Using Security Intelligence To Mitigate Today's Real Threats

Ken Westin
Tripwire Inc.
Product Marketing Manager
kwestin@tripwire.com

y Big SIEM Implementations Fail

e + Process + Technology

g SIEM" deployments are a massive project,
quires management buy-in for the long haul

quires a great deal of "care and feeding"

ng time-to-value

ck of out-of-the-box functionality

lk Before You Run

'Deploy log management functions before you attempt wide-scale implementations of real-time event management"

Dr. Anton Chuvakin

ving from Log Management to SIEM

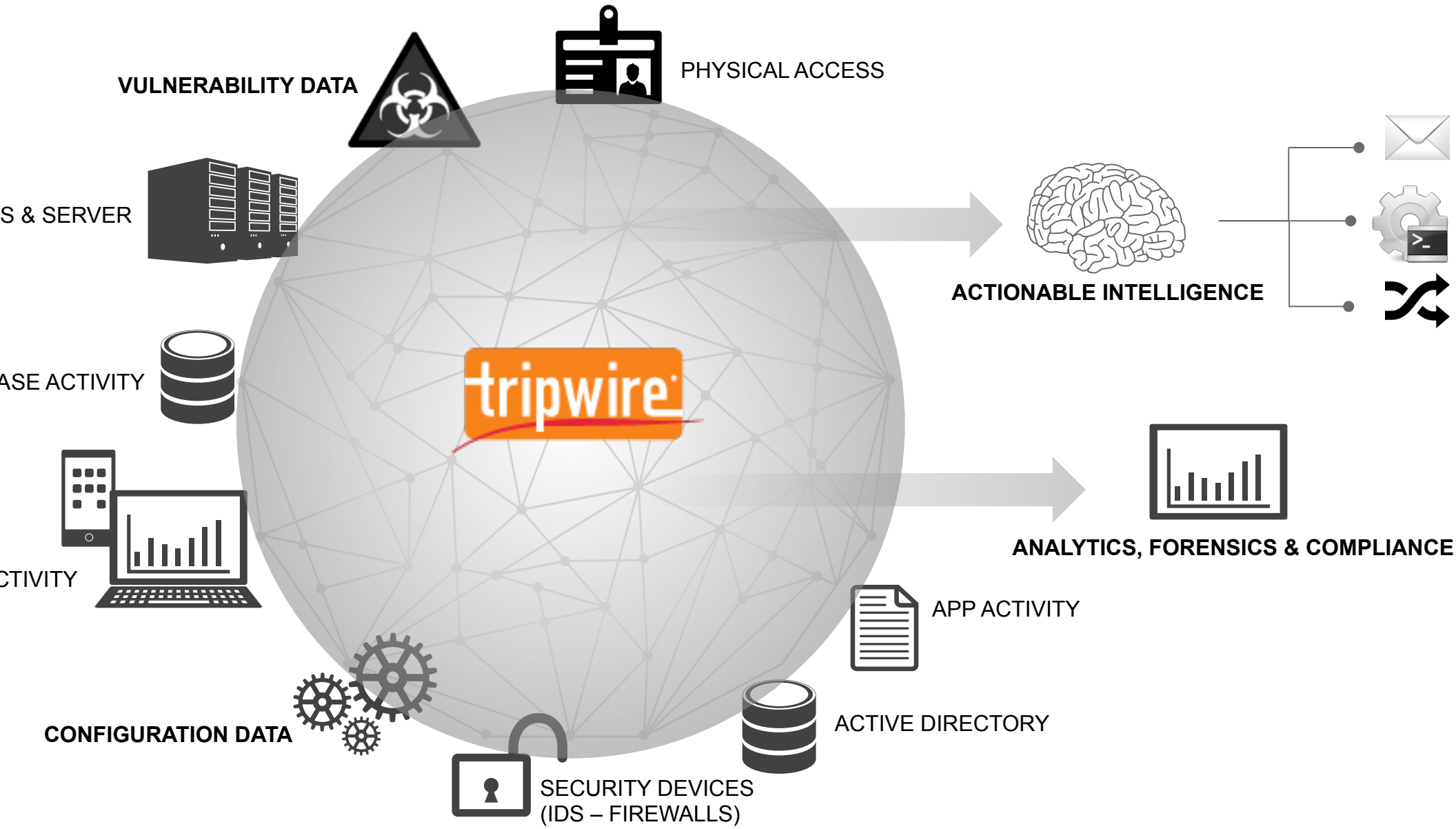
e + Process + Technology

onitoring process in place and properly staffed

bility to respond to alerts

uning and customizing

ho has access to information, how will reporting request
e handled?


