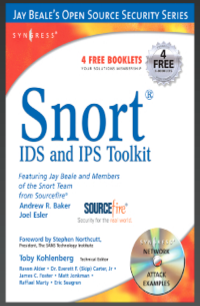
Insider Threat Visualizatio

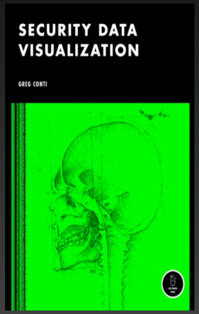
Raffael Marty, GCIA, CISSP
Chief Security Strategist @ Splunk>

Hack In The Box - September 07 - Malaysia

Who Am I?

- Chief Security Strategist and Product Manager @ Splunk>
- Manager Solutions @ ArcSight, Inc.
- Intrusion Detection Research @ IBM Research
  - http://thor.cryptojail.net
- IT Security Consultant @ PriceWaterhouse Coopers
- Open Vulnerability and Assessment Language (OVAL) board
- Common Event Enumeration (CEE) founding member
- Passion for Visualization





Agenda

- Convicted
- Visualization
- Log Data Processing
  - Data to Graph
  - AfterGlow and the Splunk Integration
- Insider Threat Visualization
- Insider Detection Process
  - Precursors
  - Scoring
  - Watch Lists
- Visual Conviction

Convicted

In February of 2007 a fairly large information leak case made the news. The scientist Gary Min faces up to 10 years in prison for stealing ***16,706*** documents and over ***22,000*** scientific abstracts from his employer DuPont. The intellectual property he was about to leak to a DuPont competitor, Victrex, was assessed to be worth $***400*** million. There is no evidence Gary actually turned the documents over to Victrex.

DuPont Case
How It Could Have Been Prevented

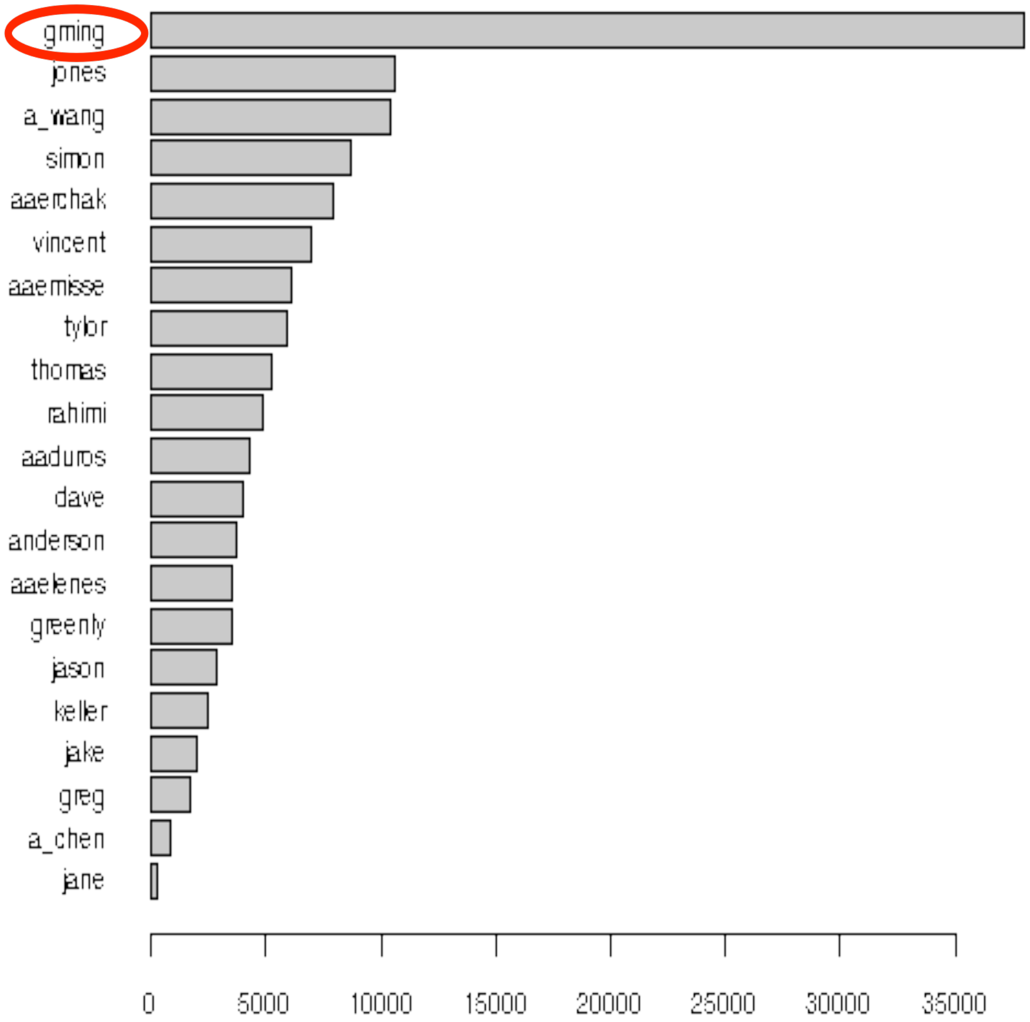
What's the answer?

DuPont Case

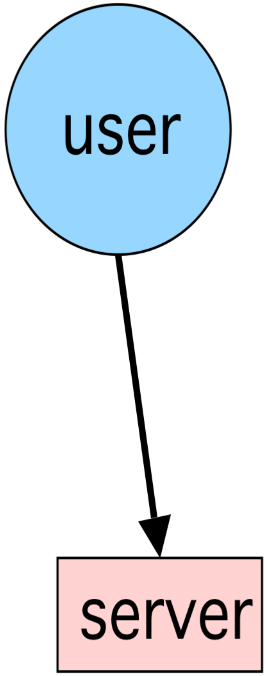
Log Collection!

