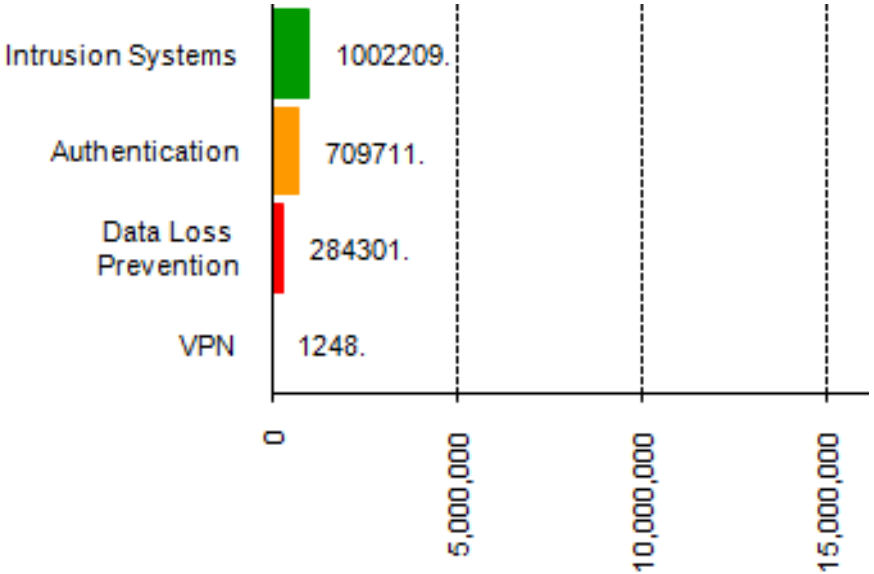
- Reports summarizing case dispositions can provide the ArcSight Administrators data to fine tune rules



Daily Intelligence Briefing

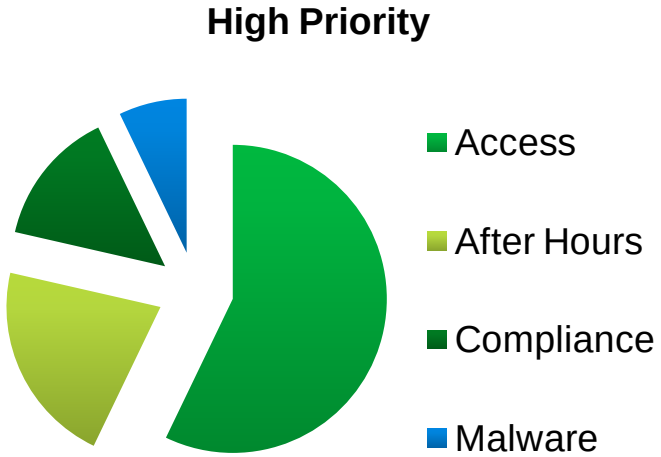
Event Count

- Summarized by Type



Cases

- Queued Status



Thank you

PROTECT 2011

POWERED BY HP ENTERPRISE SECURITY