VULNERABILITY DATA
PHYSICAL ACCESS
S & SERVER
ASE ACTIVITY
CTIVITY
tripwire
ACTIONABLE INTELLIGENCE
ANALYTICS, FORENSICS & COMPLIANCE
APP ACTIVITY
ACTIVE DIRECTORY
CONFIGURATION DATA
SECURITY DEVICES
(IDS – FIREWALLS)

h systems are vulnerable?

h systems are being attacked?

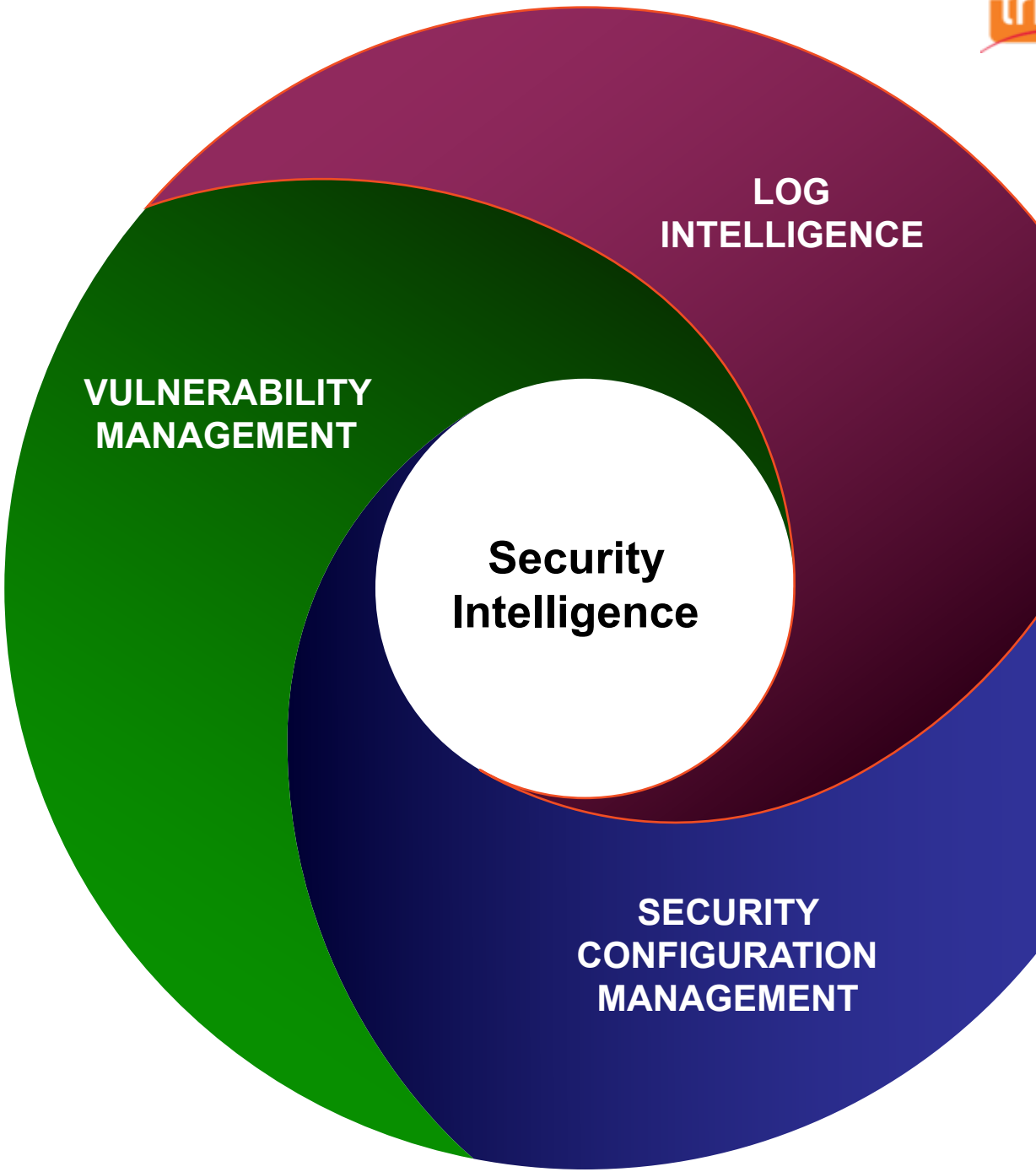
h systems have already been
promised?

h systems should we fix first?

we seen this before?

n was it in a trusted state?

can we keep this from
ening again?

