„**NET**working Summ**IT Online“ 16-18 Juni 2020**

HERZLICH WILLKOMMEN! Wir starten in Kürze!

Bitte wählen Sie Ihren Audio-Mode in Ihrem Fenster ganz rechts aus. Wir empfehlen „Mikro + Lautsprecher“ zu verwenden, wenn Sie ein Headset am PC haben.

Falls sie keinen Ton hören, wählen Sie sich bitte per Telefon ein. Die Rufnummern und den Zugangscode entnehmen Sie bitte Ihrem Bildschirm ganz rechts.

NETworking SummIT Online-Agenda

16. Juni 2020

- 10-11 Uhr Riverbed – SaaS Accelerator Schneller Zugriff auf SaaS Anwendungen
- 14-15 Uhr Aternity – der End-User im Fokus

17. Juni 2020

- 10-11 Uhr Zscaler Security as a Service & O365 – mit Hilfe von Zscaler wird das Internet zum sicheren Unternehmensnetzwerk
- 14-15 Uhr A10 Network SSL-Visibility & DDoS-Detection – Sicherheit im Highspeed-Netz

18. Juni 2020

- **10-11 Uhr IXIA Threat Simulator Breach and Attack Defense –Hack yourself before they do!** ⬅
- 14-15 Uhr ExtraHop - Sicherheitslücken mit High Speed Anomalie-Erkennung identifizieren

riverbed Aternity zscaler™ A10 ixia A Keysight Business ExtraHop

A Keysight Business

IXIA Threat Simulator Breach and Attack Defense
Hack yourself before they do!

Präsentation: Andreas Hünten
Senior System Engineer, Ixia Solutions Group
andreas.huenten@keysight.com
0171-8450465

Moderation: Silvija Herdrich
Senior Account Manager dakoServ GmbH
S.Herdrich@dakoServ.de
0174-3042472

GERNE STEHEN WIR IHNEN FÜR EINEN BERATUNGSTERMIN ZUR VERFÜGUNG!

INTRODUCING THREAT SIMULATOR

YOUR BEST DEFENSE IS A GOOD OFFENSE

Keysight Threat Simulator is a Breach and Attack Simulation (**BAS**) product, simulating real attacks in an AUTOMATED, CONTINUOUS and safe manner and PROVIDING REMEDIATION with actionable intelligence.

How Do You Measure Security Posture?

HACK YOURSELF, BEFORE THEY DO

GAPS IN YOUR COVERAGE

Can a certain type of attack get in?

MISCONFIGURATIONS

“Are all my tools working properly?”

OVERLAPPING TOOL COVERAGE

“Am I overspending on redundant tools?”

THREAT REMEDIATION

"How do I fix the gaps in my coverage?"

RISK AND EXPOSURE

“How do I prioritize security fixes?”

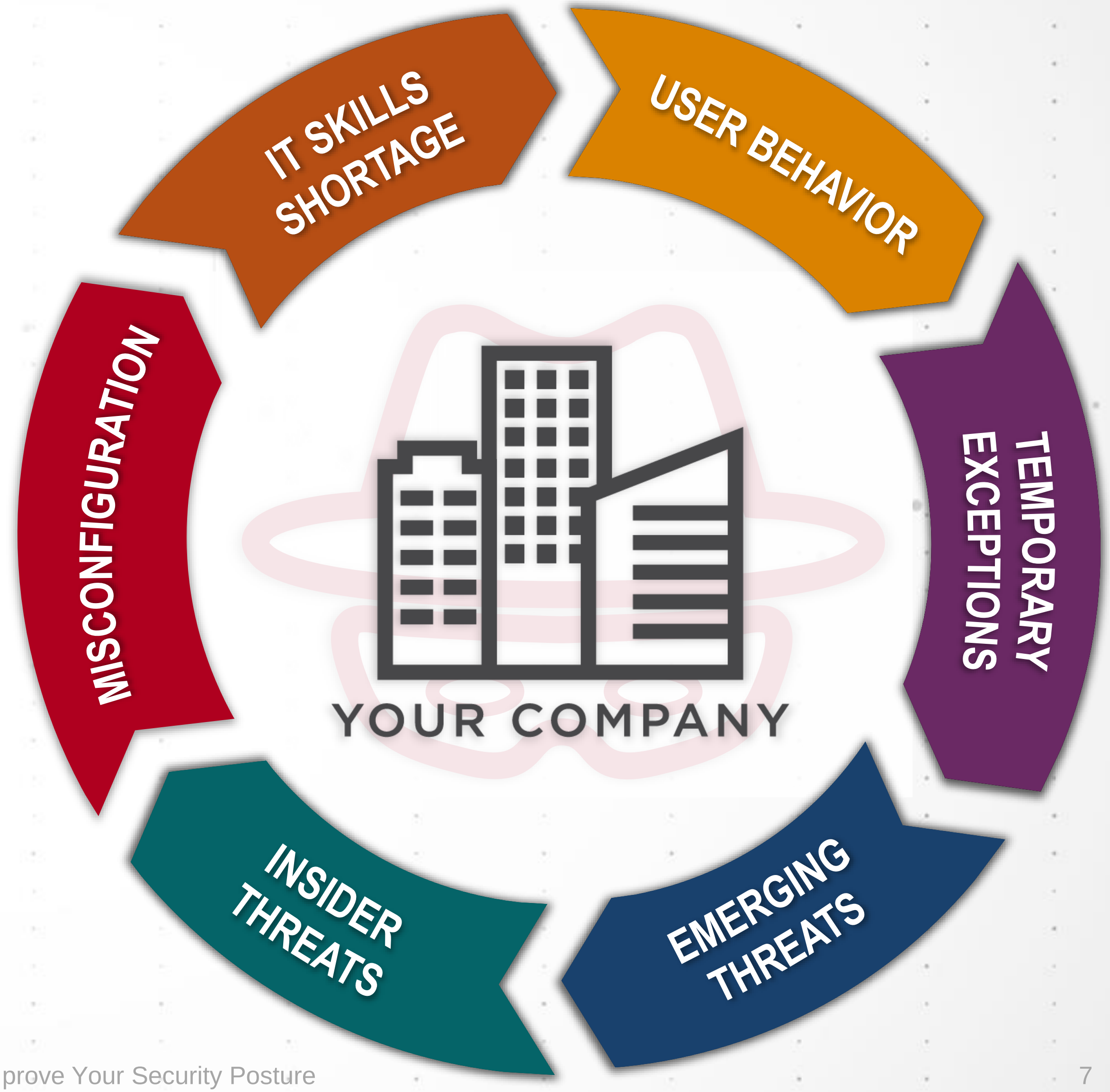
– Security is difficult to measure -

If you can’t measure it,
you can’t improve it !

