

# **Analysis and Management Tools (IDS)**

## **Open Source Security Tools for Information Technology Professionals**

**School of Professional Studies (SPS)**

**The City University of New York (CUNY)**

Aron Trauring  
Adjunct Professor  
CEO, Zoteca

Class 11 December 5th, 2005

# Analyzing Information

- Too much information leads to “analysis paralysis”
- Sysadmins often ignore available information for “lack of time”
- Need tools to quickly analyze and manage output of tools

# System Logs

- `/var/log/messages`
- `/var/log/syslog`
- Failed logins precursor to attack
- Servers rebooting at strange time
- Syslog Data Mining Tools [http://www.syslog.org/index.php?name=Web\\_Links&req=viewlink&cid=4&min=0&orderby=titleA&show=10](http://www.syslog.org/index.php?name=Web_Links&req=viewlink&cid=4&min=0&orderby=titleA&show=10)

## Swatch

- How To Configure Swatch <http://sial.org/howto/logging/swatch/>
- Looks for some string in logfile
- Takes notification action (e.g. send email) if match is found

## SEC — Simple Event Correlator

- Triggering Actions Using SEC <http://sial.org/howto/logging/sec.pl/>
- Looks for some string in logfile
- Takes real action (e.g. generate firewall rule) if match is found

# Network Monitoring Systems

- Nagios Screenshots <http://www.nagios.org/about/screenshots.php>
- Pluggable architecture
- Works with backend database
- Nagmin — Webmin management plugin
- Nagmin Screenshots [http://nagmin.sourceforge.net/screen\\_shots.htmNa](http://nagmin.sourceforge.net/screen_shots.htmNa)
- OpenNMS

# Analysis Console for Intrusion Databases (ACID)

- Works with `snort` and `syslog`
- Port all IDS data into a database
- Sort and organize from database
- ACID Screenshots <http://www.cert.org/kb/acid/>

# SGUIL - The Analyst Console for Network Security Monitoring

- GUI-based vs. ACID web-based
- Claims deeper and quicker analysis
- SGUIL Screenshots `http://sguil.sourceforge.net/index.php?page=screenshots`
- SGUIL Flash Demo `http://sguil.sourceforge.net/index.php?page=flashdemo`