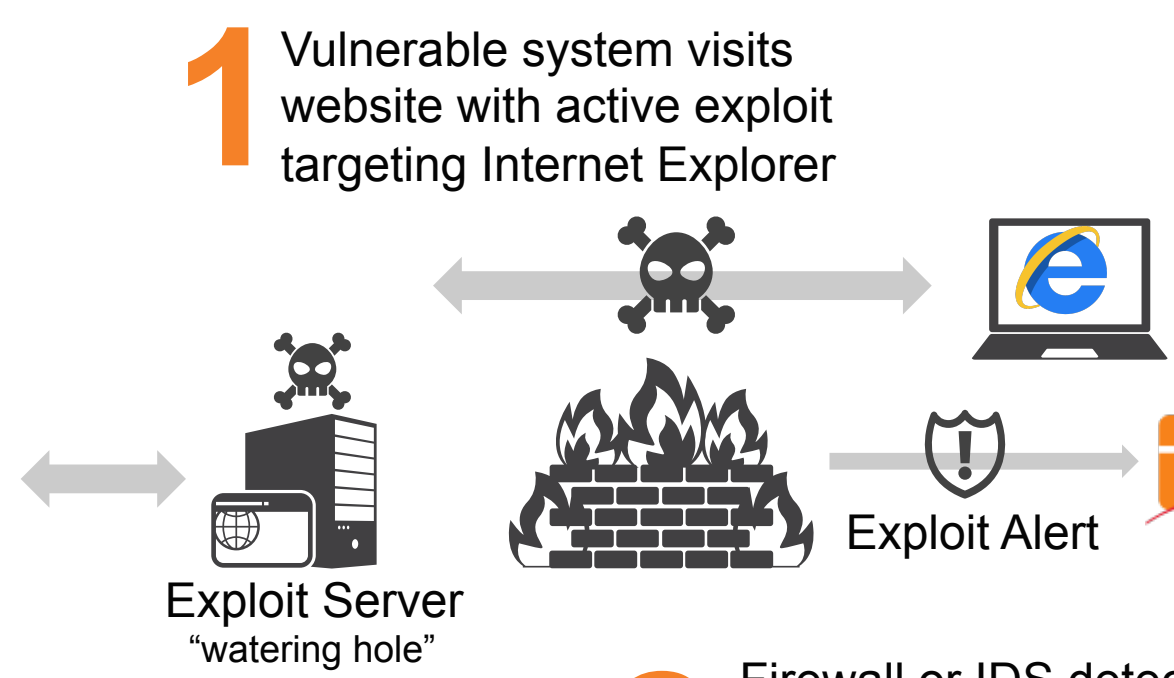


CT & PREVENT IE 0-DAY THREATS WITH TRIPWIRE

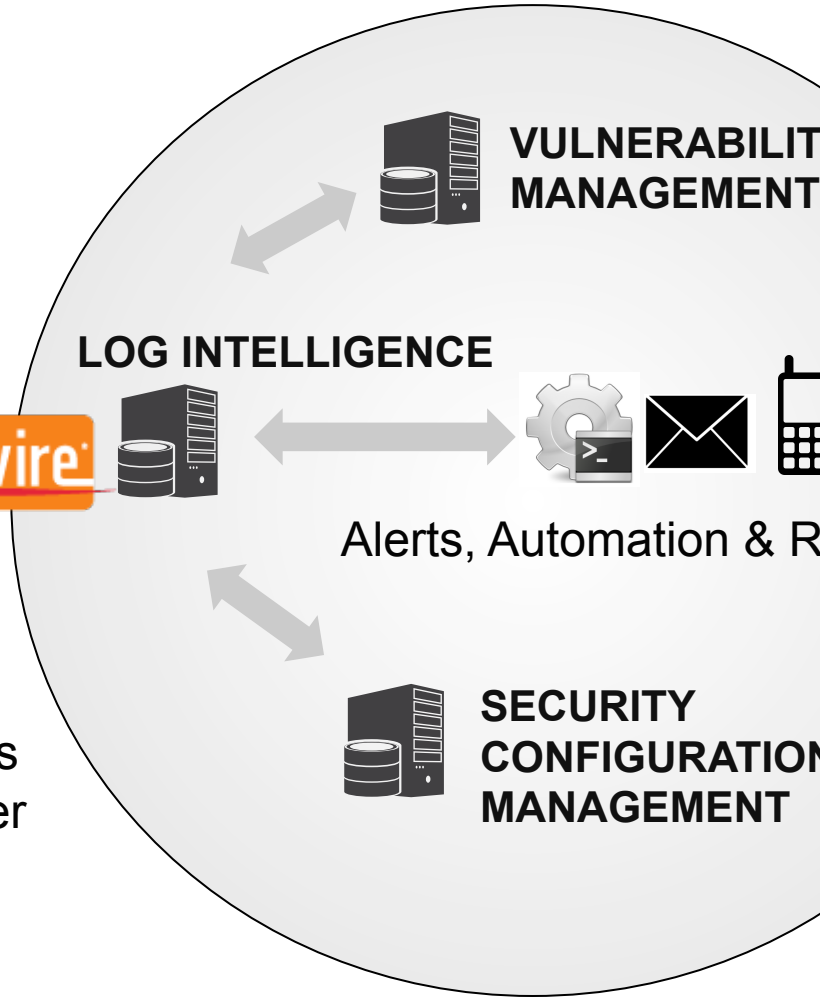
014-1776

3 Real-time intelligence of threat: corre
vulnerabilities, configuration and bus
context of target system

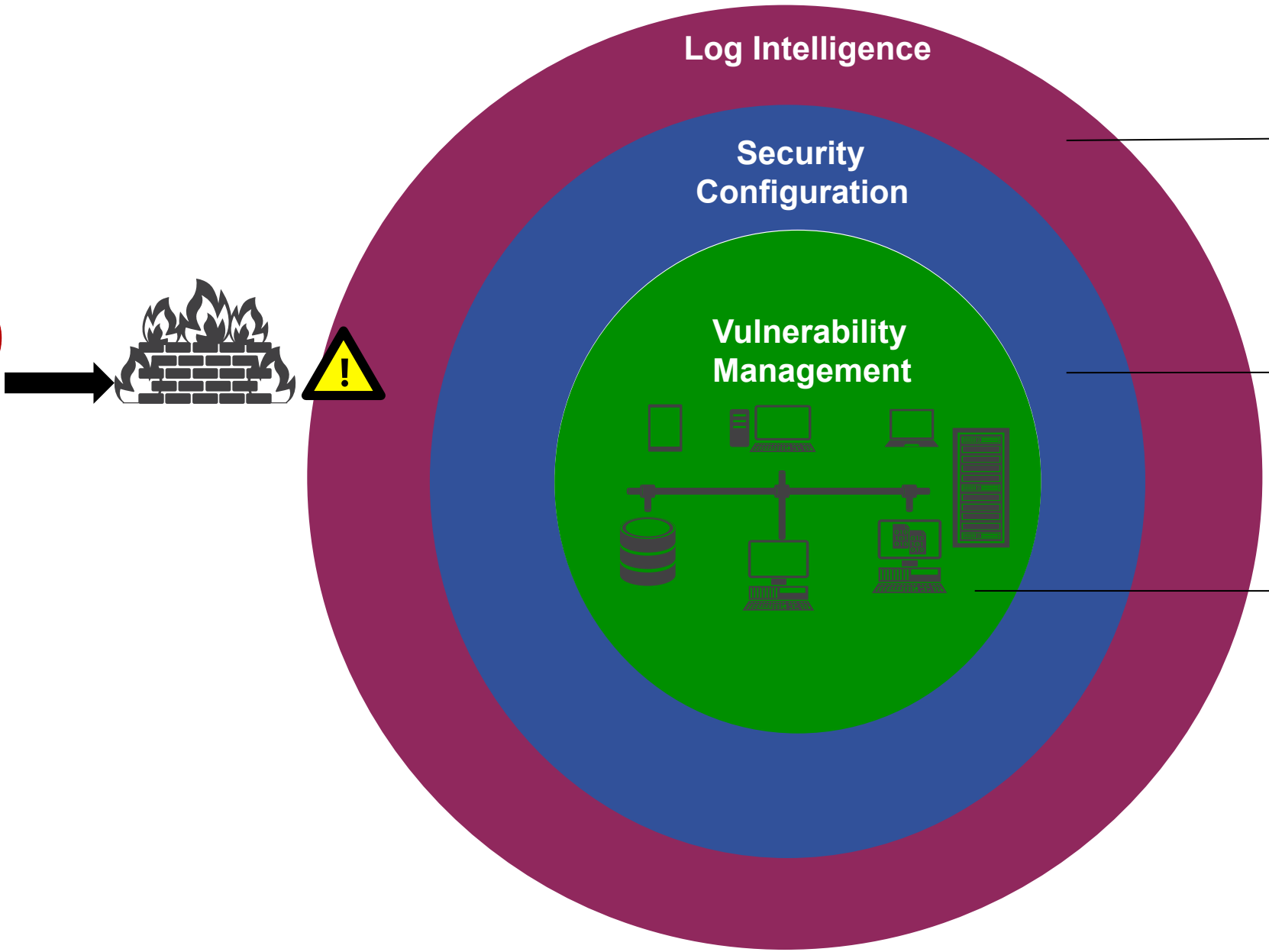
1 Vulnerable system visits
website with active exploit
targeting Internet Explorer



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



TBLEED AND OTHER REMOTE EXPLOITS WITH TRIPWIRE



arn More

sit www.tripwire.com

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

act Info

Westin

tin@tripwire.com

er: @kwestin