itsa 2019
Die IT-Security Messe und Kongress

HACK YOURSELF

FIND IT BEFORE THEY DO

Christian Hirsch
Sr System Engineer, Ixia

September 2019

AGENDA

PART 1. THE NEED FOR SELF-HACKING

PART 2. BREACH AND ATTACK SIMULATION

PART 3. THE NEW IXIA SOLUTION

PART 1

"THE NEED FOR SELF-HACKING"

PREVENTING BREACHES

DIFFICULT AND EXPENSIVE

YOUR NETWORK IS EXPOSED TO THREATS EVERY DAY FROM

- Bad user behavior
- Emerging malware
- Motivated attackers
- Firewall misconfiguration
- “Temporary” policy exceptions
- Insider threats

ixia

KNOWING IF YOUR SECURITY IS ALWAYS WORKING

Increased Complexity

Dynamic Environment

'Alert Fatigue' + Expert Scarcity

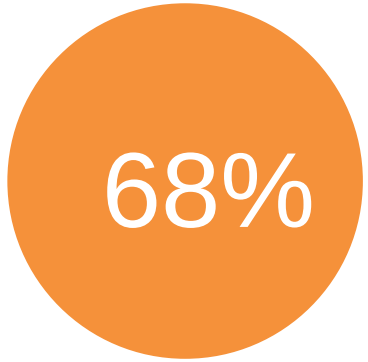
ixia

THE PROBLEM

PREVENTION IS GREAT BUT NOT SUFFICIENT

not 100% effective

A compromise takes minutes or less to execute



[1] breaches remain undetected for months

[1] Source: 2018 Verizon Data Breach Report

ixia

WHAT, OTHER THAN PREVENTION?