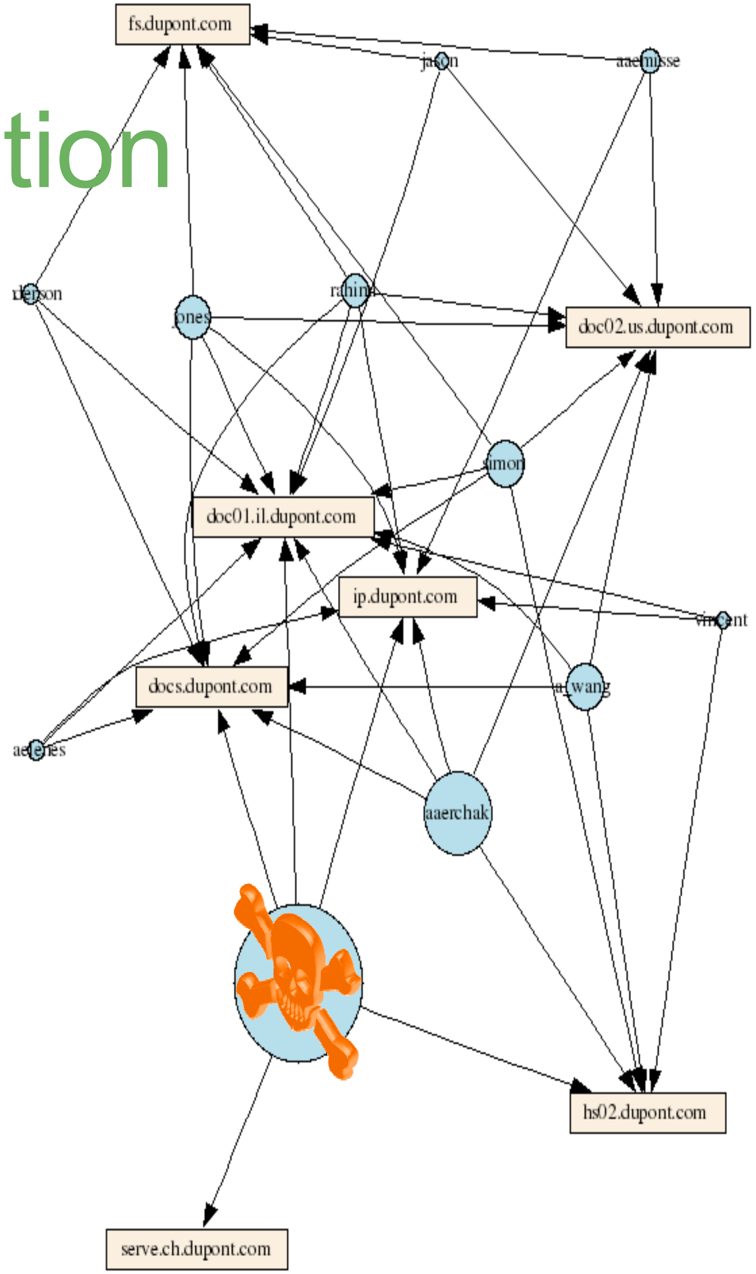
DuPont Case

Simple Solution



DuPont Case
More Generic Solution





Visualization - Questions

- Who uses visualization for log analysis?
- Who is using visualization?
- Who is using AfterGlow?
- Have you heard of SecViz.org?
- What tools are you using for log processing?

Visualization

Answer questions you didn't even know of

Increase Efficiency

- ✓ Quickly understand thousands of data entries
- ✓ Facilitate communication
- ✓ Increase response time through improved understanding

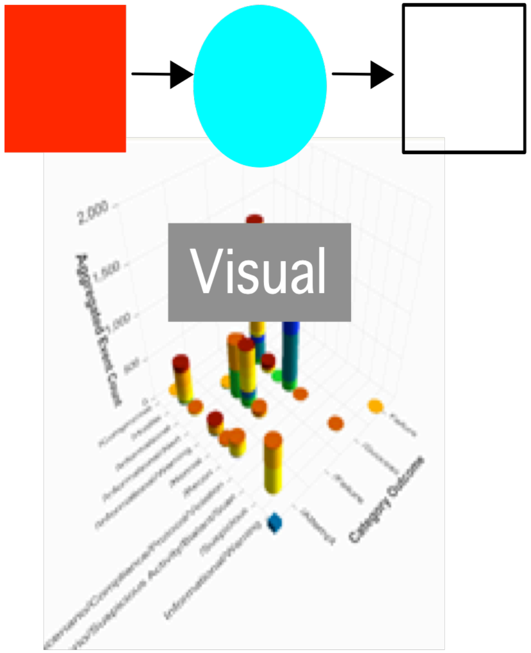
Make Informed Decisions

Insider Threat Visualization

- Huge amounts of data
- More and other data sources than for the traditional security use-cases
- Insiders often have legitimate access to machines and data. You need to log more than the exceptions.
- Insider crimes are often executed on the application layer. You need transaction data and chatty application logs.
- The questions are not known in advance!
- Visualization provokes questions and helps find answers.
- Dynamic nature of fraud
- Problem for static algorithms.
- Bandits quickly adapt to fixed threshold-based detection systems.
- Looking for any unusual patterns

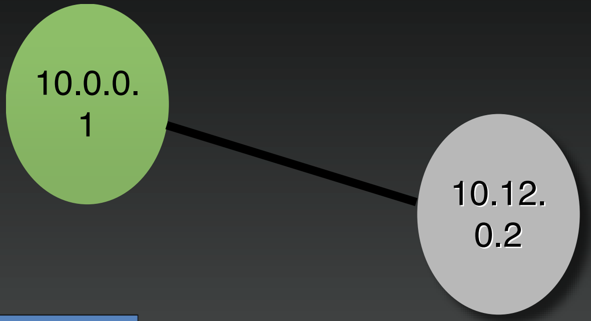
Visualizing Log Data

```
Jun 17 09:42:30   rmarty ifup   : Determining IP information for eth0...
Jun 17 09:42:35   rmarty ifup   :  failed; no link present.  Check cable?
Jun 17 09:42:35   rmarty   network: Bringing up interface eth0:  failed
Jun 17 09:42:38   rmarty sendmail   :  sendmail    shutdown succeeded
Jun 17 09:42:38   rmarty sendmail   :  sm-client    shutdown succeeded
Jun 17 09:42:39   rmarty sendmail   :  sendmail startup       succeeded
Jun 17 09:42:39   rmarty sendmail   :  sm-client startup       succeeded
Jun 17 09:43:39   rmarty vmnet-dhcpd   : DHCPINFORM from 172.16.48.128
Jun 17 09:45:42   rmarty   last message repeated 2 times
Jun 17 09:45:47   rmarty vmnet-dhcpd   : DHCPINFORM from 172.16.48.128
Jun 17 09:56:02   rmarty vmnet-dhcpd   : DHCPDISCOVER from 00:0c:29:b7:b2:47 via vmnet8
Jun 17 09:56:03   rmarty vmnet-dhcpd   : DHCPOFFER on 172.16.48.128 to 00:0c:29:b7:b2:47 via vmnet8
NH
```

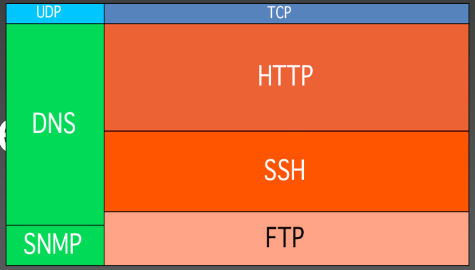


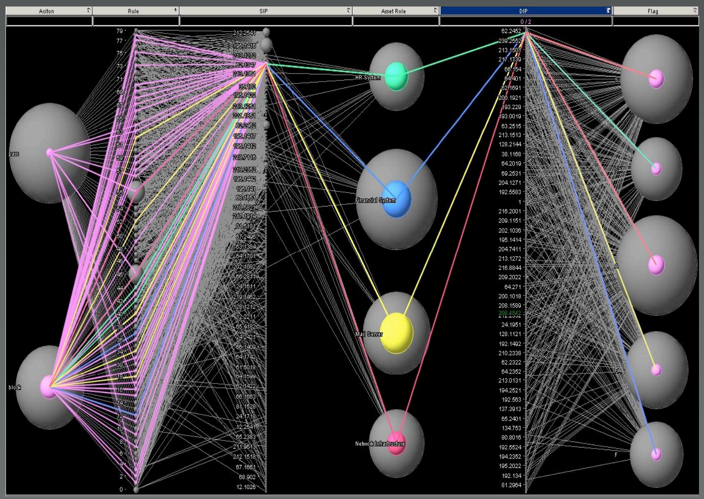
- ✓ Interpret Data
- ✓ Knows Data Formats
- ✓ Re-use don't re-invent
- ✓ Find some at: http://secviz.org/?q=node/8

