Insider Threat –
The Visual Conviction

Raffael Marty, GCIA, CISSP
Manager Solutions @ ArcSight, Inc.

FIRST – June 2007 – Seville
Who Am I?

- Raffael Marty, GCIA, CISSP
- Manager Solutions @ ArcSight, Inc.
  - Log management, correlation
  - Regulatory compliance
- Intrusion Detection Research @ IBM Research
  - http://thor.cryptojail.net
- IT Security Consultant @ PriceWaterhouse Coopers
- Open Vulnerability and Assessment Language (OVAL) board member
- Common Event Enumeration (CEE) founding member
Who Am I?

- Passion for Visual Security Event Analysis
  - http://secviz.org
  - http://raffy.ch/blog
My Books / Book Contributions

Applied Security Visualization
Paperback: 350 pages
Publisher: Addison Wesley (February, 2008)
ISBN: 0321510100

How to Cheat at Configuring Open Source Security Tools
Paperback: 504 pages
Publisher: Syngress Publishing (May 1, 2007)
ISBN: 1597491705

Security Data Visualization
Paperback: 256 pages
Publisher: No Starch Press (August 25, 2007)
ISBN: 1593271433

Snort IDS and IPS Toolkit
Paperback:
Publisher: Syngress Publishing (April 20, 2007)
Agenda

- Visualization
- Insider Threat Theory
- Log Data Processing
- Open Source Visualization Tools
- Visualization Exercise with AfterGlow
- Simple I-Threat Visualizations
  - DuPont Information Leak
  - SAP Fraud Detection
Agenda

- Insider Detection Process (IDP)
- Applying IDP (Exercise)
- Insider Threat Solution
- Round Up
Disclaimer

“IP addresses and host names showing up in event graphs and descriptions were obfuscated/changed. The addresses are completely random and any resemblance with well-known addresses or host names are purely coincidental.”
Visualization
A Picture is Worth a Thousand Log Entries

Detect the Expected & Discover the Unexpected

Reduce Analysis and Response Times

Make Better Decisions
Why a Visual Approach Helps

A picture tells more than a thousand log lines

► Reduce analysis and response times
  • Quickly visualize thousands of events

► Make better decisions
  • Situational awareness
  • Visualize status of business posture
  • Visual display of most important properties

► Be more efficient
  • Facilitate communication
  • Use graphs to communicate with other teams
  • Graphs are easier to understand than textual events
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
Graph Types
Simple Charts

Bar Charts

Pie Charts

Line Charts

Scatter Plots

3D Scatter Plots
Graph Types
Multivariate Graphs

Link Graphs

Parallel Coordinates

TreeMaps

I like this word!
Multivariate Graphs
Link Graphs
Raw Event:
[**] [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 ->
192.168.10.255:111
UDP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:148 DF Len: 120

Different node configurations:
Tree Maps

What is this?

<table>
<thead>
<tr>
<th>UDP</th>
<th>TCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>HTTP</td>
</tr>
<tr>
<td></td>
<td>SSH</td>
</tr>
<tr>
<td>SNMP</td>
<td>FTP</td>
</tr>
</tbody>
</table>
Configuration (Hierarchy): Protocol
Tree Maps

Configuration (Hierarchy): Protocol -> Service
Size: Count
Color: Protocol
Tree Maps
Advanced Usage

► More than three dimensions

► Probably less than 5 dimensions

► Color and Size
  • Additional dimensions
  • Not shown in the “main” hierarchy
### Parallel Coordinates

<table>
<thead>
<tr>
<th>Action</th>
<th>Rule</th>
<th>SIP</th>
<th>Asset Role</th>
<th>DIP</th>
<th>Flag</th>
</tr>
</thead>
</table>

- Size proportional to occurrence
- Selection propagates
- n dimensions

Copyright (c) 2007 by Raffael Marty
Questions and Answers
Thank You

Raffael Marty
Manager Solutions
ArcSight, Inc.

raffy@secviz.org

..................

Security Data Visualization
www.secviz.org

ArcSight®
Insider Threat Theory

Raffael Marty, GCIA, CISSP
Manager Solutions @ ArcSight, Inc.

