Simplified SIEM Use Case Management

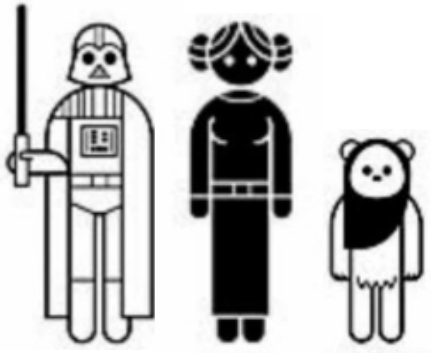
Ryan Voloch
9/25/2015

Outline

- About Ryan Voloch
- SIEM (Security Incident/Event Management) Use Case Database (UCDB) Basics
- Quick Start Steps
- Review Schema
- Sample Reports

Download http://voloch.com/siemucdb.zip

Ryan Voloch



- Christian
- Husband
- Father
- Information Security Engineer
  - Graduate of Rochester Institute of Technology
  - 12 years InfoSec experience, 8 years with SIEM
  - Implemented over 10 different enterprise security systems from the ground up
  - Experience with multiple SIEM products
  - Developed two security operations programs
  - Currently employed with a for profit education system

ROCHESTER INSTITUTE OF TECHNOLOGY
R·I·T
1829

CISSP
GCIH

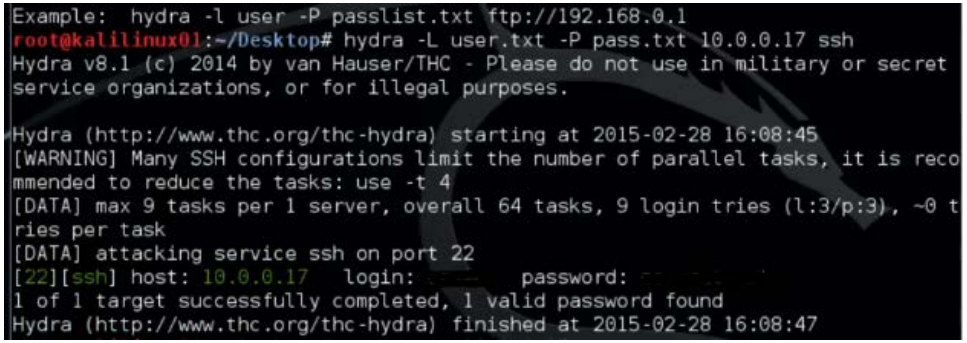
Download http://voloch.com/siemucdb.zip

The Basics

- What is a SIEM use case?
  - Documented actionable output for your SIEM.
  - In simplistic terms…it's what you want your SIEM to do.
  - Defines who, what, where, when & why.
  - An alert, report, or dashboard.
  - Could be as simple as an idea with little definition or theory to being very well defined.

Example Use Case:

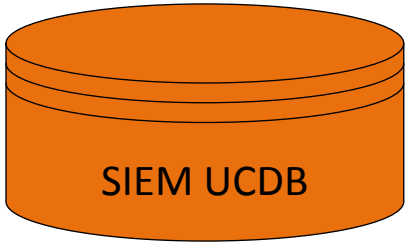
"Alert when there are 10 failed login attempts to a critical UNIX server within one hour. Inform the Security Operations team who will then investigate."



Download http://voloch.com/siemucdb.zip

Why maintain a SIEM Use Case Database (UCDB)?

- Allows you to define the ocean you want to boil.
  - SIEM systems *SHOULD* do anything you can dream of if provided the data. SIEM is just a data framework.
- Your environment is unique
- A place to document and organize:
  - Ideas….When you get one, then document it so you don't forget it!
  - Incident lessoned learned findings.
  - Requests from other non-Security teams.



Download http://voloch.com/siemucdb.zip

Why develop and maintain a UCDB?

- If you are the SIEM developer, a UCDB allows you to:
  - Prioritize your time and effort
  - Determine what data to collect
  - Develop a work queue
  - Keep up with the ever-changing threat landscape
  - Manage a lifecycle
    - Concept → Development → Production → Disabled/Defunct

Why develop and maintain a UCDB?