Charts - Going Beyond Excel

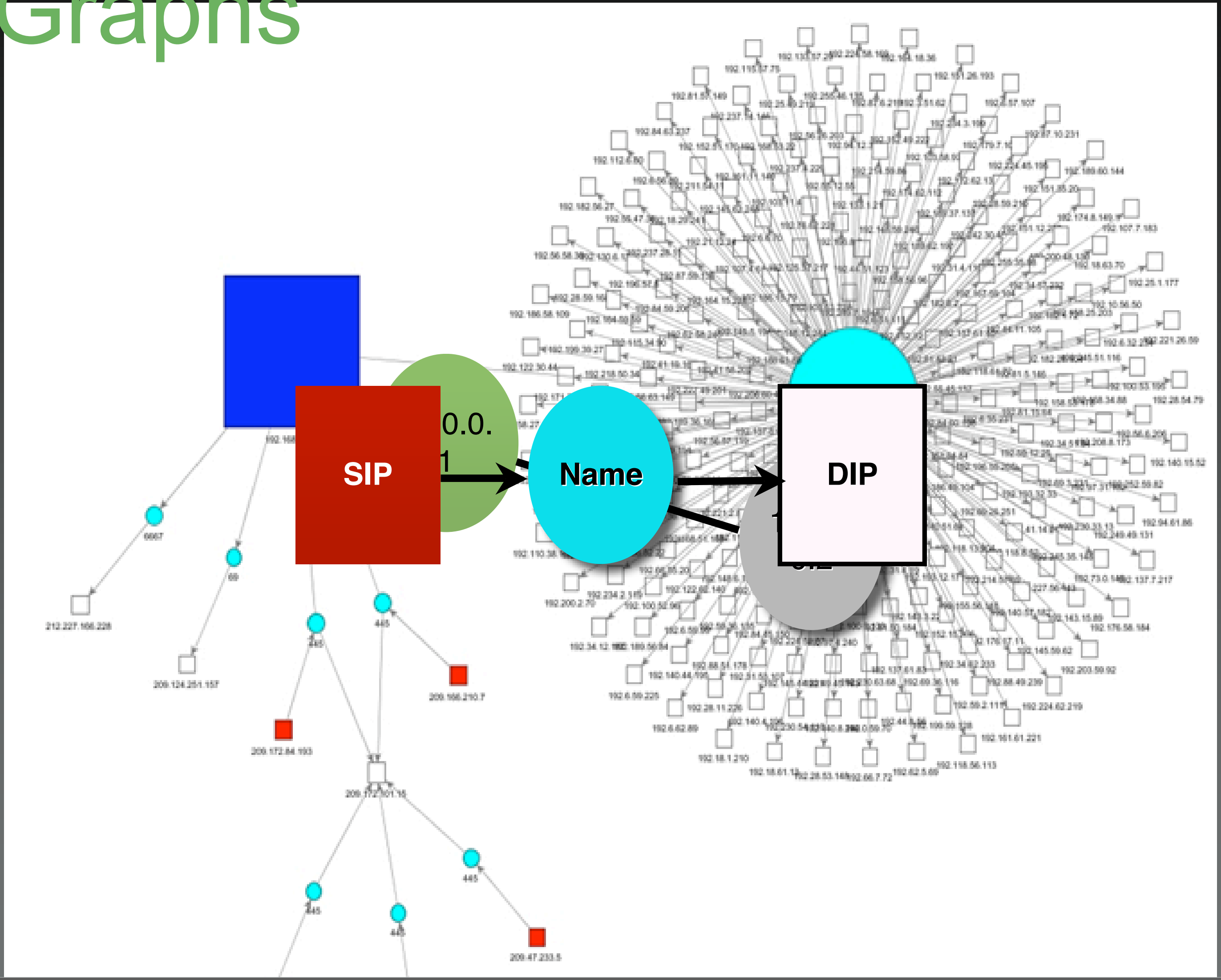


- Multi-variate graphs
  - Link Graphs
  - TreeMaps
  - Parallel Coordinat



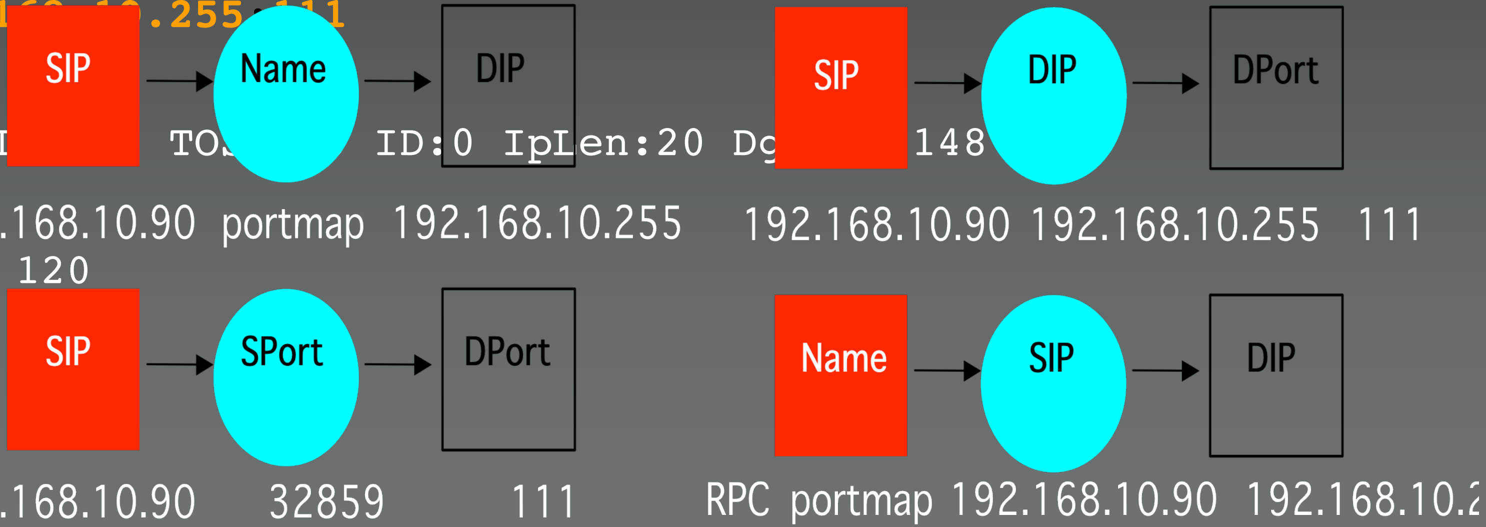


Beyond The Boring Defaults For Link Graphs



Link Graph Shake Up

```
[**] [1:1923:2] RPC portmap UDP proxy attempt [**]

[Classification: Decode of an RPC Query] [Priority: 2]

06/04-15:56:28.219753 192.168.10.90:32859 ->

192.1    .255:  1

UDP T      TO      ID:0 IpLen:20 Dg     148

Len: 120
```