DETECTION, VISIBILITY AND NOISE REDUCTION

A key aspect
of your security posture

Visibility

Noise
Reduction

ixia

ITS TIME FOR A CHANGE

YOU HAVE TO TEST…

CONTINOUSLY

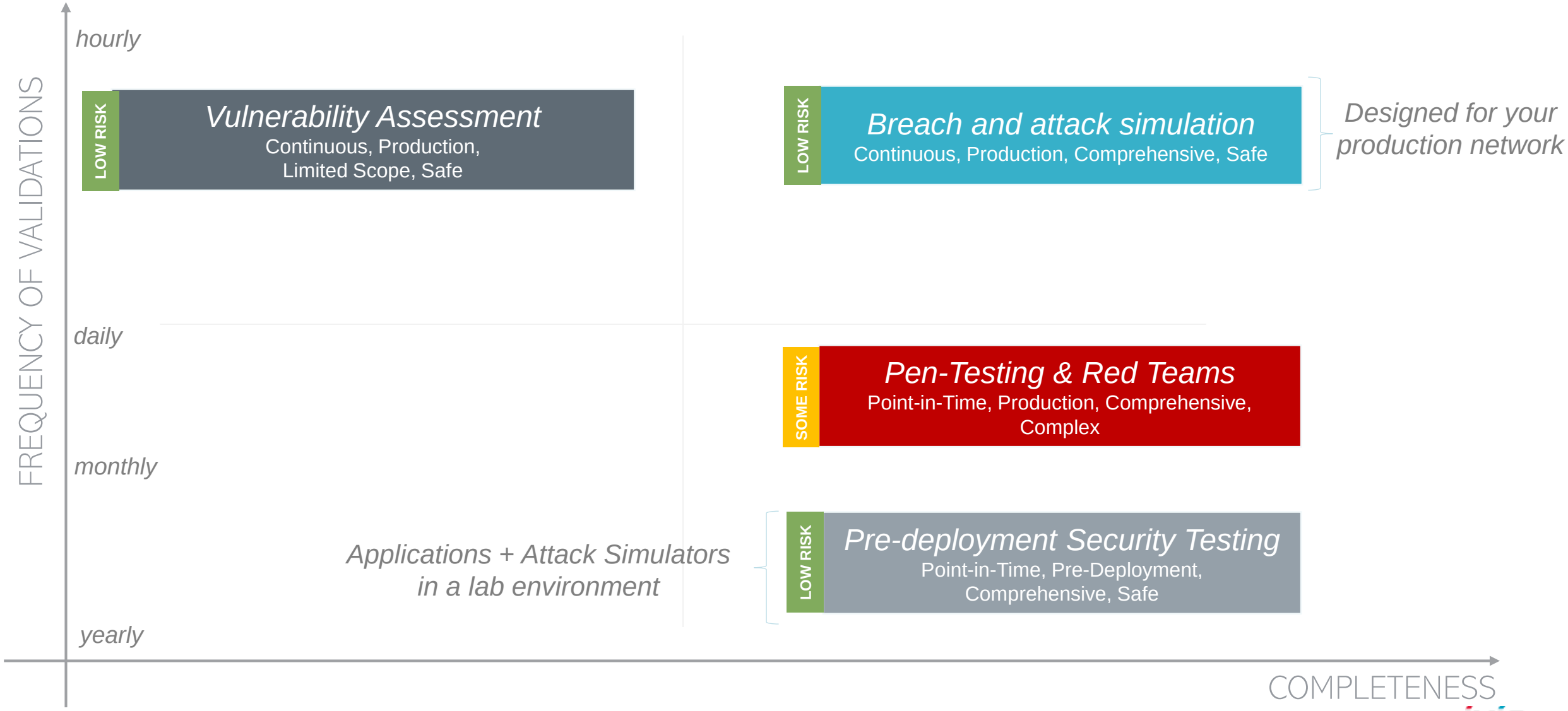
Your Tools

Your People

Your Processes

ixia

Options for Security Validations



ixia

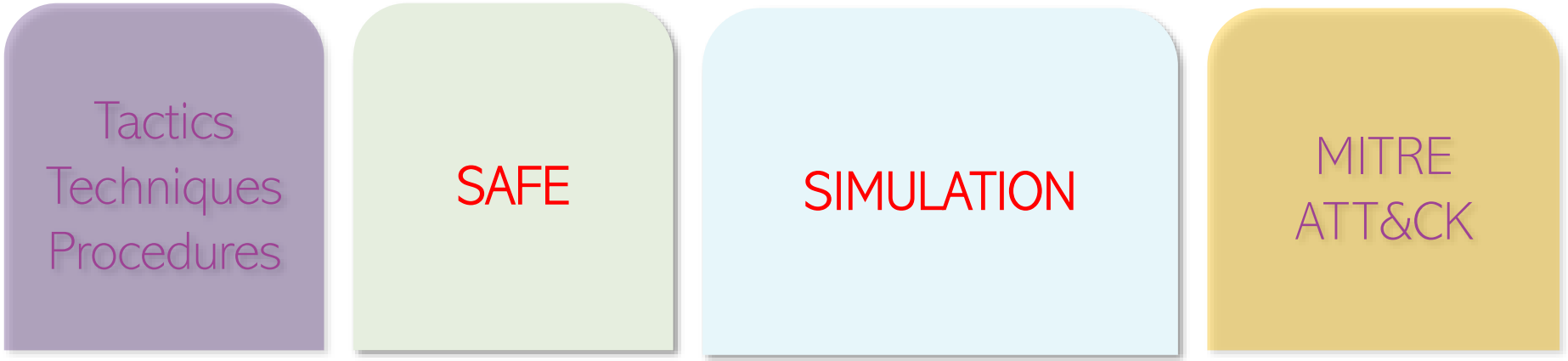
PART 2

"BREACH AND ATTACK SIMULATION"

BREACH AND ATTACK SIMULATION

WHAT IS IT?

