

# Putting Logs on a Diet

Maximizing Impact and Effect of your Logs

10 December 2011 – BayThreat 2011 – Mountain View, CA



Presented by:  
Kevin W. Lawrence  
Stach & Liu, LLC  
[www.stachliu.com](http://www.stachliu.com)

# Agenda

## OVERVIEW

- Introduction/Background
- Baseline
  - Why Log
  - Less is More
  - Targeting
- Analyze
  - Combing Logs
  - Execution
- Recap

# Introduction/ Background

# About Me

- Senior Security Associate for Stach & Liu
- Over eight years designing, implementing, and responding to various cyber security controls
- Alphabet Soup
  - CISSP, GCIA, GREM, GCFA, CEH

# Problem Statement

Finding actionable security events within system, network, and application logs can be overwhelming due to data volume.

# Baseline

What do your logs tell you?

# Why Log

- Auditing

# Why Log

- Auditing
  - Compliance



# Why Log

- Auditing
  - Compliance
- Operational Monitoring

# Why Log

- Auditing
  - Compliance
- Operational Monitoring
  - Up/Down
  - Performance

# Why Log

- Auditing
  - Compliance
- Operational Monitoring
  - Up/Down
  - Performance
- Security

# Why Log

- Auditing
  - Compliance
- Operational Monitoring
  - Up/Down
  - Performance
- Security
- Solving A Problem

# Less is More

- Filter

# Less is More

- Filter
  - Before

# Less is More

- Filter
  - Before
  - During

# Less is More

- Filter
  - Before
  - During
  - After



# Less is More

- Filter
  - Before
  - During
  - After
- Signal to Noise



# Targeting

- What Do You Need

# Targeting

- What Do You Need
- Removing Known Good

# Targeting

- What Do You Need
- Removing Known Good
- What Can You See

# Targeting

- What Do You Need
- Removing Known Good
- What Can You Use
- Remove Excess Data

# Analyze

# Combing Logs

- Aggregate and Correlate



# Combing Logs

- Aggregate and Correlate
- Multiple Sources

# Combing Logs

- Aggregate and Correlate
- Multiple Sources
  - Network
  - System
  - Application

# Combing Logs

- Aggregate and Correlate
- Multiple Sources
  - Network
  - System
  - Application
- Time

# Combing Logs

- Aggregate and Correlate
- Multiple Sources
  - Network
  - System
  - Application
- Time
  - NTP
  - Time Zone

# Execution

- Monitor Log Flow

# Execution

- Monitor Log Flow
  - Passive

# Execution

- Monitor Log Flow
  - Passive
  - Active

# Execution

- Monitor Log Flow
  - Passive
  - Active
- Honey Tokens



# Execution

- Monitor Log Flow
  - Passive
  - Active
- Honey Tokens
  - Credentials
    - Accounts
  - Database
    - Records
  - API
    - Keys
  - Files
    - Robot.txt

Adminn00b

Credit Card Numbers

Social Network API Keys

oldadmin.php

# Future Direction

# Future

- Integration

# Future

- Integration
- Automation

# Future

- Integration
- Automation
- Proactive Detection

# Recap

- **Baseline**
  - Why Log
  - Less is More
  - Targeting
- **Analyze**
  - Combing Logs
  - Execution

# Special Thanks

Christie Grabyan

Fran Brown

Vincent Liu

# Questions?

For more info:

Email:

[klawrence@stachliu.com](mailto:klawrence@stachliu.com)

Stach & Liu, LLC

[www.stachliu.com](http://www.stachliu.com)



Thank You