192.168.10.90 portmap 192.168.10.255

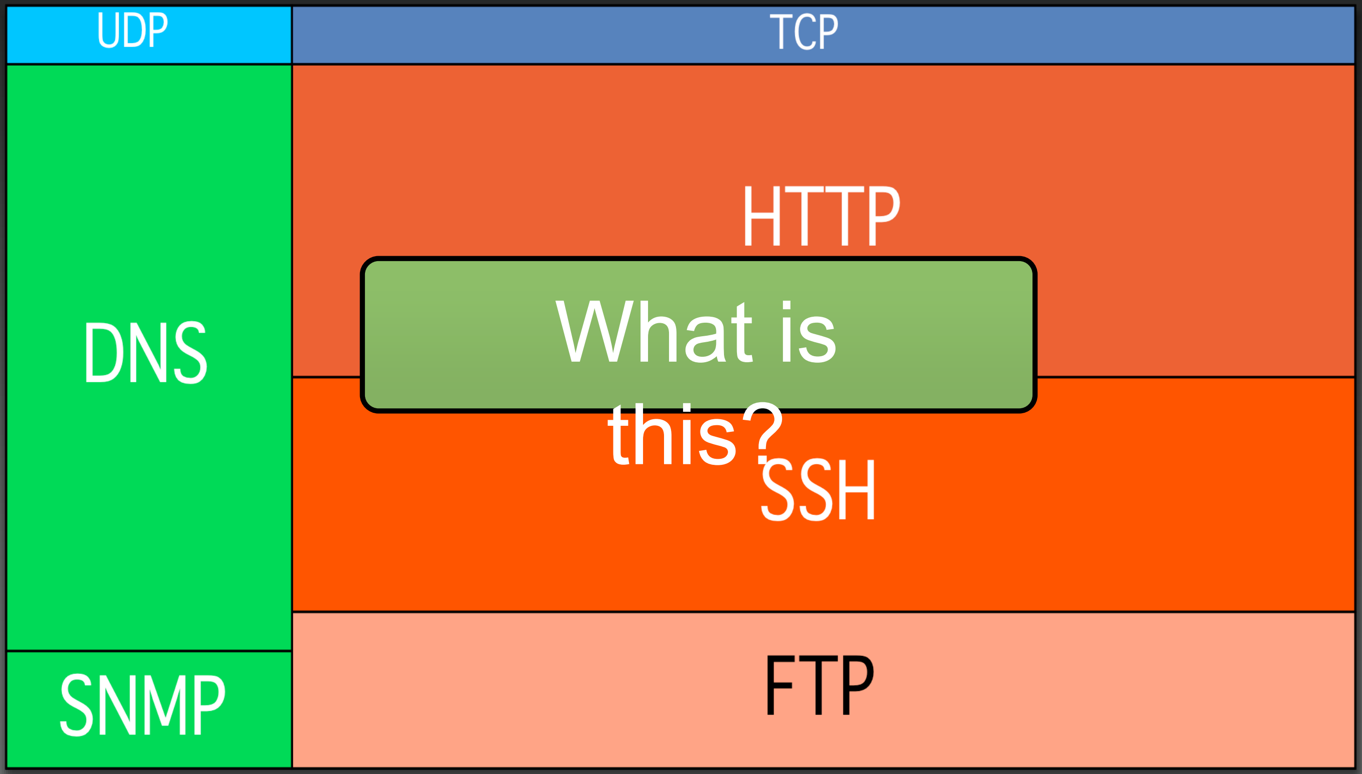
192.168.10.90 192.168.10.255 111

192.168.10.90 32859 111

RPC portmap 192.168.10.90 192.168.10.2

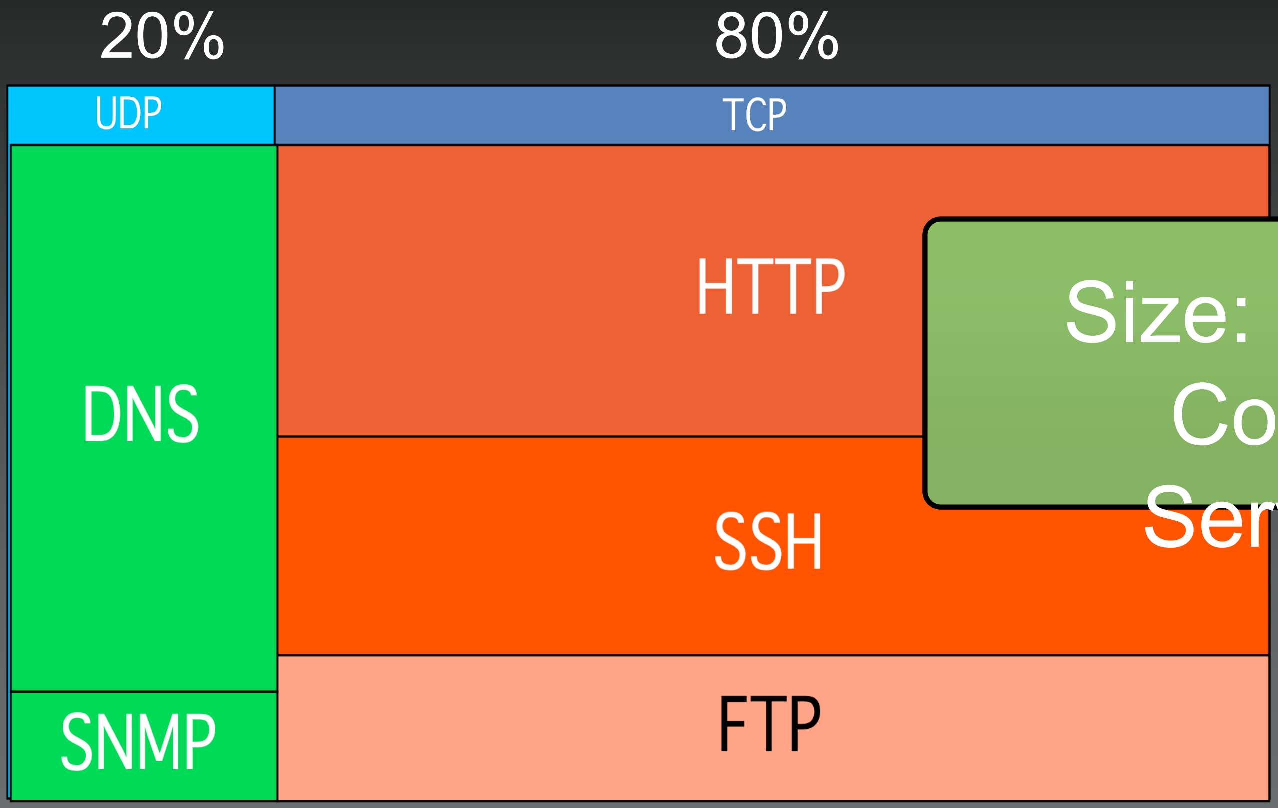
splunk>

TreeMaps



What is this?