Preventing Breaches is Challenging

Key Use Cases we want to address:

- Right security tools
- Security tools misconfiguration
- “Temporary” policy exceptions
- IT skills shortage
- Bad user behaviors
- Emerging Threats (Malware)
- Insider threats



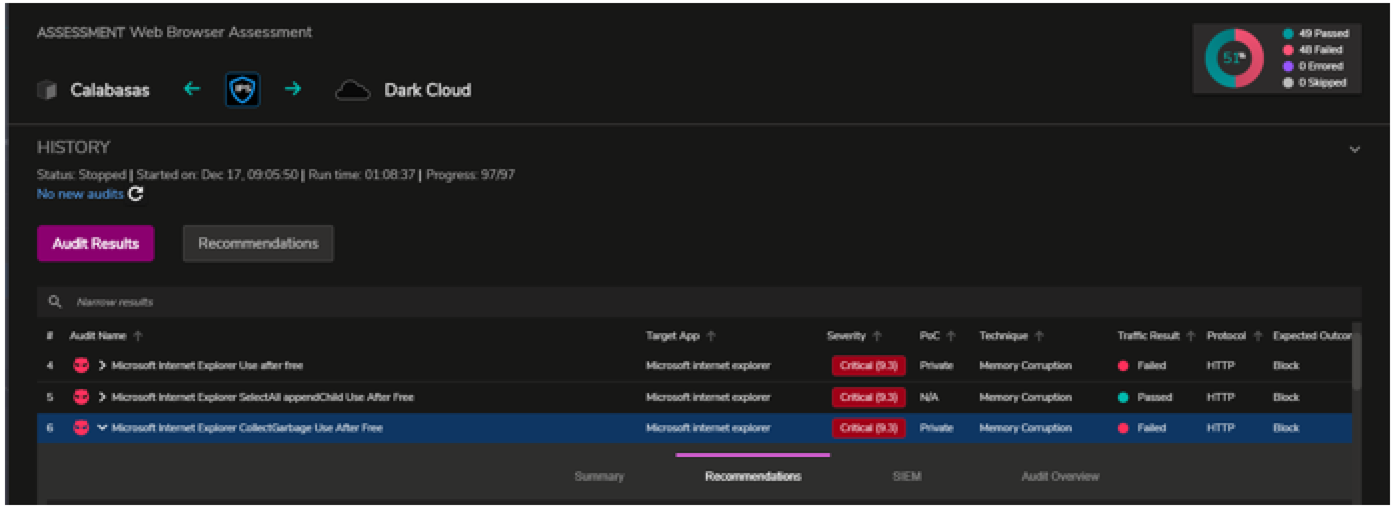
Misconfiguration + Security Updates

FIREWALL/IPS

Opportunity

Immediate Security Remediation; Proof of Effectiveness

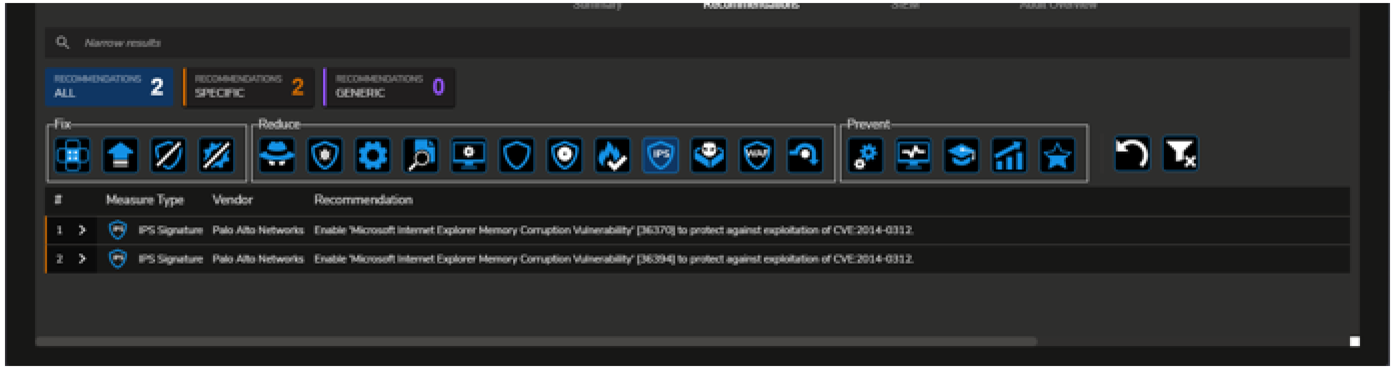
- Threat Simulator Kill Chain Assessment shows NGFW is allowing a Internet Explorer Memory Corruption attack to pass through; internal systems would be vulnerable
- Threat Simulator not only identifies the CVE of the attack, but tells you exactly how to remediate that vulnerability on your NGFW, in this a Palo Alto Firewall



Status: Stopped | Started on: Dec 17, 09:05:50 | Run time: 01:08:37 | Progress: 97/97

No new audits

#	Audit Name	Target App	Severity	PoC	Technique	Traffic Result	Protocol	Expected Outcor
4	Microsoft Internet Explorer Use after free	Microsoft internet explorer	Critical (9.3)	Private	Memory Corruption	● Failed	HTTP	Block
5	Microsoft Internet Explorer SelectAll appendChild Use After Free	Microsoft internet explorer	Critical (9.3)	N/A	Memory Corruption	● Passed	HTTP	Block
6	Microsoft Internet Explorer CollectGarbage Use After Free	Microsoft internet explorer	Critical (9.3)	Private	Memory Corruption	● Failed	HTTP	Block



#		Measure Type	Vendor	Recommendation
1	>	IPS Signature	Palo Alto Networks	Enable 'Microsoft Internet Explorer Memory Corruption Vulnerability' [36370] to protect against exploitation of CVE-2014-0312.
2	>	IPS Signature	Palo Alto Networks	Enable 'Microsoft Internet Explorer Memory Corruption Vulnerability' [36394] to protect against exploitation of CVE-2014-0312.