- Keep SIEM developers/consultants accountable
  - Include use cases from your UCDB in your statement of work
- Show value to management
  - Metrics
  - Statuses
  - Work to-do versus accomplished
  - Show SIEM or Security Operations Program Usefulness
- Status reports can be provided to others such as internal or external auditors.

But what if I don't have a SIEM?

- Use a UCDB to define your needs:
  - Replace manual reviews of individual log systems, start documenting a UCDB.
  - Document your process gaps.
  - Develop TCO.

- Use UCDB as a tool to identify which SIEM to purchase or replace
  - Include your UCDB in your RFP

Sample UCDB Quickstart Steps

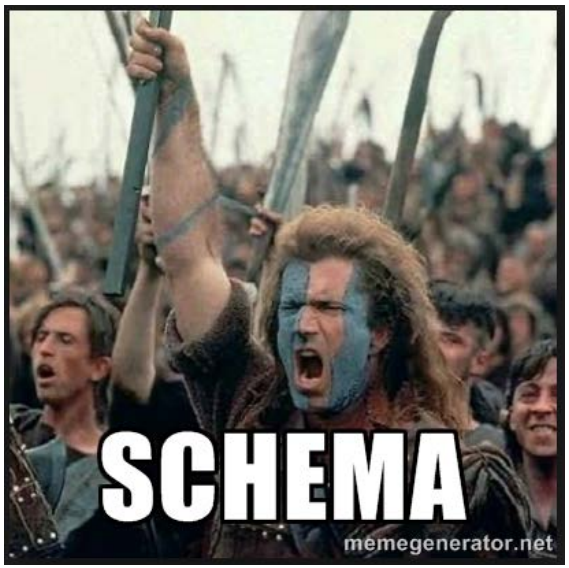
- Sample SIEM Use Case Database. What is it?
- The format is just an Excel spreadsheet…nothing fancy.
  1. Delete all sample data except for the ID field.
  2. Edit values on 'Data Validation' worksheet to your environment.
  3. Modify schema as necessary.
  4. Data entry.

You may download the sample spreadsheet, URL is below.

Download http://voloch.com/siemucdb.zip

Schema

- ID#
  - Just a key and a reference number



- Status

Concept	In consideration for development; an idea.
Development	Developed and being tested.
Production	Use case is being used in a production operational process.
Disabled	Disabled due to a problem such as data feed issue or high false positive rate.
Defunct	Technology changed, data feed lost.

Download http://voloch.com/siemucdb.zip

Schema

- Title
  - Name of alert, report or dashboard.
  - Should be intuitive and make sense to recipients
  - Keep the same title in SIEM
  - Example naming scheme:

```
(<Vendor|system name|Correlated>) (<Excessive|Baseline|Threshold>)
<Failed|Successful|Exceeded> <Login|Attack|File|Scan|Traffic>
<to|from|against|for|on> <system|network|user|application>
<Detected|Accessed|Deleted|Added|Changed|Blocked> <Type>
```

  - **"Unix Excessive Failed Login to Critical Server Alert"**
  - More example titles:
    - Correlated IPS Signature against DMZ Server Vulnerability Alert
    - Windows Excessive Failed Logins against Multiple Users Alert
    - Netflow Threshold Exceeded Traffic from Database to Internet Report
    - Top Alerts by Score Dashboard

Schema

- Type
  - What kind of output is it?

Alert	Actionable alert based on binary logic. Must have a documented procedure, defined responsible owner to perform, and a defined response timeframe.
Report (Ad-hoc)	Report only ran when requested by user.
Report (Scheduled)	Regularly scheduled report with defined recipients, purpose and procedure.
Dashboard	Real time view for eyes on glass.
Execution Command	Execute a command based on value selected in SIEM GUI.
Table/List	Temporary or permanent table within SIEM.

- Example
  - "Alert"

Schema

- Importance
  - How important it is to the business to develop this use case?