> "A TOOL THAT ALLOWS YOU TO SIMULATE ACTIVITIES THAT ARE USED BY HACKERS, SAFELY WITHIN YOUR PRODUCTION NETWORK"



SAFE → *Your production network must not have a negative impact from your testing*

SIMULATION → *Somethings are simulated, some must be real*

ixia

BREACH AND ATTACK SIMULATION

INSIGHT INTO SECURITY

Model
Threat Vectors

Simulate
Security Breaches

Distributed
Modeling

Report
Security Score

ixia

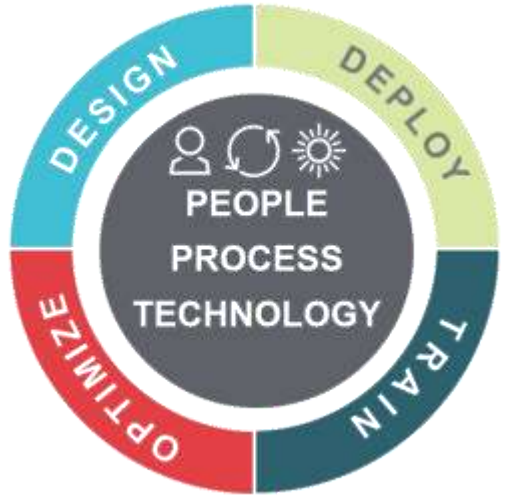
PART 3

"THE NEW IXIA SOLUTION"

ixia Threat Simulator

Breach and Attack Simulation Software

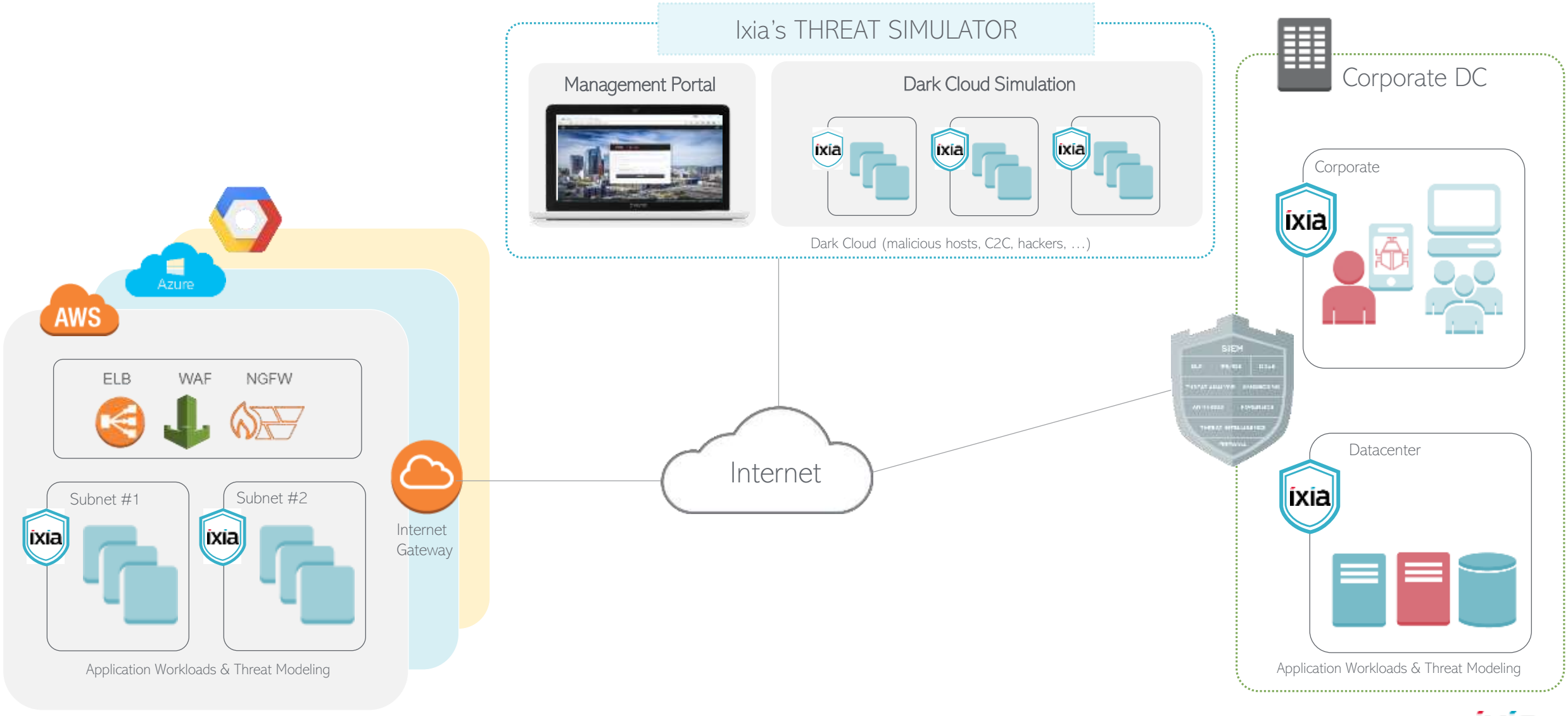
Provides enterprise security teams with **insights** into the effectiveness of their security posture and actionable intelligence to improve it