KEYSIGHT TECHNOLOGIES

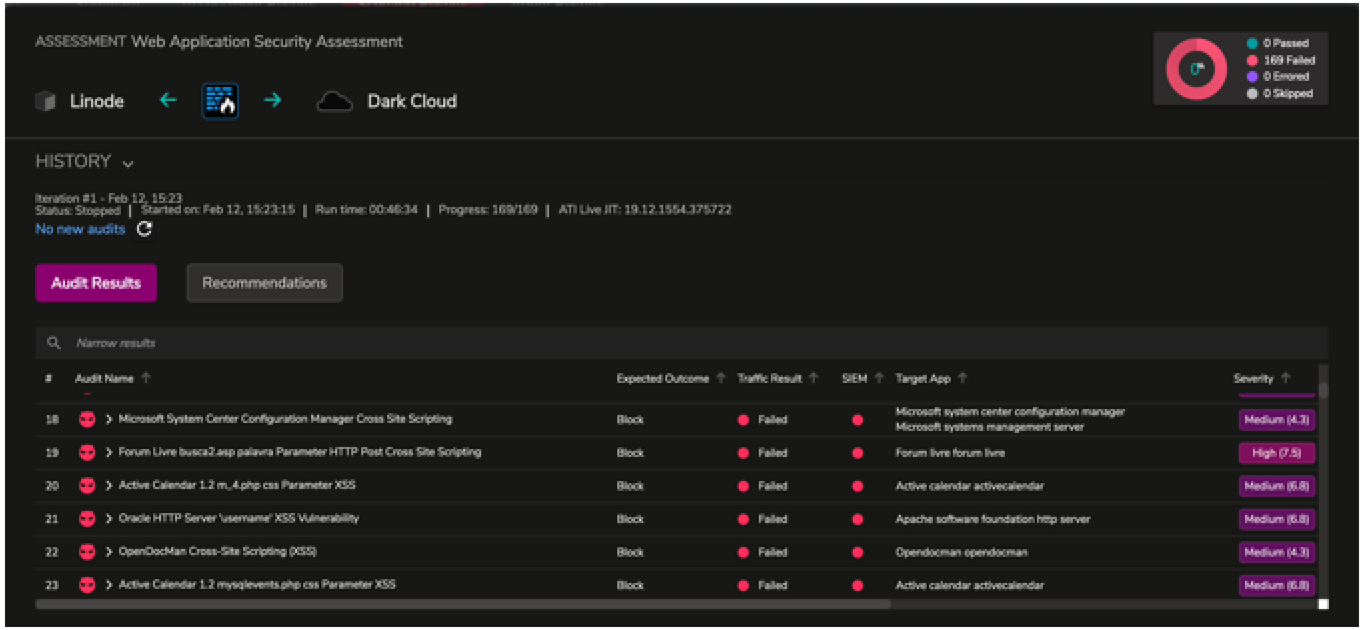
Misconfiguration + Policy Exceptions

WEB APP SECURITY

Opportunity

Remediation services of misconfigurations and updated policy exception.

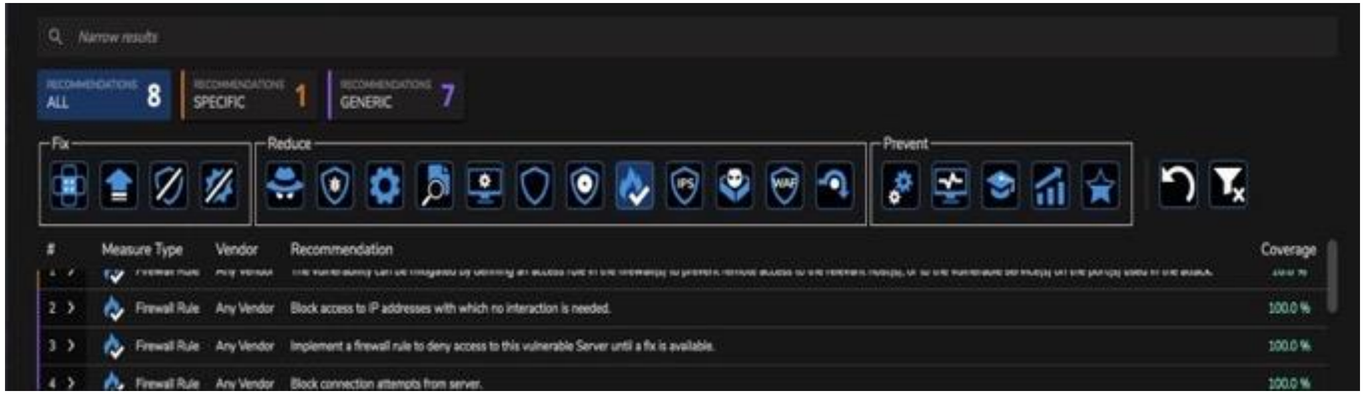
- Sometimes there's not a simple product fix; Threat Simulator gives you information about the threat and best practices to remediate it
- Threat Simulator provides specific, tailored steps to fix common misconfigurations
- Also shows topology-specific steps to change settings and gain additional protection for web applications



ASSESSMENT Web Application Security Assessment

Iteration #1 - Feb 12, 15:23
Status: Stopped | Started on: Feb 12, 15:23:15 | Run time: 00:46:34 | Progress: 169/169 | ATI Live JIT: 19.12.1554.375722
No new audits

#	Audit Name	Expected Outcome	Traffic Result	SIEM	Target App	Severity
18	Microsoft System Center Configuration Manager Cross Site Scripting	Block	● Failed	●	Microsoft system center configuration manager Microsoft systems management server	Medium (4.3)
19	Forum Livre busca2.asp palavra Parameter HTTP Post Cross Site Scripting	Block	● Failed	●	Forum livre forum livre	High (7.5)
20	Active Calendar 1.2 m_4.php css Parameter XSS	Block	● Failed	●	Active calendar activecalendar	Medium (6.8)
21	Oracle HTTP Server 'username' XSS Vulnerability	Block	● Failed	●	Apache software foundation http server	Medium (6.8)
22	OpenDocMan Cross-Site Scripting (XSS)	Block	● Failed	●	Opendocman opendocman	Medium (4.3)
23	Active Calendar 1.2 mysqlevents.php css Parameter XSS	Block	● Failed	●	Active calendar activecalendar	Medium (6.8)