4-CRITICAL	Business critical
3-HIGH	High priority
2-MEDIUM	Medium Priority
1-LOW	Get to it someday

- Development Effort
  - The amount of effort required to develop the use case. Assumes the data feed is in place.

X

4-LOW	Less than 5 hours of development time
3-MEDIUM	Between 6-10 hours of development time
2-HIGH	Between 11-39 hours of development time
1-VERY HIGH	Over 40 hours of development time

- Current Data Collection
  - Is the data currently in your SIEM?
  - 2x multiplier if yes
- Priority Score
  - Calculated to identify quick wins.
  - (I + DE) x 2 if data collection = Priority Score

Importance	Development	Current Data Collection (y/n)	Priority Score
4-CRITICAL	4-LOW	Yes	32
3-HIGH	2-HIGH	Yes	12
1-LOW	2-HIGH	No	2

Download http://voloch.com/siemucdb.zip

Schema

- Primary & Correlated Data Source (50 generic samples included) Example: *"Syslog (Unix)"*
- Primary Security Detection Classification

Primary Detection Security Classification	Primary method of detection for:
Application Problem	A problem with an application.
Compliance	Compliance issue only and not any Security Classification listed here.
Data Loss	Methods of unauthorized data extraction or leakage.
Efficiency	Provide efficiency or benefit within operations program.
Insider Threat	Insider threats.
Malfunctioning Control	Security controls not functioning but should be.
Malware	Malware, virus, C&C or APT related activity.
Other	Non-security based events.
Policy Violation	Violations of security policy.
Security Recommendation	Events that proves a need for a security control.
SIEM Health	Problems within the SIEM such as data collection issues, hardware/software alarms, etc…
Standard Violation	A standard is not implemented as defined or a control is not working.
Unauthorized Account Usage	When an account/identity/credential is used not for its intended purpose. Ex/ Unauthorized access and failed logins.
Unauthorized Change	Potential unauthorized changes.
Unknown Activity	Problems beyond knowledge of security, applications or system administrators.

- Example: *"Unauthorized Account Usage"*

Consider: VERIS veriscommunity.net & WASC webappsec.org

Download http://voloch.com/siemucdb.zip

Schema

- Some open text fields:
  - Benefit/ROI
    - *"Rather than manually reviewing every messages file on every UNIX host, this alert will reduce resources that currently take 10 minutes per host. Additionally, the accuracy of detection should surpass human review."*
  - Description & Goal
    - *"Alerts if 10 failed logins occur on a critical UNIX server. It's primary goal is to detect password cracking attacks."*
  - Pseduo Code/Logic/Sample Query
    - *"device=Unix source=syslog outcome=failure hostsubnet=critical, 10 in 1 hour."*
  - Next Step Notes
    - *"Make sure all UNIX servers are sending syslogs to SIEM."*

