Using Security Intelligence To Mitigate Today’s Real Threats

Ken Westin
Tripwire Inc.
Product Marketing Manager
kwestin@tripwire.com
Why Big SIEM Implementations Fail

People + Process + Technology

- Big SIEM” deployments are a massive project, requires management buy-in for the long haul
- Requires a great deal of “care and feeding”
- Long time-to-value
- Lack of out-of-the-box functionality
Walk Before You Run

“Deploy log management functions before you attempt wide-scale implementations of real-time event management”

Dr. Anton Chuvakin
Moving from Log Management to SIEM

People + Process + Technology

• Monitoring process in place and properly staffed
• Ability to respond to alerts
• Tuning and customizing
• Who has access to information, how will reporting requests be handled?
Which systems are vulnerable?
Which systems are being attacked?
Which systems have already been compromised?
Which systems should we fix first?
Have we seen this before?
When was it in a trusted state?
How can we keep this from happening again?
Vulnerable system visits website with active exploit targeting Internet Explorer

1. Vulnerable system visits website with active exploit targeting Internet Explorer

2. Firewall or IDS detects exploit attempt and passes alert to Tripwire Log Center

3. Real-time intelligence of threat: correlation of vulnerabilities, configuration and business context of target system
Log Intelligence

Are we being attacked? Have we seen it before?

Security Configuration

What has changed? What is the trusted state?

Vulnerability Management

What is vulnerable? What is the risk?

HEARTBLEED AND OTHER REMOTE EXPLOITS WITH TRIPWIRE
Learn More

Visit www.tripwire.com

We will be at Black Hat again this year booth #141

Contact Info

Ken Westin
kwestin@tripwire.com
Twitter: @kwestin