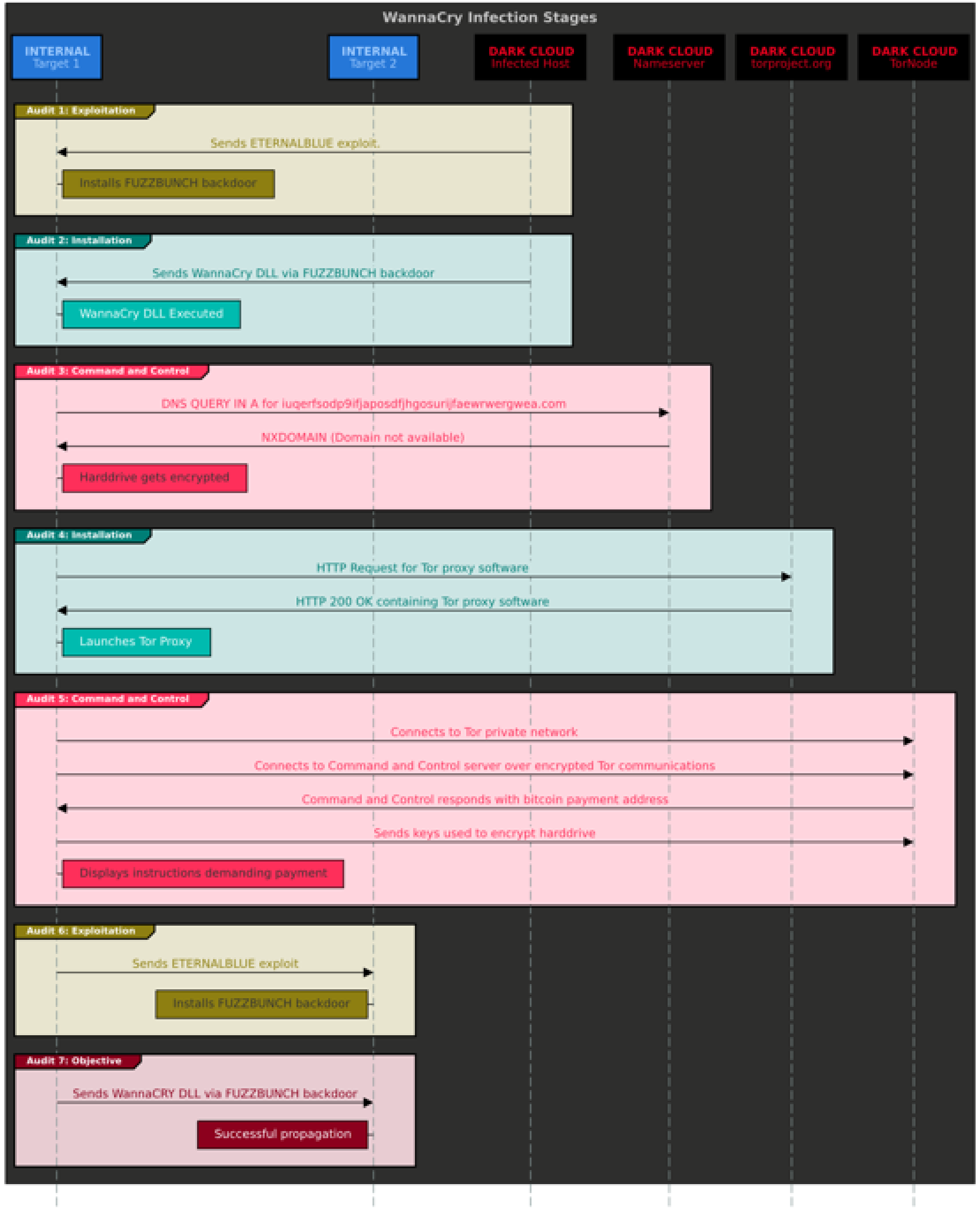
#	Measure Type	Vendor	Recommendation	Coverage
1	Firewall Rule	Any Vendor	The vulnerability can be mitigated by defining an access rule in the firewall(s) to prevent remote access to the relevant host(s), or to the vulnerable service(s) on the port(s) used in the attack.	100.0 %
2	Firewall Rule	Any Vendor	Block access to IP addresses with which no interaction is needed.	100.0 %
3	Firewall Rule	Any Vendor	Implement a firewall rule to deny access to this vulnerable Server until a fix is available.	100.0 %
4	Firewall Rule	Any Vendor	Block connection attempts from server.	100.0 %

Malware Detection

CAN YOU CATCH THE LATEST THREATS?

Opportunity
Security operations strategy;
Managed detection services;
Additional detection solutions.

- Run 'Kill Chain Security Assessment’
  - Simulates WannaCry, Mirai, etc.
  - Includes entire kill chain, including exploitation, installation, command & control, and propagation
- Threat Simulator summarizes exactly what happened at every step in the Kill Chain, including how to remediate any gaps



WannaCry Infection Stages

INTERNAL Target 1
INTERNAL Target 2
DARK CLOUD Infected Host
DARK CLOUD Nameserver
DARK CLOUD torproject.org
DARK CLOUD TorNode

Audit 1: Exploitation
Sends ETERNALBLUE exploit.
Installs FUZZBUNCH backdoor

Audit 2: Installation
Sends WannaCry DLL via FUZZBUNCH backdoor
WannaCry DLL Executed

Audit 3: Command and Control
DNS QUERY IN A for iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
NXDOMAIN (Domain not available)
Harddrive gets encrypted

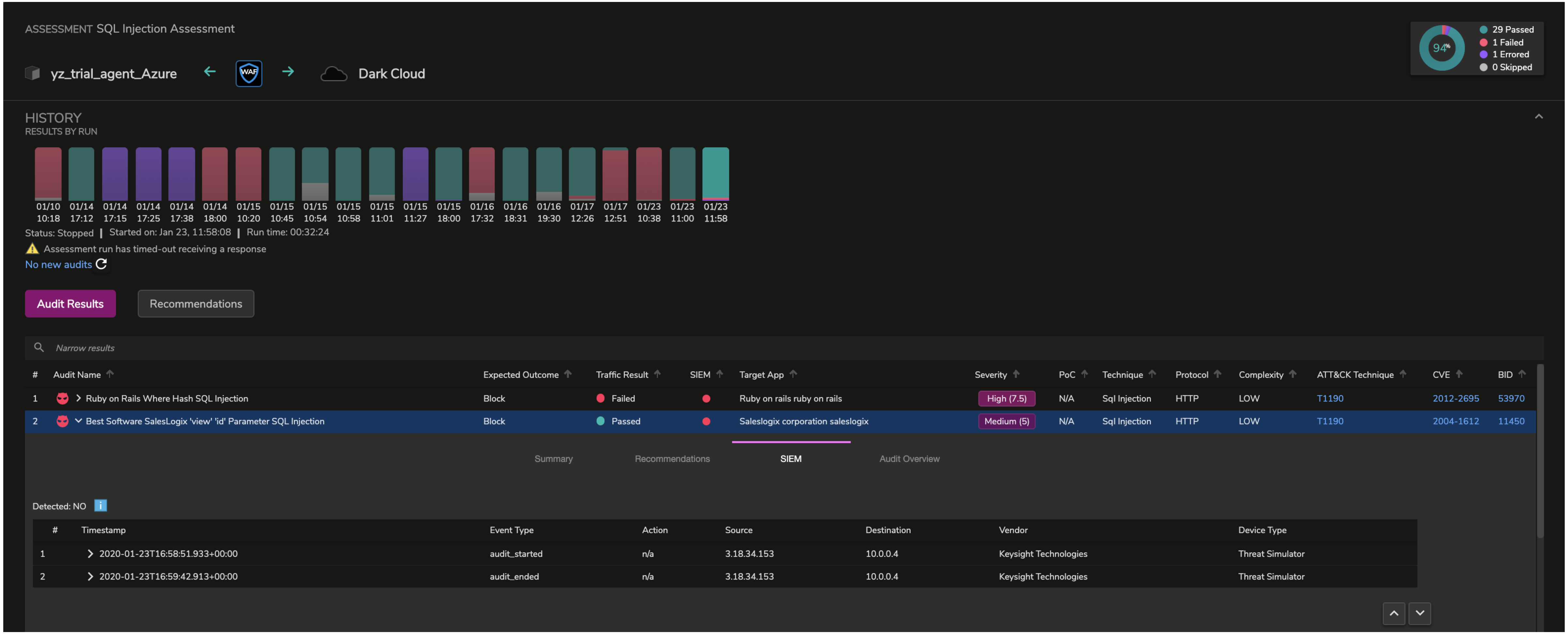
Audit 4: Installation
HTTP Request for Tor proxy software
HTTP 200 OK containing Tor proxy software
Launches Tor Proxy