FIRST – June 2007 – Seville
Agenda

- Visualization

😊 Insider Threat Theory

- Log Data Processing
- Open Source Visualization Tools

- Visualization Exercise with AfterGlow
- Simple I-Threat Visualizations
  - DuPont Information Leak
  - SAP Fraud Detection
Insider Threat
Definition

"Current or former employee or contractors 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]
Insider Threat
Three Types of Insider Threat

- Fraud
- Sabotage
- Information Theft
*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.
Insider Threat
Information Theft

► Hard to stop:

• Cell Phones / iPods / USB sticks

• Email

• Hard copies (printer)

► Information is intangible. How do you protect that?
Insider Threat
Information Protection

► Extrusion Detection

► Document Management

► Policies and Procedures

► Awareness

► Document Classification

► …
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.
Insider Threat
Type of Fraud

► Real estate
► Insurance
► Tax
► Bank
► Occupational
► Financial Statement
Various different approaches

• User Identification

• Transaction verification / checks and balances

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

- Information Destruction
- Denial of Service
- Theft
- Harm to organization of individuals
How can you detect this?

Wouldn’t it be too late if you detected sabotage?
Insider Threat Personae
Why are They Important?

► Understand who is behind the crime.
► Know what to look for
► Stop insiders **before** they become a problem
Former employees or employees on their way out

Three types

• Financially motivated
• Employees taking information to new job (starting new company)
• Embarrass former employee (organization or individual)

Using their access privileges and in some cases compromised accounts

Mostly committed crime from within workspace
Insider Persona
Fraudsters

- Current employees
- Using their own account and access privileges
- Generally have system administration or privileged access
- While financially motivated, fraudsters are in general not in financial need
- Generally no sophisticated attack methods (such as exploits)
- Mostly committed crime from within workspace
Insider Persona
Saboteur

► Former employees

► Revenge for negative event (fired, no bonus, new boss, etc.)

► Generally (used to) have system administration or privileged access

► No authorized access when committing crime

► Mostly using compromised accounts, some using backdoor accounts

► Some using technically sophisticated means (scripts as logic bombs, etc.)

► Some took preparatory action
Questions and Answers
Thank You

Raffael Marty
Manager Solutions
ArcSight, Inc.

raffy@secviz.org

Security Data Visualization
www.secviz.org
Insider Threat –
Log Data Processing

Raffael Marty, GCIA, CISSP
Manager Solutions @ ArcSight, Inc.

FIRST – June 2007 – Seville
Agenda

- Visualization
- Insider Threat Theory

Log Data Processing
- Open Source Visualization Tools
- **Visualization Exercise with AfterGlow**
- Simple I-Threat Visualizations
  - DuPont Information Leak
  - SAP Fraud Detection
What Tools Are You Using For Log Processing?
How To Generate A Graph

Device | Normalization | Event Visualizer

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 network: Bringing up interface eth0: failed
Jun 17 09:42:39 rmarty sendmail: sendmail startup succeeded
Jun 17 09:42:39 rmarty sendmail: sendmail 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 09:56:03 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

Log File
UNIX Tools

► awk

awk -F, '{printf("%s,%s",$2,$1);}'}

► Sed

sed 's/fubar/foobar/' filename

► Grep

cat file | grep -v
Regular Expressions

What?

► Text processing
  • Searching
  • Replacing
  • Extracting

► Example

Raf{2}a.l Mart[yi]
Regular Expressions
Basics

^  Beginning of string
$  End of string
.  Any character
[  Start of character list
]  End of character list
(  Start of expression group
)  End of expression group
|  ORs two expressions
\  Escape character
*  Preceding expression occurs zero or more times
?  Preceding expression occurs zero or one times
+  Preceding expression occurs one or more times
Regular Expressions Examples

► Searching
  • perl -ne 'print if (/^1/)\' file.txt
  • egrep '^1[0-9]+ +K' file.txt

► Replacing
  • perl -pe 's/^ +//' phonelist.txt
  • sed 's/^$/d' price.txt

► Extracting
  • perl -pe 's/.*(IN=([^ ]*)\).*$/\1/'
Greedy vs. non-greedy

Apr 17 08:22:27 rmarty kernel: OutputIN= OUT=vmnet8 SRC=192.168.170.1 DST=192.168.170.255 LEN=258 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=138 DPT=138 LEN=238

```
perl -pe 's/(.*) .*/\1/'
```

```
OUT=vmnet8 SRC=192.168.170.1 DST=192.168.170.255 LEN=258 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=138 DPT=138
```

```
perl -pe 's/(.*) .*/\1/'
```

```
OUT=vmnet8
```
Crazy example: Creates an index of links from a HTML file

s/<\[\s]*\[Aa][ ]*\[Hh][Rr][Ee][Ff]/<a href=/g
:loop
/a href *= *"[^#]"/;
x; s/[^\n]*&;9876543210 999990000099990000999000990090;/
s/([0-8]{0,1})\(9*\);[^1]*(.\)1[^;]*2\(0*\)[^;]*\([^;]*\)/3\4\5/
x; G; s
<a href *= *"([^\n]+)"[^>]*>/([^\n]*\(\n\))/(^[^\n]*\)/(.*$)\</a href="[^\n]*\(\n\)"[^>]*>\</a href="/a href=g;


