BISHOP FOX

Monitoring Threats and Measuring Risk

MY, WHAT NICE LOGS YOU HAVE…

InformationWeek DARKReading

October 31, 2014

Agenda

WHAT IS THIS ALL ABOUT?

- About Me
- Monitoring
- Threat Intelligence
- Intelligent Monitoring
- Summary
- Questions

About Me

SO JUST 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

SEEING BEHIND THE CURTAIN

Monitoring

INTRODUCTION

What is Monitoring?

- The act of reviewing one or more data sources for information of interest

Why Monitor ?

- To identify suspicious or otherwise unusual event information that may be indicative of malicious activity

Monitoring vs. Logging?

- Logging is the act of collecting data from one or more sources. Monitoring is the act reviewing the logs you collect. Logging is important but monitoring the logs is better.

Monitoring

PLACE TO MONITOR

Source	Logs
Network	• Firewalls • IDS • Routers • Email Gateways
System	• Workstation • Server • Point of Sale
Applications	• IIS/Apache • Anti Virus • VPN

Monitoring

WHAT TO MONITOR

Use Cases

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

THREAT INTELLIGENCE

CHANGING THREATS

Threat Intelligence (TI)

INTRODUCTION

What is TI?

- Knowledge of new or emerging threats based on specific evidence, which may include information to detect or respond effectively

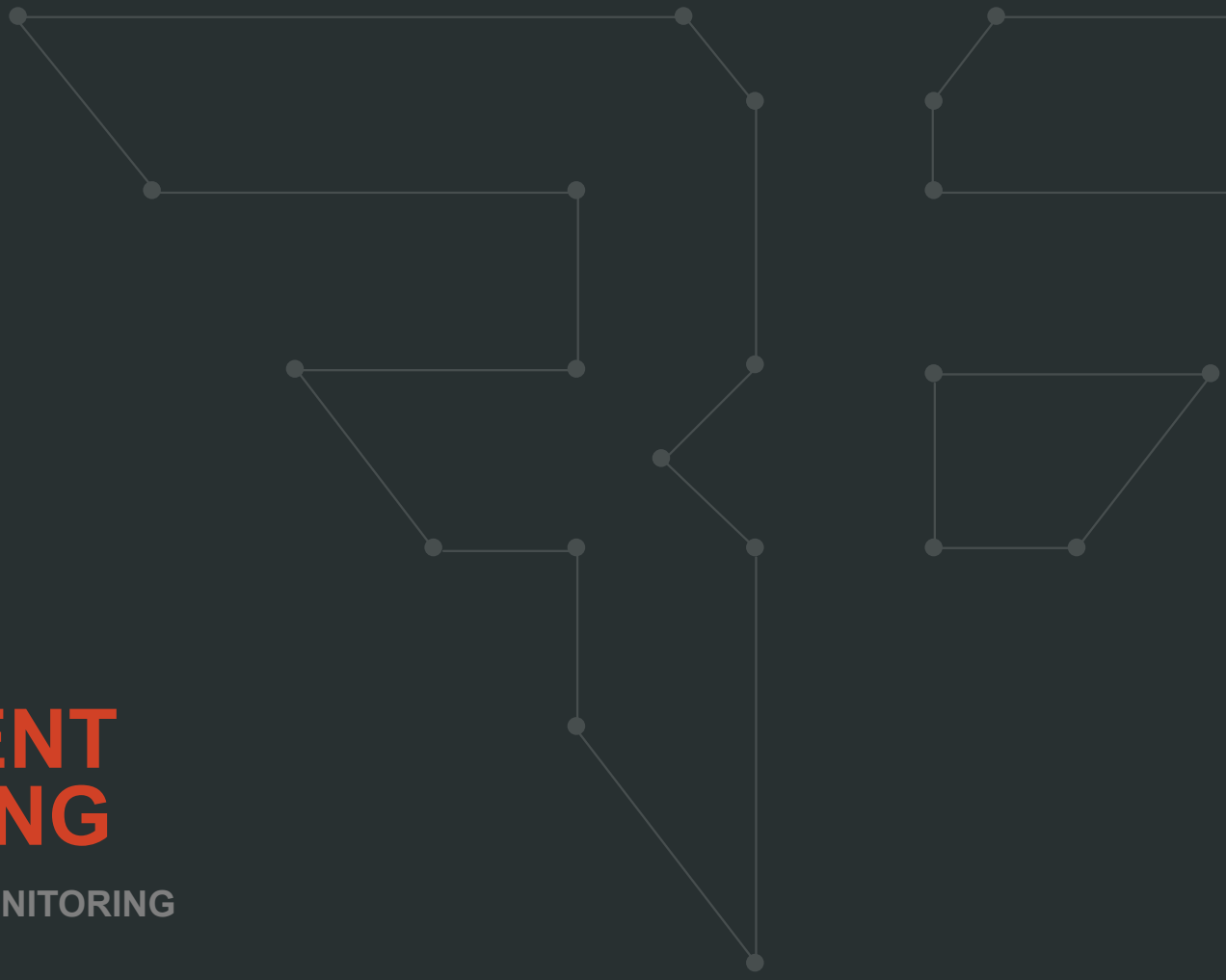
Why keep up?

- To prepare and identify new and emerging attacks that may be focused on a given industry segment or vendor

Monitoring

SOURCE OF 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

COMBINING TI WITH MONITORING

Intelligent Monitoring

INTRODUCTION

What is Intelligent Monitoring

- The act of looking for new and emerging threats in your monitoring solutions
- Using information provided by a threat intelligence source to modify what your focus monitoring tools on

Why use IM

- To identify and detect new and emerging attacks before an attacker successfully breaches your network

Intelligent Monitoring

COMBINING INTELLIGENCE WITH MONITORING

Dynamic Monitoring

- Automatic monitoring based on information from a threat intelligence source

Preventative Detections

- Blocking or patching, vulnerability systems and tools based upon information and recommendations form threat intelligence sources

Information Sharing

- Providing additional anonymized information about what detective, preventative, and remediation solutions are working best for you
- Don’t just take the information but share what you have learned.

SUMMARY

WRAP UP

Summary

WRAP UP

Monitoring – Don't just log your data, watch and review it for potential security events.

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.

Thank you

BISHOP FOX®

We’re Hiring

www.bishopfox.com

contact@bishopfox.com

@bishopfox

BISHOP FOX®