Audit 5: Command and Control
Connects to Tor private network
Connects to Command and Control server over encrypted Tor communications
Command and Control responds with bitcoin payment address
Sends keys used to encrypt harddrive
Displays instructions demanding payment

Audit 6: Exploitation
Sends ETERNALBLUE exploit
Installs FUZZBUNCH backdoor

Audit 7: Objective
Sends WannaCRY DLL via FUZZBUNCH backdoor
Successful propagation

SIEM Integration



ASSESSMENT SQL Injection Assessment

yz_trial_agent_Azure ← WAF → Dark Cloud

94%

- ● 29 Passed
- ● 1 Failed
- ● 1 Errored
- ● 0 Skipped

HISTORY
RESULTS BY RUN

Status: Stopped | Started on: Jan 23, 11:58:08 | Run time: 00:32:24

⚠ Assessment run has timed-out receiving a response

No new audits

Audit Results | Recommendations

Narrow results

#	Audit Name	Expected Outcome	Traffic Result	SIEM	Target App	Severity	PoC	Technique	Protocol	Complexity	ATT&CK Technique	CVE	BID
1	> Ruby on Rails Where Hash SQL Injection	Block	● Failed	●	Ruby on rails ruby on rails	High (7.5)	N/A	Sql Injection	HTTP	LOW	T1190	2012-2695	53970
2	⌄ Best Software SalesLogix 'view' 'id' Parameter SQL Injection	Block	● Passed	●	Saleslogix corporation saleslogix	Medium (5)	N/A	Sql Injection	HTTP	LOW	T1190	2004-1612	11450

Summary | Recommendations | SIEM | Audit Overview

Detected: NO

#	Timestamp	Event Type	Action	Source	Destination	Vendor	Device Type
1	> 2020-01-23T16:58:51.933+00:00	audit_started	n/a	3.18.34.153	10.0.0.4	Keysight Technologies	Threat Simulator
2	> 2020-01-23T16:59:42.913+00:00	audit_ended	n/a	3.18.34.153	10.0.0.4	Keysight Technologies	Threat Simulator

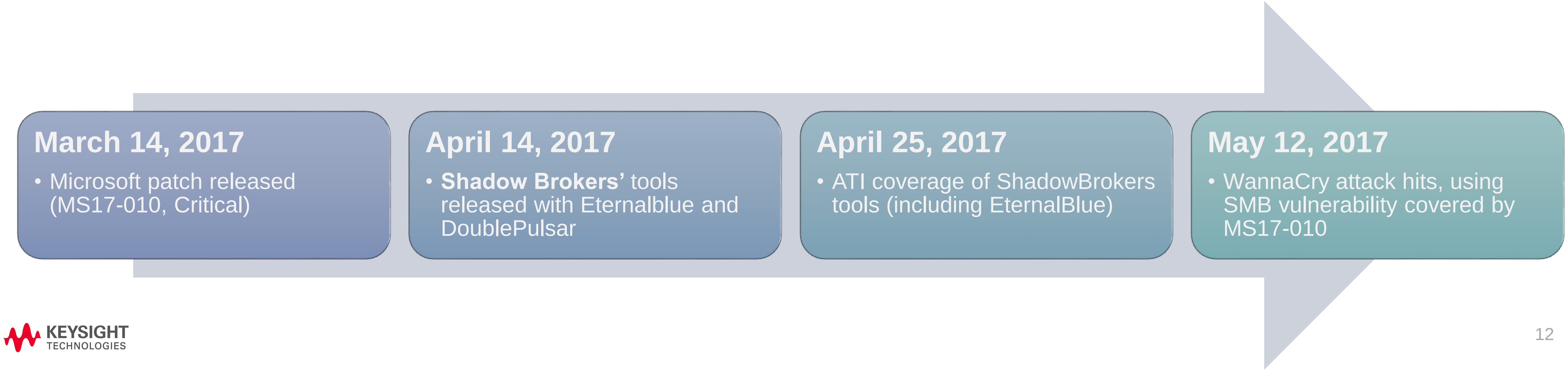
Keysight Threat Intelligence

STAY AHEAD OF ATTACKERS WITH INDUSTRY-LEADING INTELLIGENCE

Global Team of Security Researchers and Application Protocol Engineers

- 15+ years of security intelligence, research, and application protocol development.
- Manage a continuously-updated database, cataloguing millions of known and emerging threats
- Trusted partner of top NEMs, service providers, governments, and enterprises.

REAL-WORLD: Keysight Security Intel team release WannaCry audit 17days before the attack!



March 14, 2017
- Microsoft patch released (MS17-010, Critical)

April 14, 2017
- **Shadow Brokers'** tools released with Eternalblue and DoublePulsar

April 25, 2017
- ATI coverage of ShadowBrokers tools (including EternalBlue)