Schema

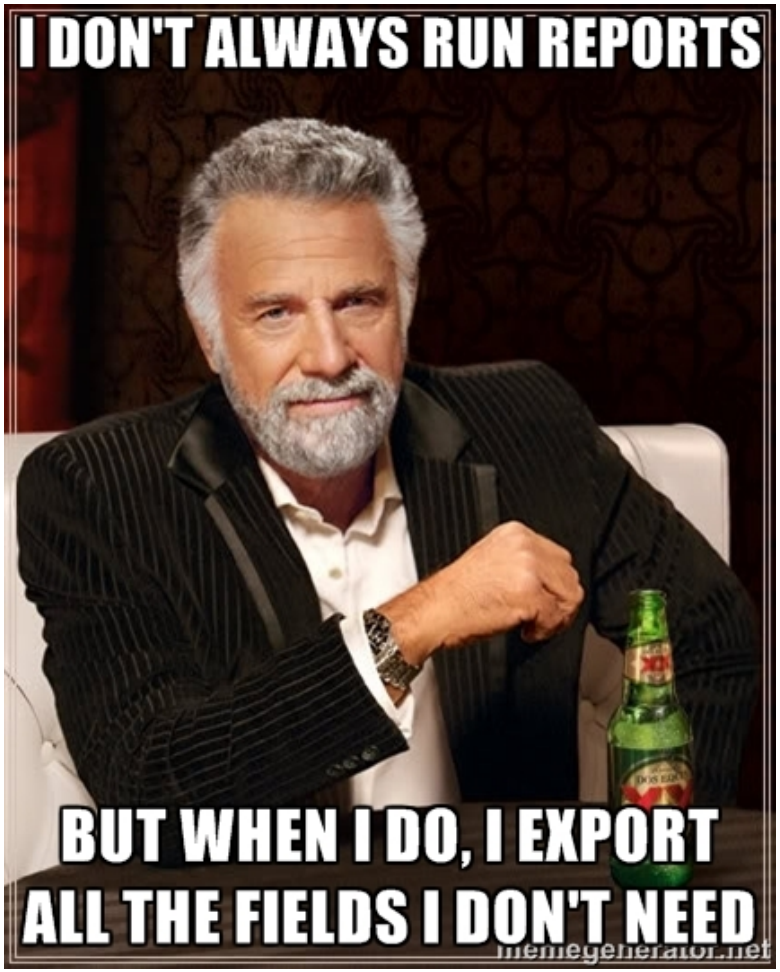
- Author
  - Who wrote the use case
- Developer
  - Who made it happen
- Go Live Date
  - When did it to go production
- Alert Priority
  - You define response times
- Report Frequency
  - How often report is ran and sent.
- Responsible Group
  - The recipient
  - Each can map to an email address
- Responsible Group Procedure
  - Documented actions to be taken.
  - "Contact the user to verify authorized use. If not, open a security incident ticket."

Alert Priority	
Priority A	Response required within 30 minutes
Priority B	Response required within 1 business day
Priority C	Response required within 3 business days
NA	Not Applicable

Report Frequency
Daily
Weekly
Monthly
Quarterly
Annually
Ad-Hoc

Download http://voloch.com/siemucdb.zip

Sample Reports



Download http://voloch.com/siemucdb.zip

Sample Report: Production Alerts by Responsible Group

- Good for internal marketing what your SIEM or Security Operations program does.

Responsible Group / Priority	Primary Security Classification	ID#	Title
HR Systems			
Priority C	Data Loss	291	CIO Uses the word "Cloud" Alert
	Policy Violation	292	Security Analyst Fell Asleep on Keyboard Alert
Security Operations Center			
Priority A	Compliance	52	Early Shift Security Analyst Leaves Early Alert
	Data Loss	182	Excessive Coffee Break Report
	Malware	78	Ice Cream Buffer Overflow Alert
		80	Excessive Failure to Invite Team Member to Lunch Alert
Priority B	Malware	57	Empty Gum Trash Can Alert
		186	Insignificant Call Received by Crisis Hotline Alert
		188	All Company Data Posted to Pastebin Alert
Priority C	Compliance	18	All of My Data Posted to Pastebin Alert
		106	CIO Uses the word "Cloud" Alert
		107	Security Analyst Fell Asleep on Keyboard Alert
		173	Early Shift Security Analyst Leaves Early Alert

Download http://voloch.com/siemucdb.zip

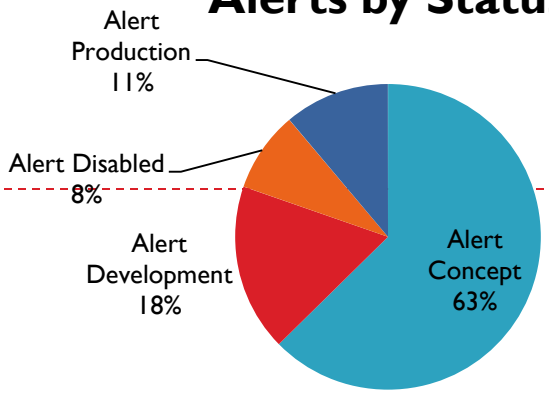
Sample Report: Concept Alerts by Category and Responsible Group

- A prioritized menu of use cases to help identify what to develop next.