TreeMaps Explained



Size: Count
Color: Service

Configuration Hierarchy: Protocol -> Service

Generating Graphs - For Free

- Log Collection
  - Database
  - Files
  - Syslog Collector
  - Splunk
- Graphing
  - AfterGlow (http://afterglow.sourceforge.net)
  - Treemap2 (http://www.cs.umd.edu/hcil/treemap)

AfterGlow

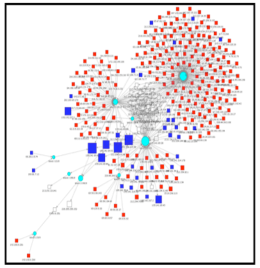
Parser

CSV File

AfterGlow

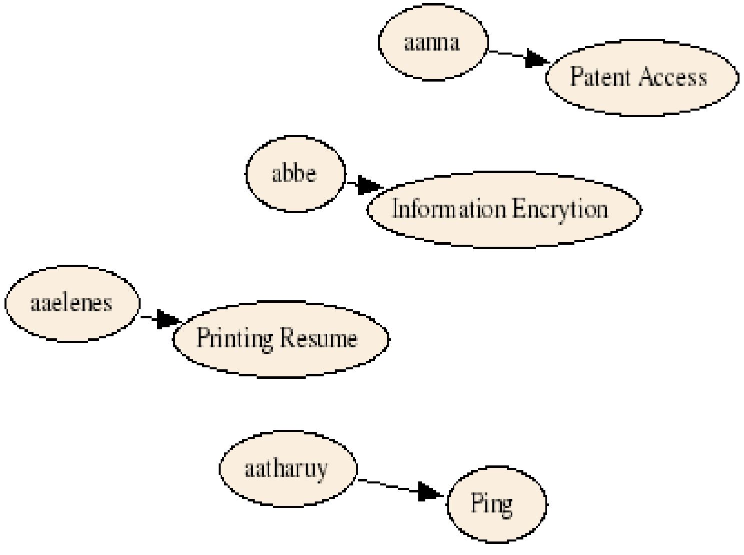
Graph LanguageFile

Grapher



aaelenes,Printing Resume
abbe,Information Encrytion
aanna,Patent Access
aatharuy,Ping

```
digraph   structs   {
  graph [label="      AfterGlow   1.5.8",      fontsize   =8];
  node [shape=ellipse  stvle=filled
               fontsize
               fixedsize
  edge [   len =1.6];

  "  aaelenes  " -> "Pı
  "  abbe" -> "Inform
  "  aanna" -> "Pater
  "  aatharuv  " -> "Pi
}
```

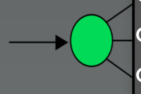


AfterGlow 1.5.9

Why AfterGlow?

- Translates CSV into graph des
- Define node and edge attribut
  - color
  - size
  - shape
- Filter and process data entries
  - threshold filter
  - fan-out filter
  - clustering

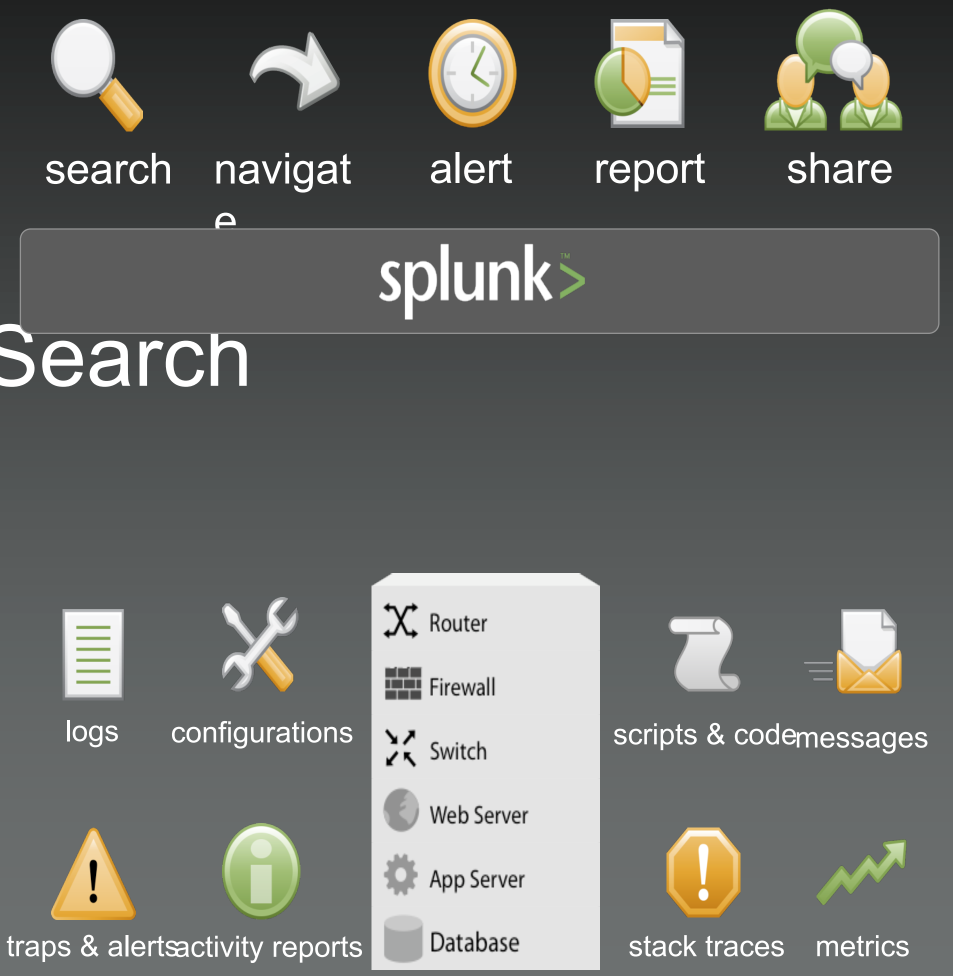
```
# Variable and Color

variable=@violation=("Backdoor Access", "HackerTool
Download”);
color.target="orange" if
(grep(/$fields[1]/,@violation));
color.target="palegreen"

# Node Size and Threshold

maxnodesize=1;
size.source=$fields[2]
size=0.5
sum.target=0;
threshold.source=14;

# Color and Cluster

color.source="palegreen" if ($fields[0] =~ /^111/)
color.source="red"
color.target="palegreen"
cluster.source=regex_replace("(\\d\+)\\.\\d+")."/8"
```



What’s Splunk?