 Regular Expressions
Advanced
Simple tools:

(Stolen from: http://raffy.ch/blog/2007/02/24/geo-lookup-on-the-command-line/)

```
10/13/2005 20:25:54.032145,195.141.211.178,195.131.61.44,2071,135

I want to get the country of the source address (first IP in the log):

cat pflog.csv | perl -M'Geo::IPfree' -na -F',/' -e '($country,$country_name)=Geo::IPfree::LookUp($F[1]);chomp; print "$_,$country_name
"

And here the output:

```
Data Sources
Different Data Sources

► PCAP

► Firewall (PF)
  • IP Tables and why its logging is bad

► Argus

► Snort
PCAP

- Packet Captures
- Binary format
- `tcpdump -nnlr <file>`
PF Firewall

► OpenBSD Firewall

Feb 18 13:39:27.977280 rule 71/0(match): pass in on xl0: 195.27.249.139.63285 > 195.141.69.42.80: S 340743432:340743432(0) win 32768 <mss 1460,nop,wscale 0,nop,nop,timestamp 24078 0> (DF)

► Reading the file/interface (which is in pseudo PCAP):

tcpdump -nnli pflog

► Make sure you are using the OpenBSD tcpdump!!
“Argus is an IP transaction auditing tool that categorizes IP packets which match the boolean expression into a protocol-specific network transaction model. Argus reports on the transactions that it discovers, as they occur.”
10 Apr 06 10:55:46  *  tcp  217.118.195.58.22  ?>
   65.219.2.99.37065 1280  1550  309440  23952  RST

- Timestamp
- Protocol
- SourceIP . SourcePort
- Direction
- DestinationIP . DestinationPort
- PacketsIn and PacketsOut
- BytesIn and BytesOut
- Status
Parsers
Parsers

► Parser?

“To analyze or separate (input, for example) into more easily processed components.” (answers.com)

► Interpret Data
► Knows data format
► Re-use don’t re-invent!
► The UNIX Paradigm: Work in a pipe!
► Some available on:

http://secviz.org/?q=node/8
AfterGlow
Parsers

► tcpdump2csv.pl
- Takes care of swapping response source and targets

```
tcpdump -vvttttnnelr /tmp/log.tcpdump | ./tcpdump2csv.pl "sip dip sport"
```

► sendmail_parser.pl
- Reassemble email conversations:

```
Jul 24 21:01:16 rmarty sendmail[17072]: j6P41Gqt017072:
from=<root@localhost.localdomain>, size=650, class=0, nrcpts=1,
Jul 24 21:01:16 rmarty sendmail[17073]: j6P41Gqt017072: to=ram,
ctladdr=<root@localhost.localdomain> (0/0), delay=00:00:00,
xdelay=00:00:00, mailer=local, pri=30881, dsn=2.0.0, stat=Sent
```
AfterGlow
Parsers

► Argus2csv.pl

ragator -r file.argus -nn -A -s +dur -s +sttl -s +dttl | ./argus2csv.pl “src dst pkts”

► pf2csv.pl

• Parsing OpenBSD pf output

tcpdump -nnli pflog | ./pflog.pl “src dst rule”

► snortalert2csv.pl

cat alert | ./snortalert2csv.pl “name src dport”
These tools are part of AfterGlow 1.5.8

mergeLogs.pl

```
./merge_logs.pl lookup.csv file.csv
```

```
lookup.csv
Account Sharing,9
AV disabled,10
Backdoor Access,10
Customer Data Access,2

file.csv
rweiss,AV disabled,10
wcwu,Account Sharing,8
bgrosof,Backdoor Access,10
```

Output:
```
rweiss,AV disabled,10
wcwu,Account Sharing,8
bgrosof,Backdoor Access,10
```
anonymize.pl

`cat file | ./anonymize.pl -c 1 -p user`

*Original:*
- rweiss, AV disabled
- wcwu, Internal Recon
- bgrosof, Source Code Access

*Anonymized:*
- user1, AV disabled
- user2, Internal Recon
- user3, Source Code Access
Questions and Answers
Thank You

Raffael Marty
Manager Solutions
ArcSight, Inc.
raffy@secviz.org

Security Data Visualization
www.secviz.org
Insider Threat – Open Source Tools

Raffael Marty, GCIA, CISSP
Manager Solutions @ ArcSight, Inc.