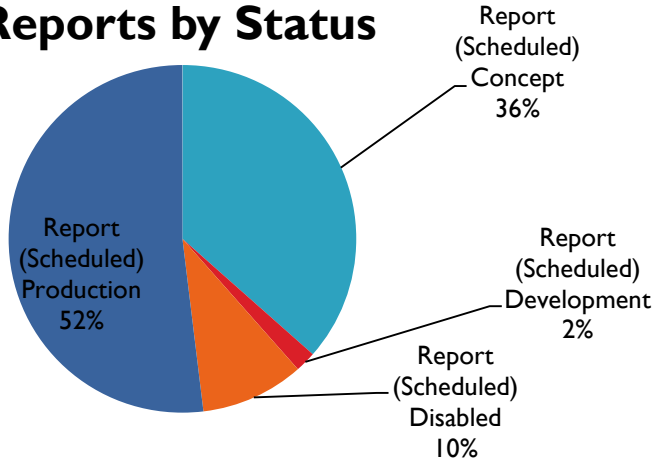
Category	Responsible Group	Priority Score	ID#	Title
Data Loss	HR	6	285	Early Shift Security Analyst Leaves Early Alert
		2	280	Excessive Coffee Break Report
	Security Operations Center	24	335	Ice Cream Buffer Overflow Alert
		18	59	Excessive Failure to Invite Team Member to Lunch Alert
		6	421	Empty Gum Trash Can Alert
	System Administration	24	37	Insignificant Call Received by Crisis Hotline Alert
Insider Threat	HR	12	2	All Company Data Posted to Pastebin Alert
		6	282	All of My Data Posted to Pastebin Alert
	IT Audit	3	210	CIO Uses the word "Cloud" Alert
	Security Operations Center	32	233	Security Analyst Fell Asleep on Keyboard Alert
		3	19	Early Shift Security Analyst Leaves Early Alert
	System Administration	12	62	CIO Uses the word "Cloud" Alert
Malware	Desktop	16	66	Security Analyst Fell Asleep on Keyboard Alert
	Email Administration	6	199	Early Shift Security Analyst Leaves Early Alert
		4	41	Excessive Coffee Break Report
		2	196	Ice Cream Buffer Overflow Alert
	Network Engineers	24	3	Excessive Failure to Invite Team Member to Lunch Alert
	Security Operations Center	32	191	Empty Gun Trash Can Alert
		16	317	Insignificant Call Received by Crisis Hotline Alert
		8	401	All Company Data Posted to Pastebin Alert