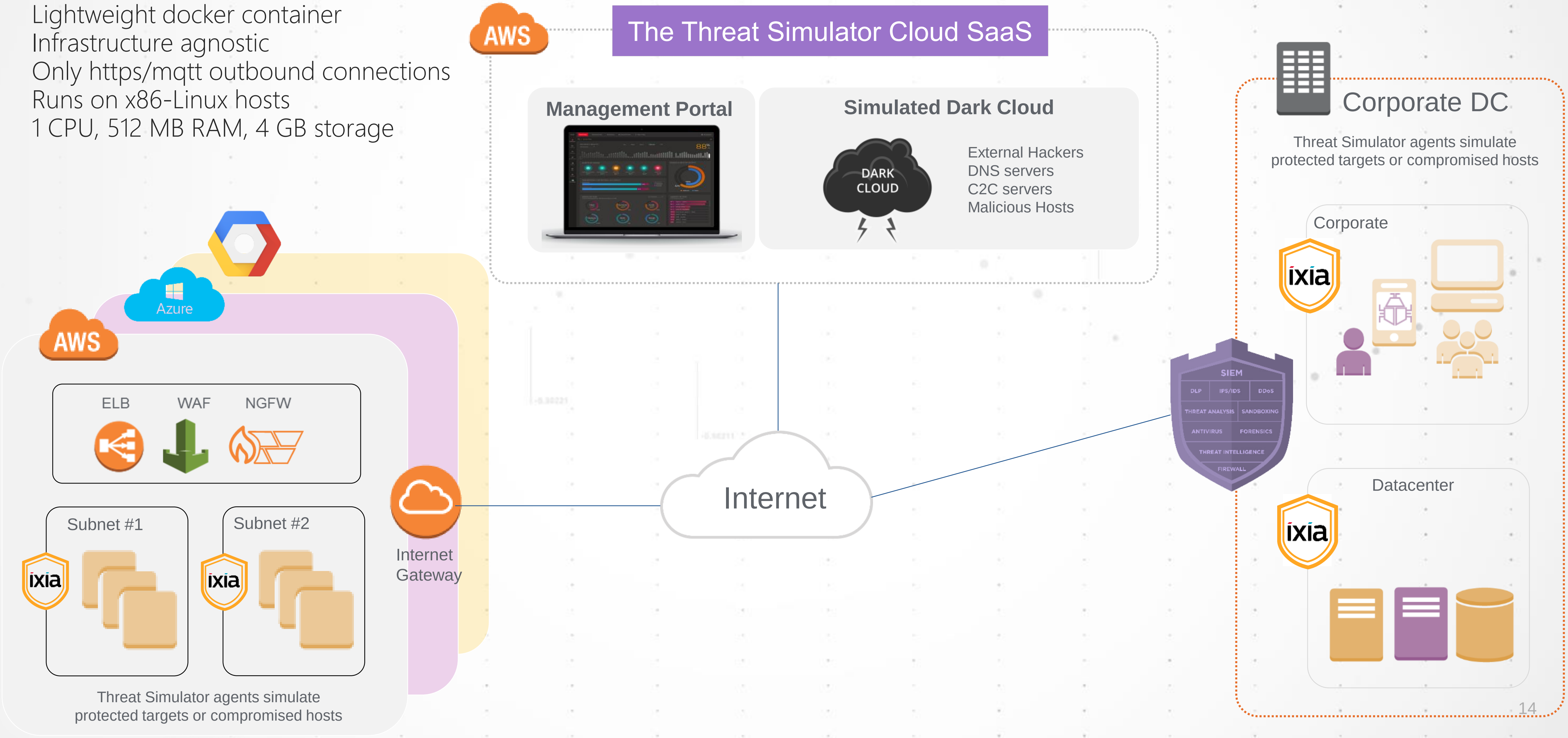
May 12, 2017
- WannaCry attack hits, using SMB vulnerability covered by MS17-010

Threat Simulator Overview

THREAT SIMULATOR'S ARCHITECTURE

Agent Architecture

Lightweight docker container
Infrastructure agnostic
Only https/mqtt outbound connections
Runs on x86-Linux hosts
1 CPU, 512 MB RAM, 4 GB storage



INSTRUMENTATION AND POLICY ASSESSMENTS

Web Application Security

-- Cross Site Scripting
-- SQL Injection
-- Remote File Inclusion
-- Local File Inclusion
-- Server Side Script Injection
-- OS Command Injection
-- Reflected XSS Efficiency
-- Stored XSS Efficiency
-- SQL Injection Efficiency

LAN Perimeter

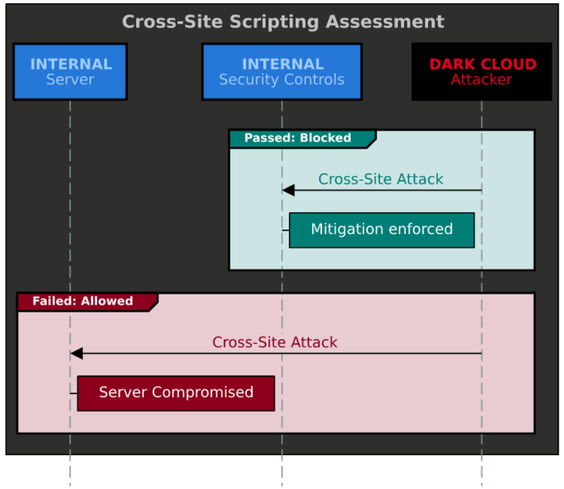
-- web browser vulnerabilities
-- file format vulnerabilities
-- malware file transfer
-- command and control

Data Exfiltration

-- PII Exfiltration via DNS Tunneling
-- PII Exfiltration via HTTP POST
-- PII Exfiltration via Pastebin
-- PII Exfiltration via SMTP
-- PII Exfiltration via WebDAV
-- PII Exfiltration via Dropbox
-- PII Exfiltration via Twitter

URL FILTERING

-- Entertainment
-- Social Networking
-- Streaming Media
-- Hacking
-- Gambling
-- Games
-- Pornography
-- Proxy Avoidance
-- Religion
-- Shopping
-- Weapons