ixia

IXIA THREAT SIMULATOR

HOW IT WORKS



IXIA THREAT SIMULATOR

WORKFLOW

Minutes away from your first insights

Install Agents

Deploy
one Threat Simulator agent
to each network segment
you need to monitor

Define Agent Groups

Use agent tags
to define dynamic groups
that are representative
for your environment

Validate Security

Run security validations
on-demand or schedule
continuous validations
using one or more agent groups

View Insights

Use the dashboard
to gain insights
into your security risk
and remediation steps

ixia

IXIA THREAT SIMULATOR

SIMULATE ATTACKS ACROSS EACH PHASE OF THE CYBER KILL CHAIN

Objectives		Adversary Tactics, Tools and Procedures
Reconnaissance		Web scanning, LinkedIn
Weaponization		Malicious Adobe PDF documents
Delivery		Spear Phishing / Watering Hole / Drive-By-Download
Exploitation		SQL injection / Adobe PDF Exploits
Installation		Shylock malware
CnC		Randomly generated .com domains, HTTP & HTTPS
Act on Objectives		Theft of Sensitive Information

Example of adversary tactics, tools and procedures used against financial organizations

THREAT SIMULATOR **AUDITS**

- Vulnerability Scanners & Asset Management tools => context
- Malware + Polymorphism + Files
- Phishing / Drive-by-Download
- Exploits + Evasions + Shellcodes
- Bots + C&C
- Data Exfiltration (SSN, CC, …)

