ITAC 2015

IT AUDIT & CONTROLS CONFERENCE

Putting Your Logs On A Diet

1 October 2015

11:00 AM

Kevin W. Lawrence

Senior Security Associate

Bishop Fox

MIS|TI TRAINING INSTITUTE

ITAC 2015

IT AUDIT & CONTROLS CONFERENCE

Presentation will be available at:

www.misti.com/download

Download password is available in your Show Guide

MIS|TI
TRAINING INSTITUTE

Key Points

- Introduction/Background
- Monitoring Your Environment
- Establishing A Baseline
- Threat Intelligence
- Intelligent Monitoring
- Summary

About Me – Who Am I?

Kevin W. Lawrence

- Senior Security Associate at Bishop Fox
- Security Operations, defensive network security, and incident response
- Multiple Certifications
- Background in Fortune 50 including Honeywell and IBM
- 10 years in the security industry

Monitoring

Use Cases

- **Business** – What is the business worried about?
  - Too many transactions
  - Unintended abuses
  - Accounting
  - Application errors
- **Security** – What concerns security?
  - Authentication
  - Network scanning
  - High-risk actions
  - Unusual network sessions
- **Anomalistic** – What isn't "normal?"
  - Baseline deviations
  - Traffic spikes
- **Other** – Think about extra use cases:
  - Honeypots
  - Honey tokens

Baseline

What is a Baseline?

- Creating a baseline is the act of establishing a known level of activity from one or more data sources.

Why Baseline?

- Baseline to identify anomalous or unusual activity that may be indicative of a possible attack.

Signal to Noise

- Filtering log data before, during, and after collection can help to better identify malicious activity. Filtering is important, but comparing to a known baseline is better.

Baseline

Combine Logs

- Aggregate and correlate multiple sources of data.

Time Synchronization

- Synchronize all log sources to a single authoritative time source. Time zones should also be synchronized when possible.

Threat Intelligence

What is TI?

- Threat intelligence is the knowledge of new or emerging threats based on specific evidence that may include information to detect or respond effectively.

Why keep up?

- Staying up-to-date helps prepare and identify new and emerging attacks that may be focused on a given industry segment or vendor.

Threat Intelligence

Source	Examples
Threat Feeds	• Paid feeds from security providers and researchers • Free feeds from community services
Websites	• Security websites • Vendor websites • Threat sharing websites
Media	• News stations • Webcasts • Conferences

Intelligent Monitoring

What is Intelligent Monitoring?

- Intelligent monitoring is the act of looking for new and emerging threats in your monitoring solutions.
- It uses information provided by a threat intelligence source to modify the focus of your monitoring tools.

Why use Intelligent Monitoring?

- This allows you to identify and detect new and emerging attacks before an attacker successfully breaches your network.

Intelligent Monitoring

Dynamic Monitoring

- Automatic monitoring occurs based on information from a threat intelligence source.

Preventative Detections

- These detections block or patch vulnerable systems and tools based upon information and recommendations from threat intelligence sources.

Information Sharing

- This provides additional anonymized information about what detective, preventative, and remediation solutions work best for you.
- Don’t just take the information; share what you have learned.

Summary

- **Monitoring** – Don't just log your data, watch and review it for potential security events.
- **Baseline** – Find attacks quickly by comparing logs against a known good level of activity.
- **Threat Intelligence** – Don't be satisfied with steady state, always look at what is new and emerging as the threat landscape changes.
- **Intelligent Monitoring** – Use the information available to continually improve your monitoring tools and procedures to help detect and prevent attacks.

ITAC 2015

IT AUDIT & CONTROLS CONFERENCE

THANK YOU!

Kevin W. Lawrence,

Klawrence@BishopFox.com

Please Remember To Fill Out Your Session Evaluation Forms!

MIS|TI TRAINING INSTITUTE