Cross-Site Scripting Assessment

INTERNAL Server

INTERNAL Security Controls

DARK CLOUD Attacker

Passed: Blocked

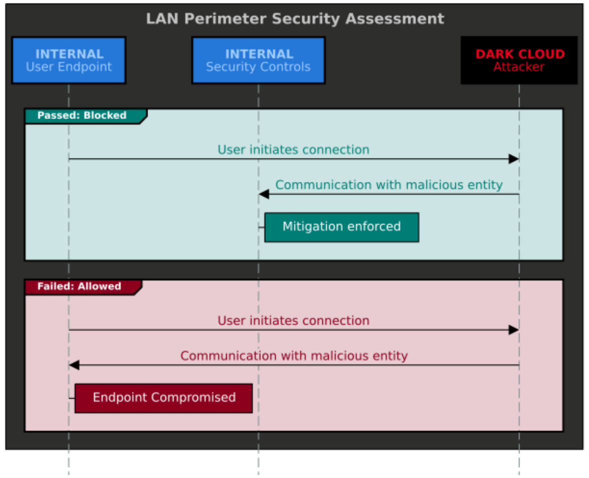
Cross-Site Attack

Mitigation enforced

Failed: Allowed

Cross-Site Attack

Server Compromised



LAN Perimeter Security Assessment

INTERNAL User Endpoint

INTERNAL Security Controls

DARK CLOUD Attacker

Passed: Blocked

User initiates connection

Communication with malicious entity

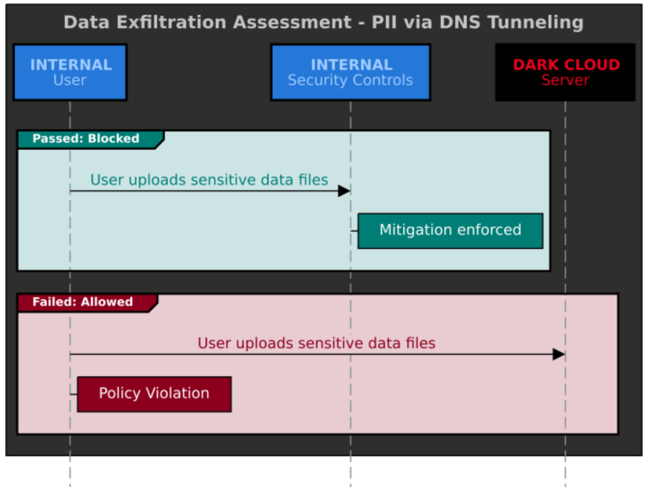
Mitigation enforced

Failed: Allowed

User initiates connection

Communication with malicious entity

Endpoint Compromised



Data Exfiltration Assessment - PII via DNS Tunneling

INTERNAL User

INTERNAL Security Controls

DARK CLOUD Server

Passed: Blocked

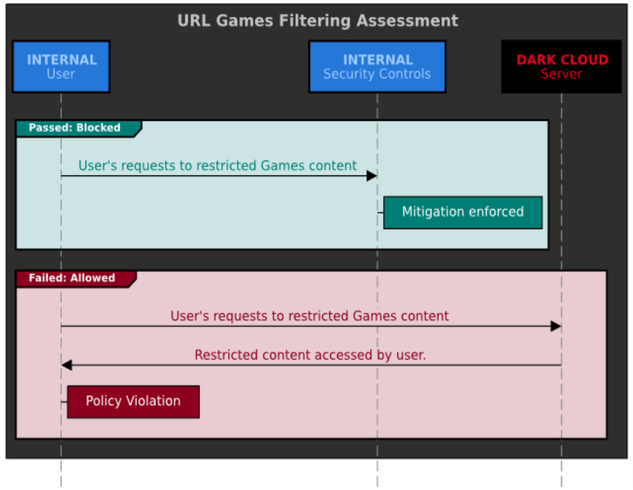
User uploads sensitive data files

Mitigation enforced

Failed: Allowed

User uploads sensitive data files

Policy Violation



URL Games Filtering Assessment

INTERNAL User

INTERNAL Security Controls

DARK CLOUD Server

Passed: Blocked

User's requests to restricted Games content

Mitigation enforced

Failed: Allowed

User's requests to restricted Games content

Restricted content accessed by user.

Policy Violation

KEYSIGHT TECHNOLOGIES

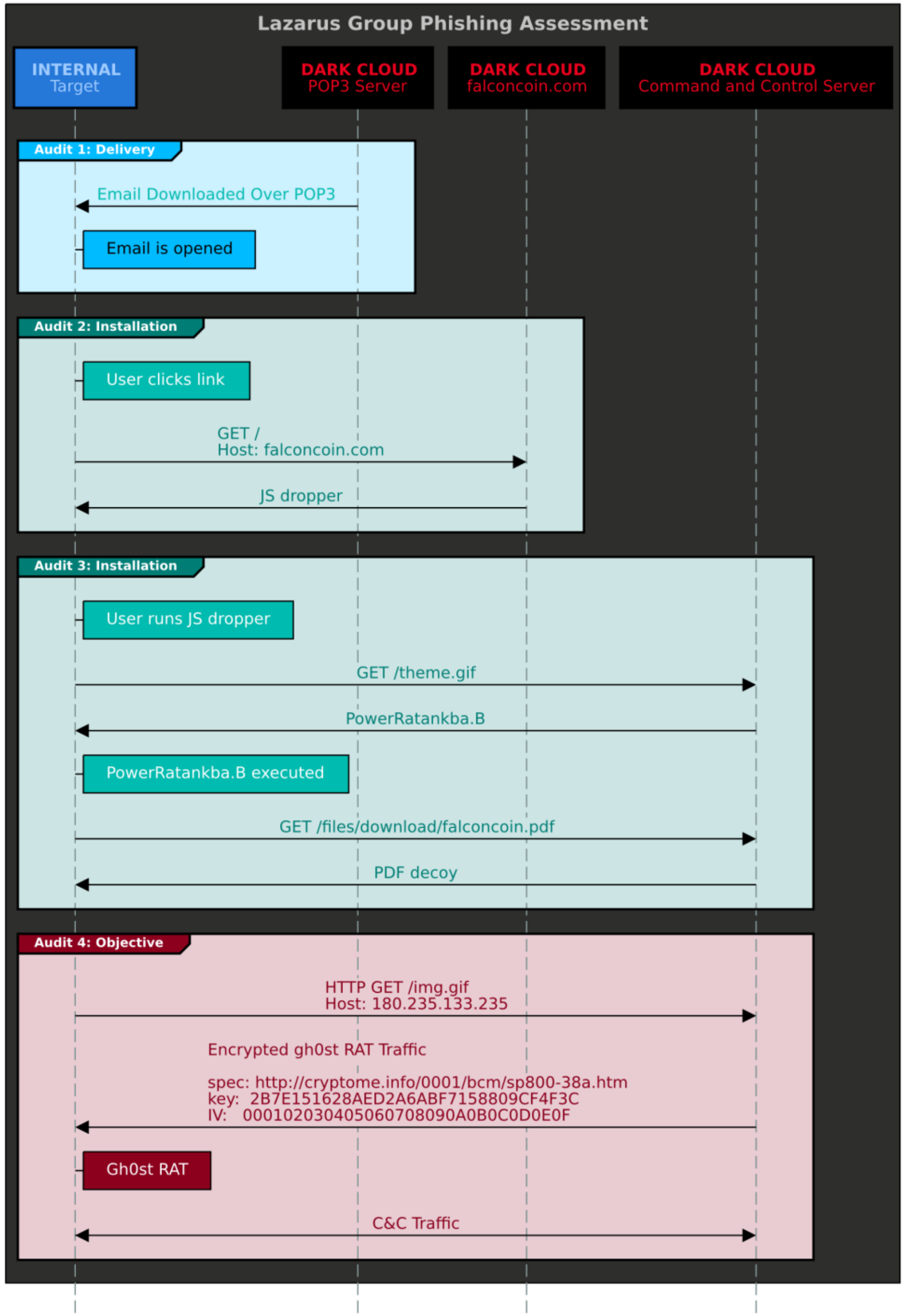
Kill Chain Example

Lazarus Group APT (Finance Industry Attack)