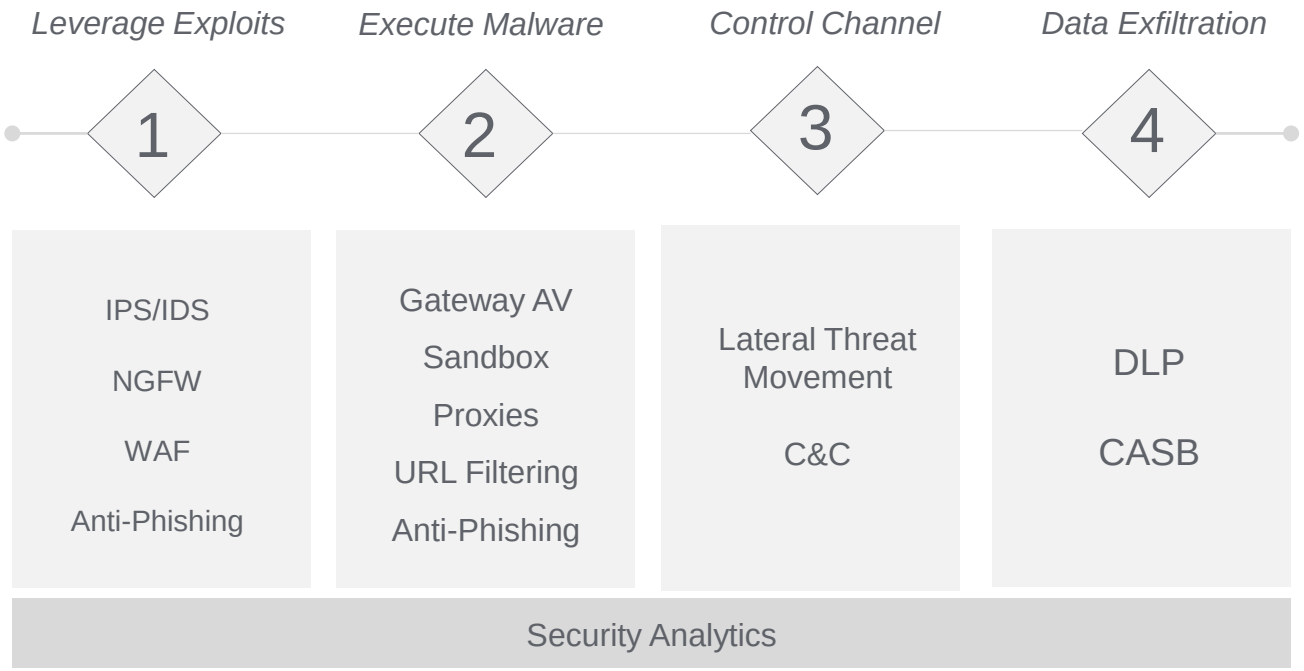
ixia

Use Case #1

Continuous validation of your Enterprise-wide security infrastructure

Always know if your security investments are making an impact.

- Proofs that security controls are deployed and configured correctly
- Provides security assurance that they stay the same
- Active validation of all phases of the Attack Life Cycle
- Justify current and future IT spending using insight of your infrastructure