FIRST – June 2007 – Seville
Agenda

- Visualization
- Insider Threat Theory
- Log Data Processing

😊 Open Source Visualization Tools

- Visualization Exercise with AfterGlow
- Simple I-Threat Visualizations
  - DuPont Information Leak
  - SAP Fraud Detection
What are some tools?

- AfterGlow 1.5.8
  
  http://afterglow.sourceforge.net

- Treemap2
  
  www.cs.umd.edu/hcil/treemap/

- …
Supported graphing tools:

- GraphViz from AT&T (dot, neato, circo, twopi)
  http://www.graphviz.org

- LGL (Large Graph Layout) by Alex Adai
  http://bioinformatics.icmb.utexas.edu/lgl/
AfterGlow 1.x

Parser

CSV File

AfterGlow

Graph

LanguageFile

Grapher

aaelenes, Printing Resume
abbe, Information Encryption
aanna, Patent Access
aatharuv, Ping

digraph structs {
    graph [label="AfterGlow 1.5.8", fontsize=8];
    node [shape=ellipse, style=filled,
          fontsize=10, width=1, height=1,
          fixedsize=true];
    edge [len=1.6];

    "aaelenes" -> "Printing Resume" ;
    "abbe" -> "Information Encryption" ;
    "aanna" -> "Patent Access" ;
    "aatharuv" -> "Ping" ;
}

ArcSight
AfterGlow 1.x

Features

► Generate Link Graphs
► Filtering Nodes
  • Based on name
  • Based on number of occurrences
► Fan Out Filtering
► Coloring
  • Edges
  • Nodes
► Clustering
Features

► Node Sizes
  • Auto adjustment

► Variables
AfterGlow 1.x
Property File – Color Definition

- Coloring:
  
  ```perl
  color.[source|event|target|edge|sourcetarget] = <perl expression returning a color name>
  
  Array @fields contains input-line, split into tokens:
  
  color.event="red" if ($fields[1] =~ /^192\..*\n  
  Filter nodes with “invisible” color:
  
  color.target="invisible" if ($fields[0] eq "IIS Action")
  ```
Input Data:
- a, b
- a, c
- b, c
- d, e

Output:

Command:
cat file | ./afterglow -c simple.properties -t \neato -Tgif -o test.gif

simple.properties:
color.source="green" if ($fields[0] ne "d")
color.target="blue" if ($fields[1] ne "e")
color.source="red"
color="green"
Threshold:

threshold.[source|event|target]=<value>
Clustering:

\[
\text{cluster.}[\text{source}|\text{event}|\text{target}]=\text{<perl expression returning a cluster name>}
\]

Node Sizes:

\[
\text{size.}[\text{source}|\text{event}|\text{target}]=\text{<perl expression returning a number>}
\]

Maxnodesize=\text{<value>}

\[
\text{sum.}[\text{source}|\text{event}|\text{target}]=[0|1]
\]
Variables

Definition:

```bash
# Watch Lists
variable=@privileged=( "aaerchak" );
```

Use:

```bash
color.target="gold" if (grep(/$fields[0]//,@privileged));
```

There are no limits on what you do with the “variables” keyword! You can put entire scripts in there!
AfterGlow 1.x
Running AfterGlow

cat data | ./afterglow.pl -c file.prop | neato -Tgif -otest.gif

Usage: perl afterglow.pl [-adhnstv] ...

-a : turn off labelelling of the output graph with the configuration used
-b lines : number of lines to skip (e.g., 1 for header line)
-c conffile : color config file
-d : print node count
-e length : edge length
-f threshold : source fan out threshold
-g threshold : event fan out threshold (only in three node mode)
-h : this (help) message
-l lines : the maximum number of lines to read
-m : the maximum size for a node
-n : don't print node labels
-o threshold : omit threshold (minimum count for nodes to be displayed)
             Non-connected nodes will be filtered too.
-p mode : split mode for predicate nodes where mode is
          0 = only one unique predicate node (default)
          1 = one predicate node per unique subject node.
          2 = one predicate node per unique target node.
          3 = one predicate node per unique source/target node.
-s : split subject and object nodes
-t : two node mode (skip over objects)
-v : verbose output
-x : text label color
# 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"
**TM3** file (I am going to use a simple, but practical form!)