1. Universal Real Time Indexing
2. Ad-hoc Search & Navigation
3. Distributed / Federate Search
4. Interactive Alerting & Reporting
5. Knowledge Capture & Sharing

The IT Search Engine



search

navigat
e

alert

report

share

splunk>

logs

configurations

Router

Firewall

Switch

Web Server

App Server

Database

scripts & code

messages

traps & alerts

activity reports

stack traces

metrics

AfterGlow - Splunk

```
./splunk <command>
./splunk search “<search command>” -admin <user>:<pass>

./splunk search "ipfw | fields + SourceAddress
DestinationAddress DestinationPort | afterglow" -auth
admin:changeme
```

Demo

Insider Threat Definition

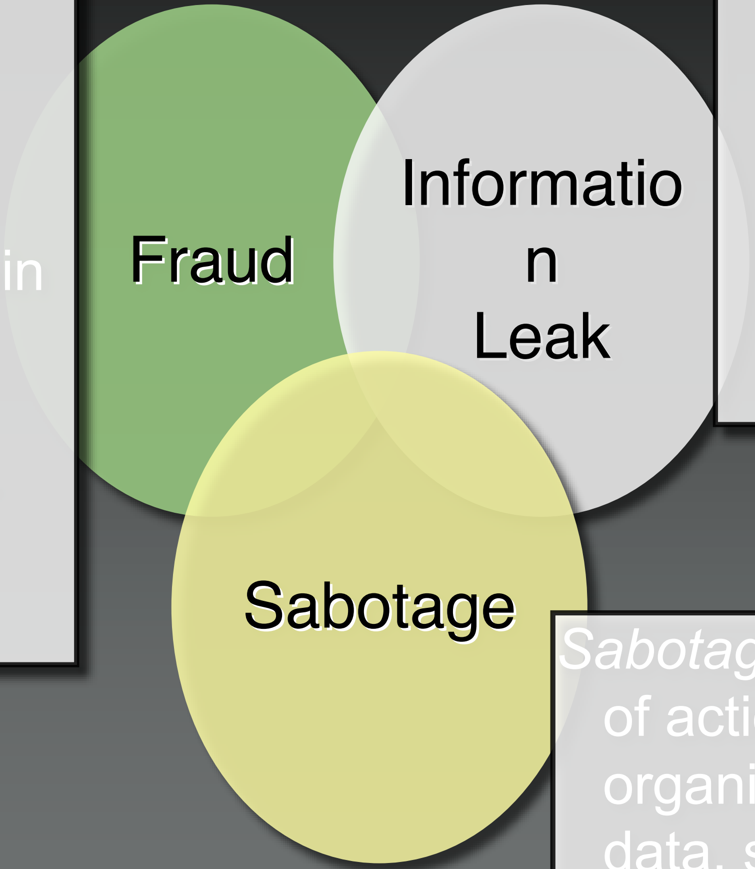
"Current or former employee or contractor who

- intentionally exceeded or misused an authorized level of access to networks, systems or data in a manner that
- targeted a specific individual or affected the security of the organization's data, systems and/or daily business operations"

[CERT: http://www.cert.org/insider_threat Definition of an Insider]

Three Types of Insider Threats

Fraud deals with the misuse of access privileges or the intentional excess of access levels to obtain property or services unjustly through deception or trickery.



Information Theft is concerned with stealing of confidential or proprietary information. This includes things like financial statements, intellectual property, design plans, source code, trade secrets, etc.

Sabotage has to do with any kind of action to harm individuals, organizations, organizational data, systems, or business operations.

Insider Threat Detection

- Understand who is behind the crime.
- Know what to look for
- Stop insiders **before** they become a problem

- Use ***precursors*** to monitor and profile users
- Define an insider detection process to analyze precursor activity

Insider Detection Process

- Build List of Precursors
- Assign ***Scores*** to Precursors

• Accessing job Web sites such as monster.com	1
• Sales person accessing patent filings	10
• Printing files with "resume" in the file name	5
• Sending emails to 50 or more recipients outside of the company	3