Download http://voloch.com/siemucdb.zip

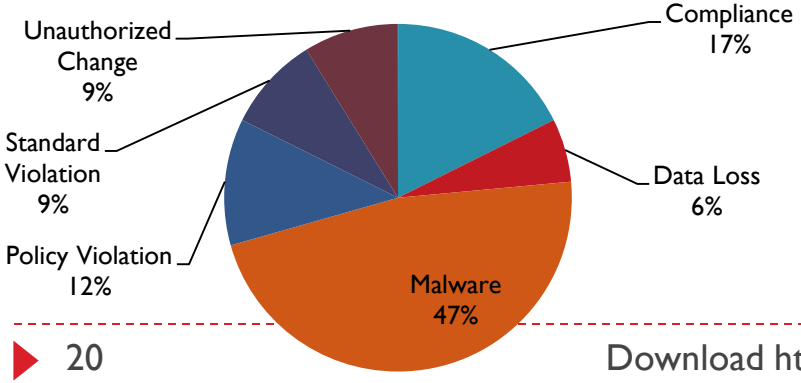
Alerts by Status



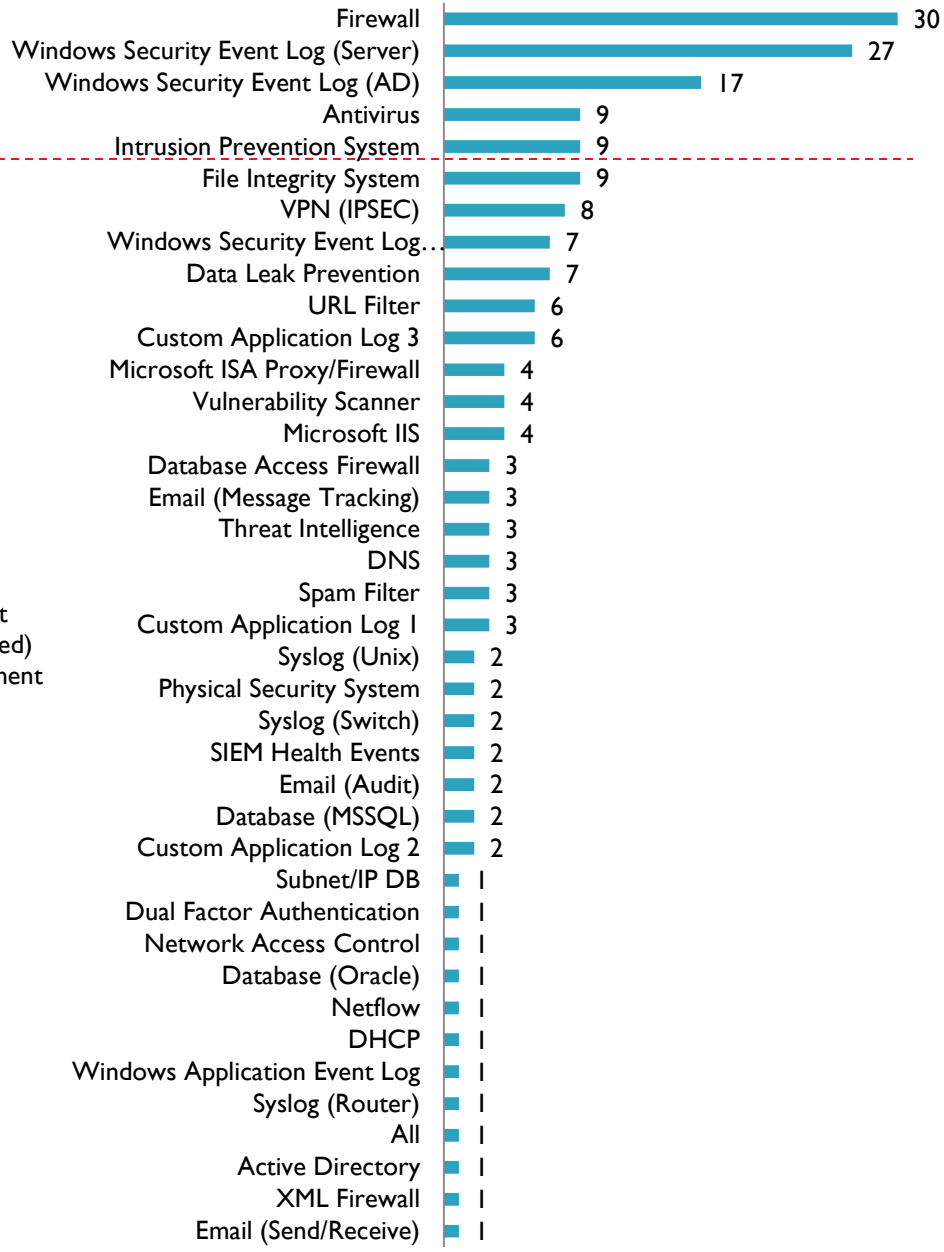
Reports by Status



Production Alerts by Classification

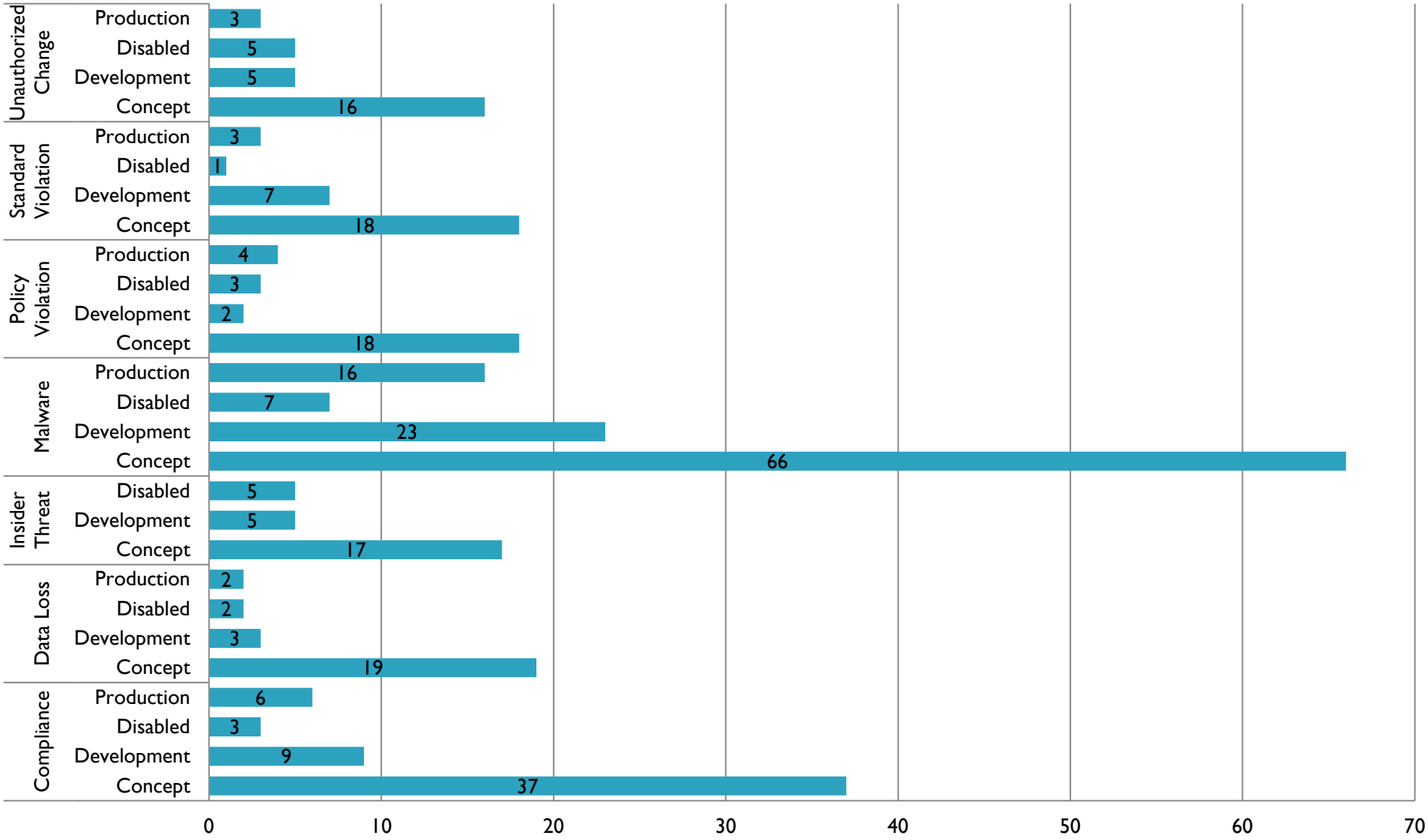


Concept Alerts by Primary Data Source



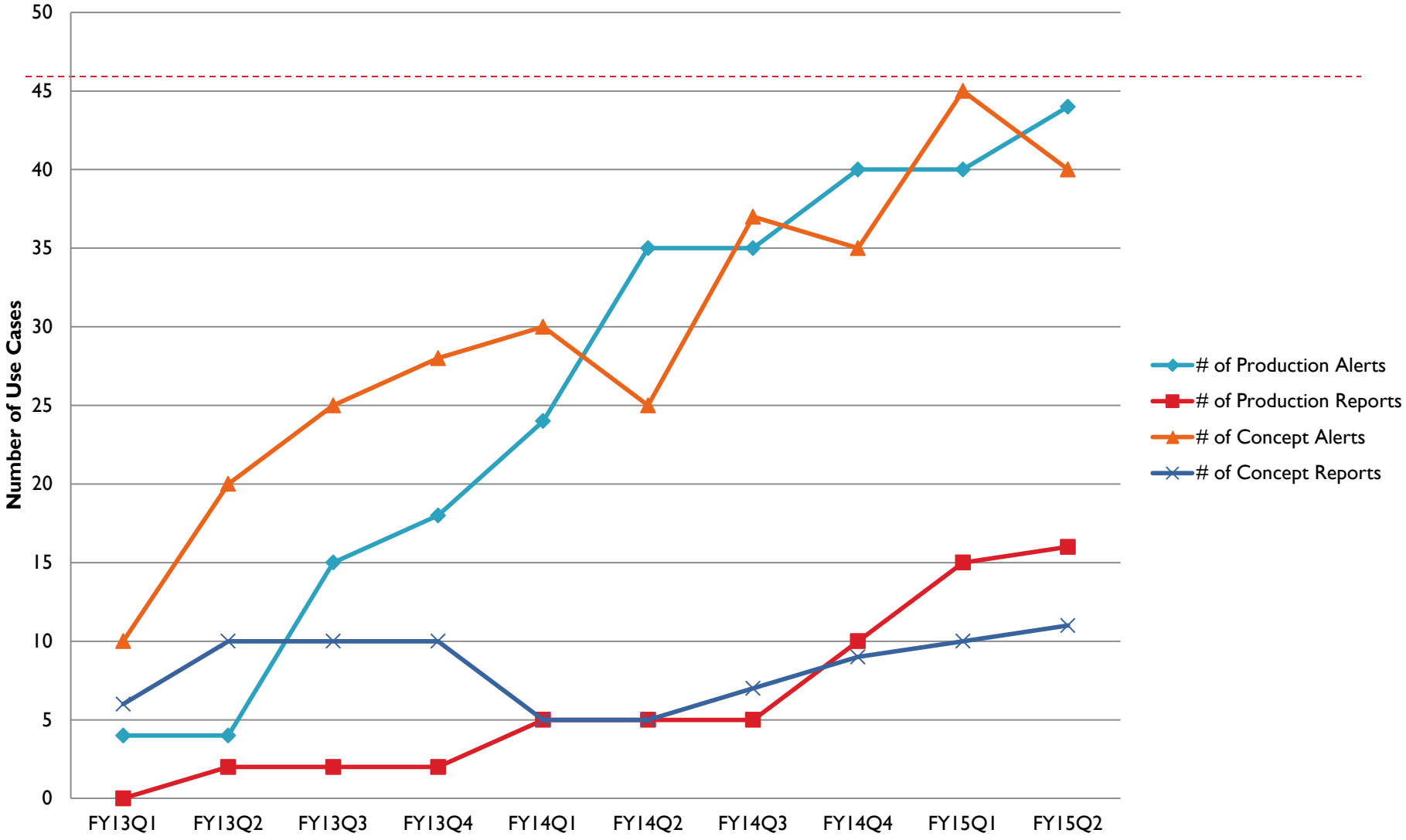
Download http://voloch.com/siemucdb.zip

Alerts by Primary Security Detection Category and Status



Download http://voloch.com/siemucdb.zip

SIEM Use Case Metrics Over Time



Download http://voloch.com/siemucdb.zip

How do I fill it up?

- Your brain + your log data
- Additional Technology: When you get a new data feed, host a brainstorm meeting. Ask "What could we do with this data?"
- Out-of-the-box SIEM vendor use cases
- Penetration Test Results – expect use cases
- Risk Assessment Results
- SIEM Vendor Customer Forums
- Ask con attendees: "What is your best use case?"
- Security incidents lessoned learned
- Ultimatewindowssecurity.com

Download http://voloch.com/siemucdb.zip

The goods!

- http://voloch.com/siemucdb.zip
  - Includes this presentation and spreadsheet of schema with sample reports.

Thank you!

Ryan Voloch

ryan@voloch.com

Special thanks to my friends in Pittsburgh who helped ☺