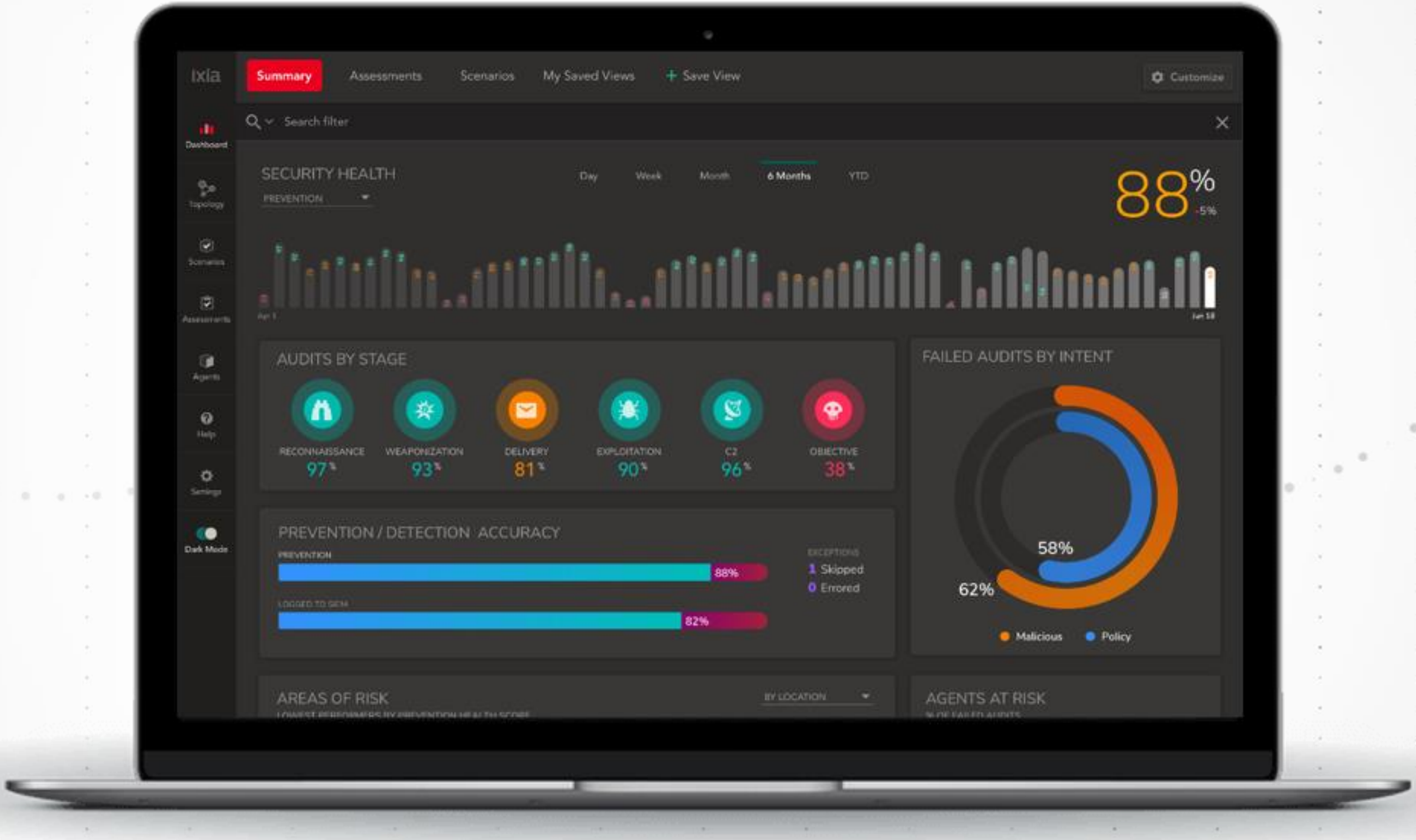
Example of adversary tactics, tools and procedures used against financial organizations

Objectives	Lazarus
Reconnaissance	-
Weapons	Malicious Adobe PDF document
Delivery	Spear phishing email advertising fantastic returns on Falconcoin, a "new" type of crypto coin advertised as an Initial Coin Offering, or ICO
Exploitation	-
Installation	The JavaScript dropper downloaded first then downloads a PDF that is displayed to the user advertising Falconcoin, the other one is an obfuscated PowerShell script known as PowerRatankba.B.
Command	The PowerShell script enables the malware to establish a persistent connection to a command and control server, while the PDF is used a visual decoy to prevent suspicion. It registers itself with the malicious network to facilitate exfiltration and remote code execution on the now infected host. After registration the bot is instructed to download and execute a variant of the Gh0stRAT malware.
Objective	The Gh0st RAT allows the attacker to take full control of the infected endpoint, log keystrokes, provide live webcam and microphone feeds, download and upload files, etc.

THE LOCKHEED MARTIN CYBER KILL CHAIN FRAMEWORK



Threat Simulator DEMO



OUR APPROACH

Automated Breach and Attack Simulation for Live Networks

MEASURE

Measures the cyber security efficacy

Identifies security gaps

Data to communicate how security works and justify IT investments

OPTIMIZE

Identifies opportunities to remediate security gaps

List of remediation actions to improve the security effectiveness

MONITOR

Monitors for environment drifts using automated, continuous validations

Opportunities to take proactive actions to maintain optimal security posture

NETworking SummIT Online-Agenda

16. Juni 2020

- 10-11 Uhr Riverbed – SaaS Accelerator Schneller Zugriff auf SaaS Anwendungen
- 14-15 Uhr Aternity – der End-User im Fokus

17. Juni 2020

- 10-11 Uhr Zscaler Security as a Service & O365 – mit Hilfe von Zscaler wird das Internet zum sicheren Unternehmensnetzwerk
- 14-15 Uhr A10 Network SSL-Visibility & DDoS-Detection – Sicherheit im Highspeed-Netz

18. Juni 2020

- **10-11 Uhr IXIA Threat Simulator Breach and Attack Defense –Hack yourself before they do!** ⬅
- 14-15 Uhr ExtraHop - Sicherheitslücken mit High Speed Anomalie-Erkennung identifizieren

riverbed Aternity zscaler™ A10 ixia A Keysight Business ExtraHop

DANKE FÜR IHRE TEILNAHME!

Haben Sie Interesse am IXIA Threat Simulator?

Dann kontaktieren Sie uns

dakoServ Daten Kommunikation Service GmbH
Borsigstraße 34
65205 Wiesbaden
Telefon: +49 (0)6122 / 53465-0
Telefax: +49 (0)6122 / 53465-19
E-Mail: info@dakoserv.de
Internet: https://www.dakoserv.de