- Tab delimited
- Two special header lines

<table>
<thead>
<tr>
<th>Target System</th>
<th>DIP</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial System</td>
<td>212.254.109.27</td>
<td>pass</td>
</tr>
<tr>
<td>Financial System</td>
<td>212.254.109.27</td>
<td>block</td>
</tr>
<tr>
<td>Financial System</td>
<td>212.254.110.102</td>
<td>pass</td>
</tr>
<tr>
<td>Mail Server</td>
<td>212.254.110.99</td>
<td>block</td>
</tr>
<tr>
<td>Mail Server</td>
<td>212.254.110.97</td>
<td>block</td>
</tr>
</tbody>
</table>
First Header Line: *Column Names*

Second Header Line: *Data Types*

<table>
<thead>
<tr>
<th>Count Target System</th>
<th>DIP</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTEGER</td>
<td>STRING</td>
<td>STRING</td>
</tr>
</tbody>
</table>
Agenda

- Visualization
- Insider Threat Theory
- Log Data Processing
- Open Source Visualization Tools

😊 Visualization Exercise with AfterGlow

- Simple I-Threat Visualizations
  - DuPont Information Leak
  - SAP Fraud Detection
Questions and Answers
Raffael Marty  
Manager Solutions  
ArcSight, Inc.  

raffy@secviz.org  

Security Data Visualization  
www.secviz.org
Insider Threat –
Simple iThreat Example

Raffael Marty, GCIA, CISSP
Manager Solutions @ ArcSight, Inc.

FIRST – June 2007 – Seville
Agenda

- Visualization
- Insider Threat Theory
- Log Data Processing
- Open Source Visualization Tools
- Visualization Exercise with AfterGlow

😊 Simple I-Threat Visualizations
- DuPont Information Leak
- SAP Fraud Detection
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
A Simple Solution

Log Collection
DuPont Case
A Simple Solution
DuPont Case
A Not so Targeted Solution

Size: #accesses
Thank You

Raffael Marty
Manager Solutions
ArcSight, Inc.

raffy@secviz.org

Security Data Visualization
www.secviz.org
Insider Detection Process

Raffael Marty, GCIA, CISSP
Manager Solutions @ ArcSight, Inc.

FIRST – June 2007 – Seville
Agenda

😊 Insider Detection Process (IDP)

- Applying IDP (Exercise)
- Insider Threat Solution
- Round Up
Insider Threat Detection Process
Overview

► Intro
► Precursors
► Scoring Precursors
► Visualizing
► Watch Lists
► Advanced Scoring
The following *Insider Threat Detection Process* is

- Ongoing research
- A proposed approach
- Not a guarantee for success
- Probably going to fail in your environment
- A lot of work to execute
- Incredibly interesting and generates nice graphs

**Related Work:** (no visualization, but uses precursors)

- "*ELICIT: A System for Detecting Insiders Who Violate Need-to-know*", Mark Maloof and Greg Stephens
Insider Threat Detection Process

Precursors

► A precursor is an activity that when observed, flags the associated user as a potential insider.

Some research calls this “detectors”.

► Examples:

• Printing off-hours
• Downloading Hacker Tools
• Accessing documents outside of user’s role
• Use of anonymous proxy
Each precursor can be assigned a score which reflects the extent to which the precursor classifies someone as an insider.

Factors to consider:

- Impact of action
- Rate of False Positives
- Is this okay for some user roles?

If I actually new some math, I would use a Bayesian Inference network for this ;-)}
Insider Threat Detection Process Visualization

► User -> Precursor -> Score

► Find outliers

  • Based on groups of users with similar behavior

  • Based on scores
Insider Threat Detection Process
Watch Lists

► Keep track of specific users

• Privileged accounts
• Contractors
• Terminated Employees
Based on the watch lists, adjust the precursor scores for these users.

For example, a user name on the terminated employees list: +5!
Insider Threat Detection Process
Advanced Watch List Application

► Do role-based behavior assessment based on watch lists
► Color users based on watch list
► Quickly spot groups, outliers, anomalies
Insider Threat Detection Process
Scoring and Coloring based on Watch Lists
Insider Threat Detection Process
Precursor Categories

Problem of scoring so far:

- Repetitive “not so bad” behavior escalates a user immediately.

Group precursors:

1. Minimal or no impact
2. Signs of a setup for a malicious act
3. Malicious behavior, normal for some users
4. Malicious behavior, this should _never_ happen
5. The insider crime itself
Insider Threat Detection Process

User Tiers

- User can accumulate a max of 20 points per category
- Categorize users based on score:

  - Nothing to worry about just yet
  - On a bad track of going malicious
  - Very likely has malicious intentions
  - Malicious Insiders
Questions and Answers
Thank You

Raffael Marty
Manager Solutions
ArcSight, Inc.

raffy@secviz.org

Security Data Visualization
www.secviz.org