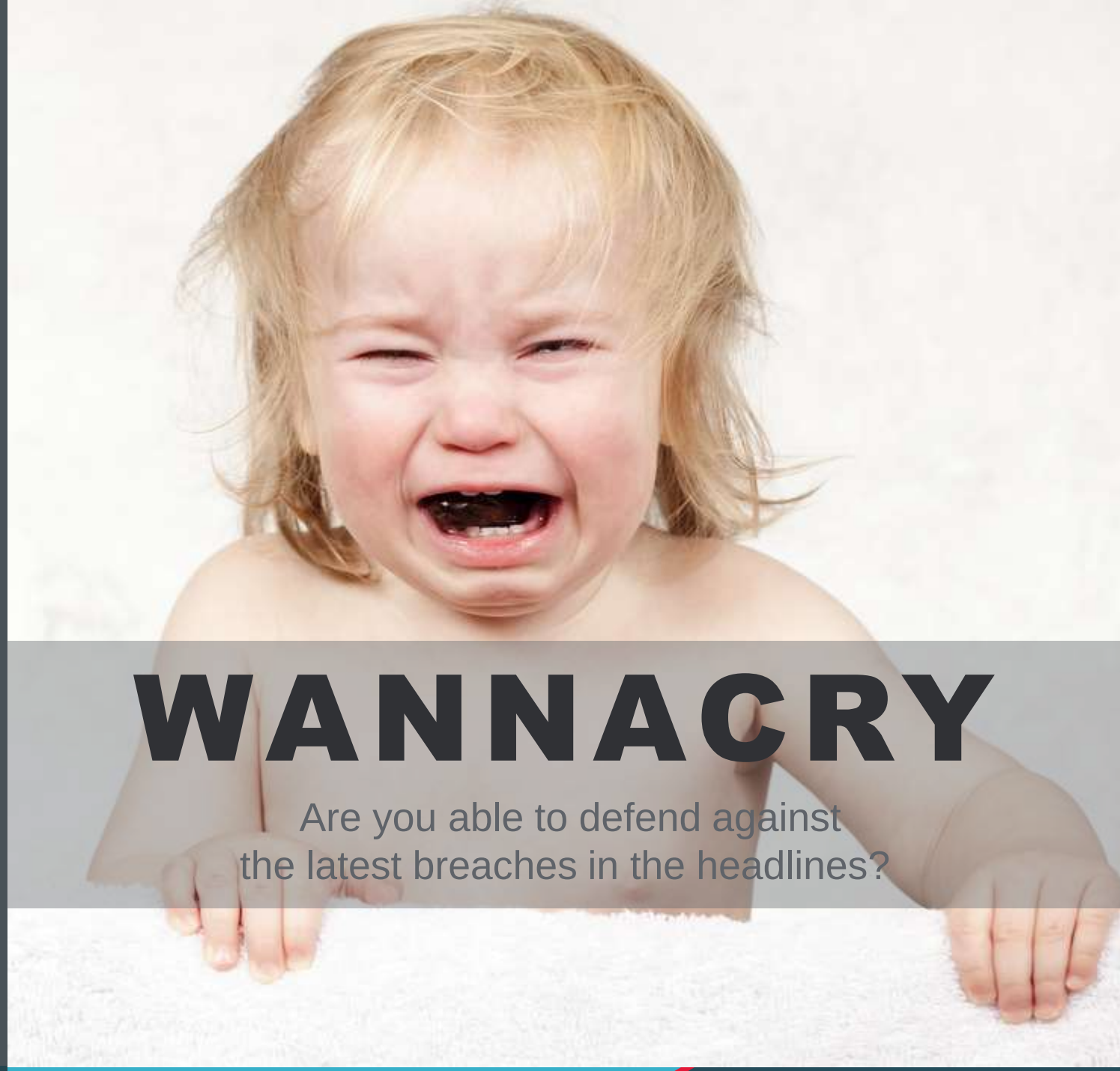


ixia

Use Case #2

Quantify the impact of latest security breaches

Always understand the impact of a new risk **before it happens**



Use Case #3

Security Technology Assessment

Select security designs and solutions based on clear, data-driven insights that tells you how each one performs

- Vendor selection – use of clear, data-driven insights
- Maximize security investments with PoC validation
- Comprehensive assessment of network security solutions

  (NGFW, IPS/IDS, WAF, DLP, GAV, Malware Sandbox, …)
- Justify current and future IT spending
- Insights into how a particular configuration or security

  setup might withstand a cyber-attack

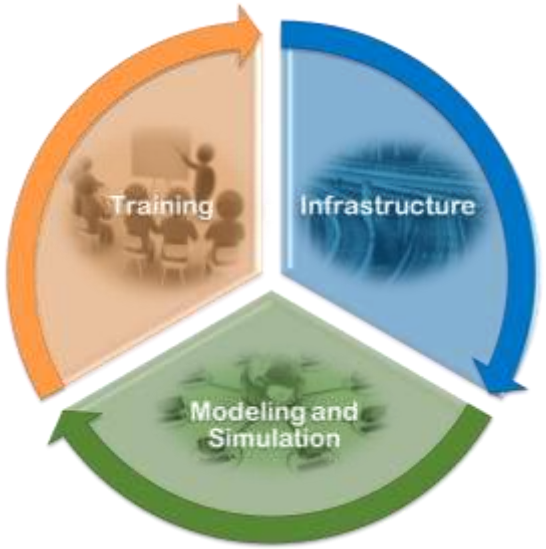
ixia

Use Case #4

Educate Network and Security Stuff

Optimize process and procedures to “detect, react and improve”

- Train SOC team in a realistic hybrid-cloud environment
- Measure personnel performance under realistic attack condition
- Enhance situational awareness for operators
- Optimize process and procedures to detect, react and improve
- Post-Breach Analysis



ixia

IXIA THREAT SIMULATOR

SUMMARY

SAFE

- Always Ixia to Ixia
- Malicious payloads are never executed or downloaded
- Agents deployed in parallel with your hosts
- Agents never contact malicious hosts in the public domain

REALISTIC

- Large and diversified threat simulation library
- Replicates same techniques used in actual attacks

REPEATABLE

- Measurable outcomes with repeatable simulations and results

END-TO-END

- Agents deployed on any infrastructure
- Covers all stages of the attack lifecycle – from infiltration to data exfiltration
- Supports distributed environments

CONTINUOUS

- Schedule assessments to identify deviations from the approved security baseline

ixia

THANK YOU

IN CASE OF QUESTION OR COMMENTS

itsa 2019
Die IT-Security Messe und Kongress

FEEL FREE TO REACH OUT!

Halle 9, Stand 536

Christian Hirsch
Senior System Engineer, Ixia Solutions Group
Keysight Technologies

e: christian.hirsch@keysight.com
m: +49 (0) 170 27 18 090
t: +49 (0) 8051 964 965 1

pgp fingerprint:
A199 A54E F7B3 655E 260A 5DD9 C82A F504 EA6D D9A

ixia