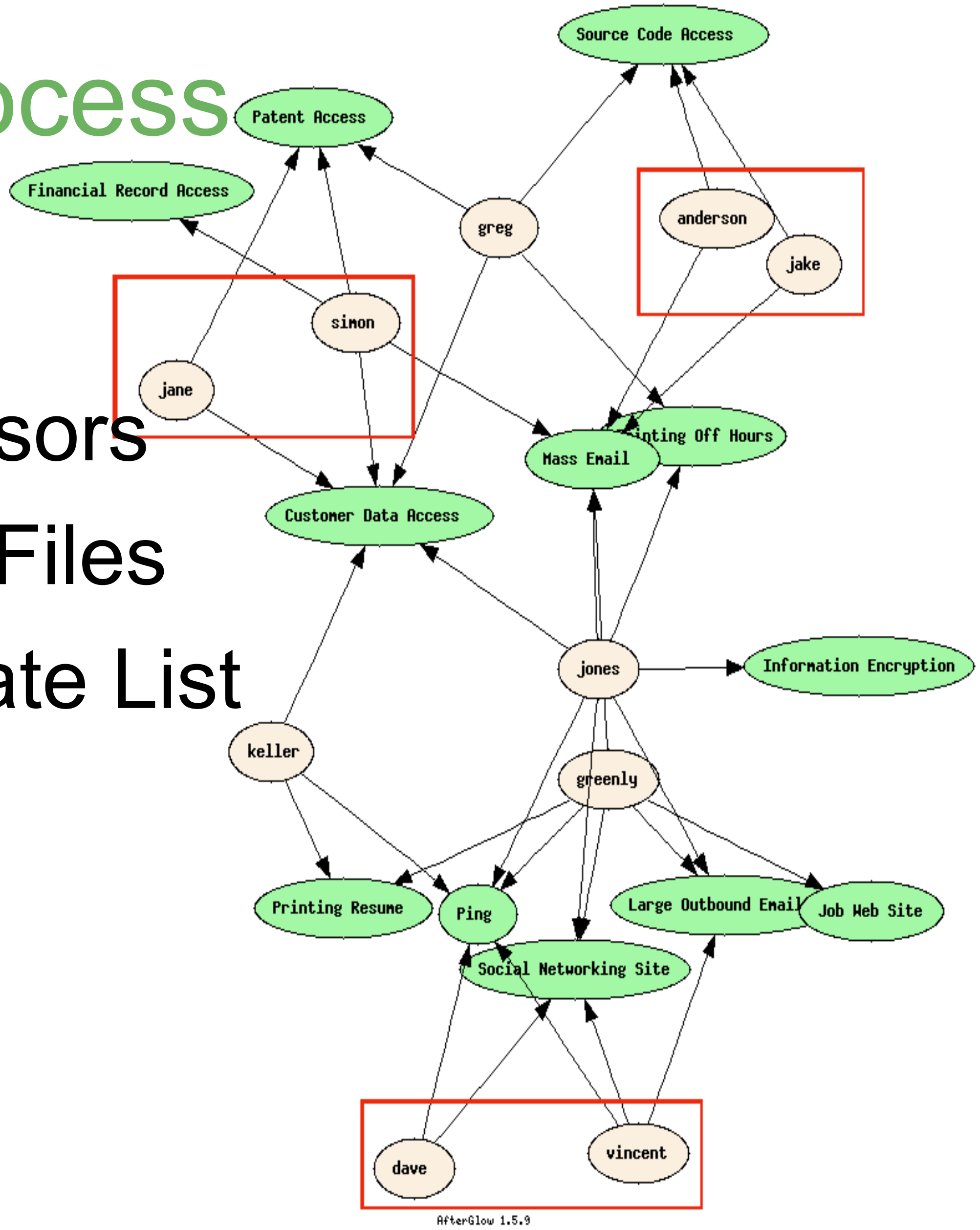
Insider Detection Process

- Build List of Precursors
- Assign ***Scores*** to Precursors
- Apply Precursors to Log Files

```
Aug 31 15:57:23  [68] ram
kCGErrorIllegalArgument:
CGXGetWindowDepth: Invalid window -1
Aug 31 15:58:06  [68] cmd "loginwindow"
(0x5c07) set hot key operating mode to all
disabled
Aug 31 15:58:06  [68] Hot key operating
mode is now all disabled
Aug 27 10:21:39 ram
com.apple.SecurityServer: authinternal failed
to authenticate user raffaelmarty.Aug 27
10:21:39 ram com.apple.SecurityServer:
Failed to authorize right system.login.tty by
process /usr/bin/sudo for authorization
created by /usr/bin/sudo.
Apr 04 19:45:29 rmarty Privoxy(b65ddba0)
Request:
www.google.com/search?q=password+crack
er
```

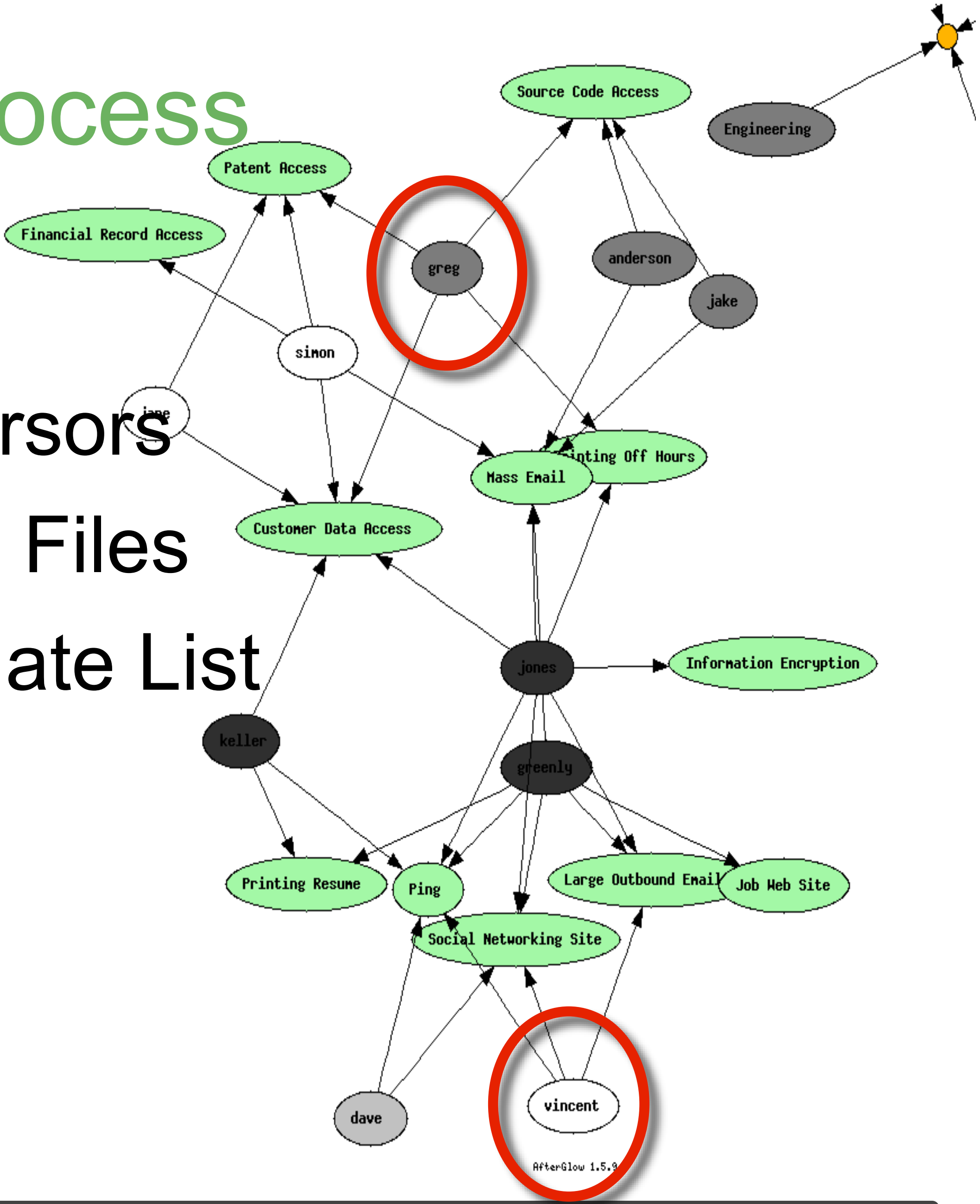
Insider Detection Process

- Build List of Precursors
- Assign ***Scores*** to Precursors
- Apply Precursors to Log Files
- Visualize Insider Candidate List



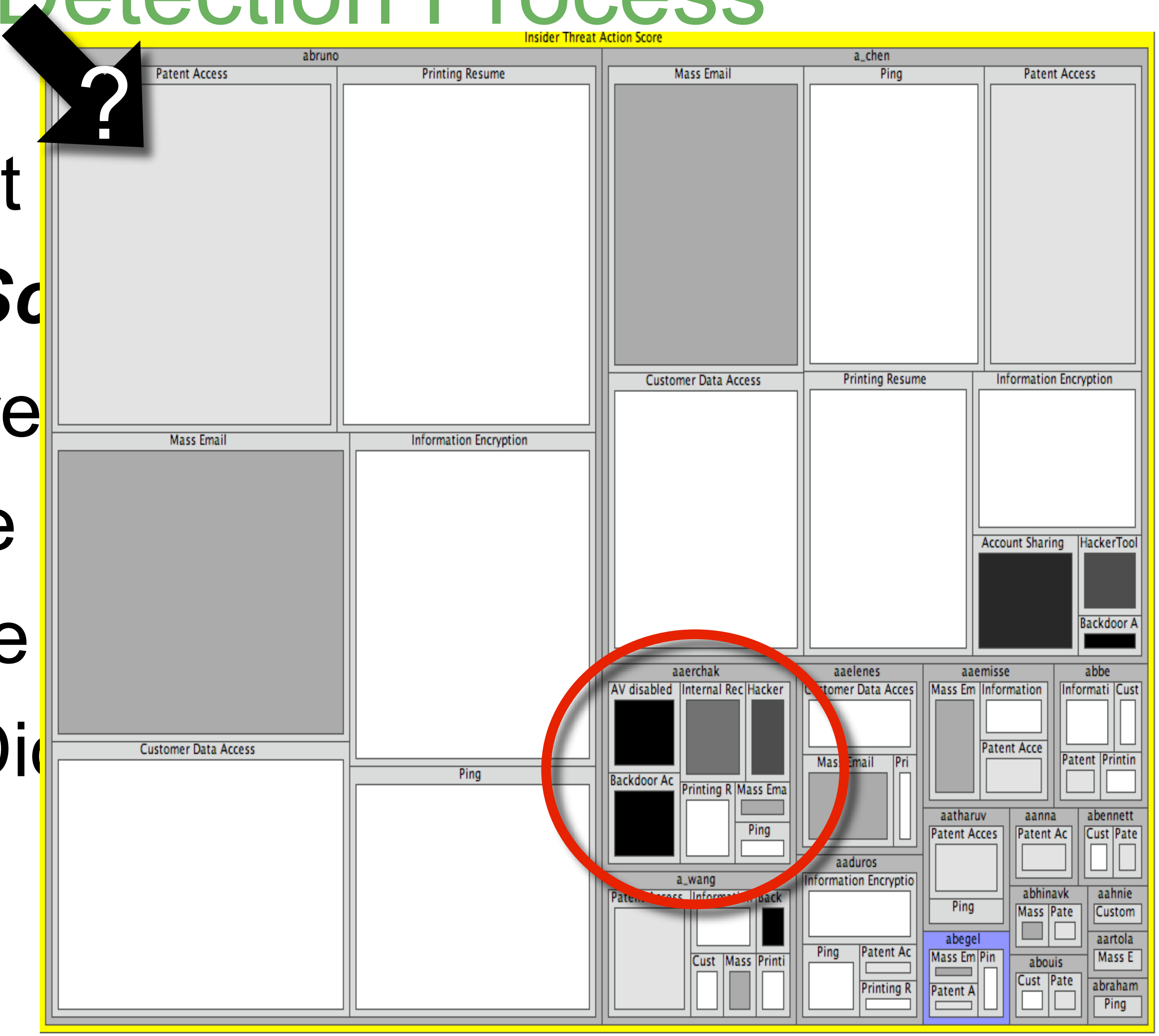
Insider Detection Process

- Build List of Precursors
- Assign ***Scores*** to Precursors
- Apply Precursors to Log Files
- Visualize Insider Candidate List
- Introduce User Roles



Insider Detection Process

- Build List
- Assign ***Sc***
- Apply Pre
- Visualize
- Introduce
- Where Di



splunk>

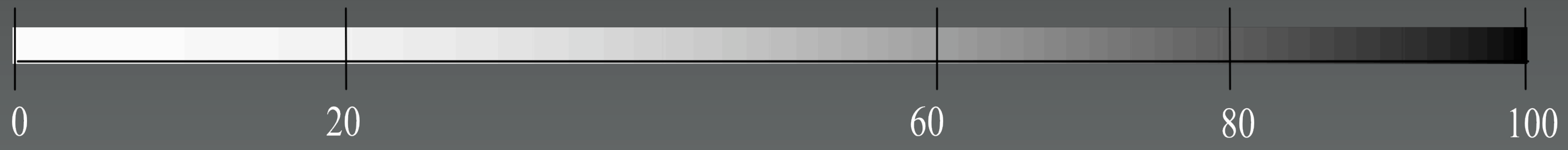
Tiers of Insiders

Nothing to worry about just yet

On a bad track of going malicious

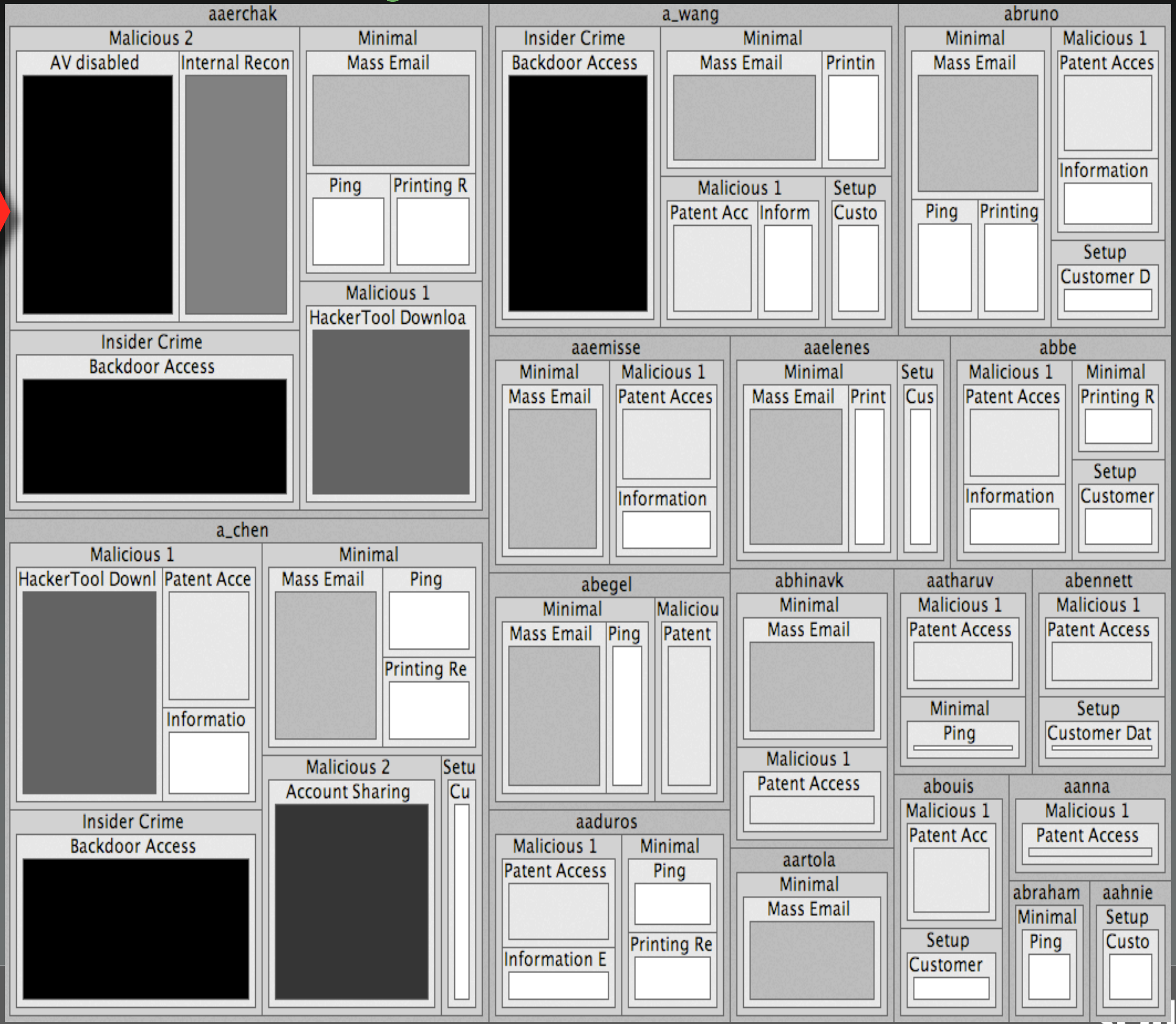
Very likely has malicious intentions

Malicious Insiders



The Insider? Finally?

Big, dark areas!



splunk>

Thank You

www.secviz.org

raffael.marty@splunk.com