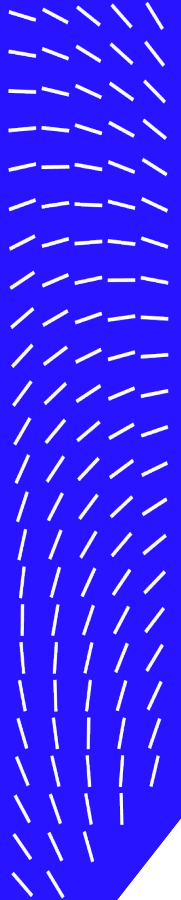


Trellix

Trellix Demo Platform - Updates and best practices

How to be more effective in the field



Intros



Luke McCoy
Senior Sales Manager
for ANZ at Trellix



Trent Bowman
Global Solutions
Architect at Trellix

Agenda



Execute Great Software Demonstrations



Customer Use Case



Trellix Crossfire - POV environment



Q&A \ Discussions

Trellix

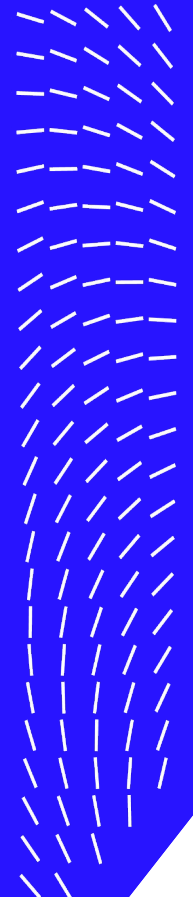
Execute Great Software Demonstrations

Development, execution and use case

Luke McCoy

Senior Manager, ANZ Solutions Engineering

July 11, 2024



Why do we do demonstrations?

dem·on·stra·tion

[dɪmənˈstreɪʃ(ə)n] 

a practical exhibition and explanation of how something works or is performed:

"a microwave cookery demonstration"

synonyms: exhibition · presentation · display · illustration · demo · taster · exposition ·
teach-in

What type of demonstrations might you do?

Vision / Qualifying / Closing

How can they go wrong ?



Consequences of poor demonstrations?



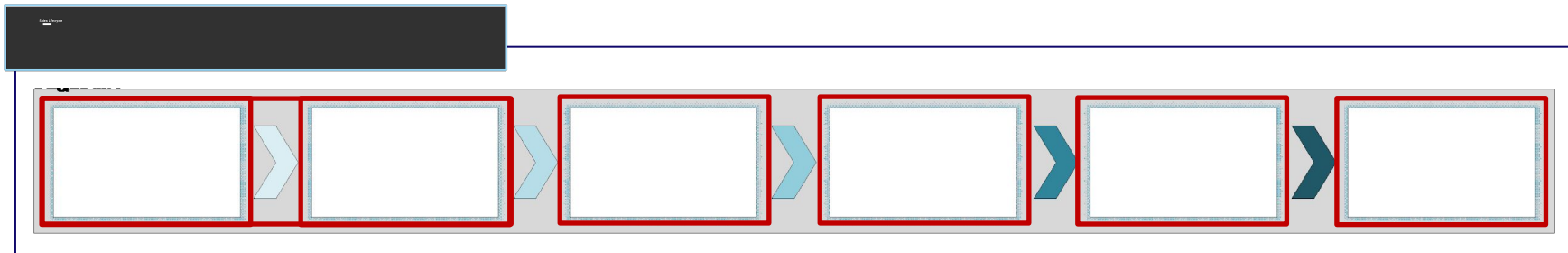
Sales

- Lost opportunity / customer goes dark
- Increased cost of sale
- Requires POC (tire kickers)
- Reduced ASPs
- Run out of time
- Harbor tours

Deployment

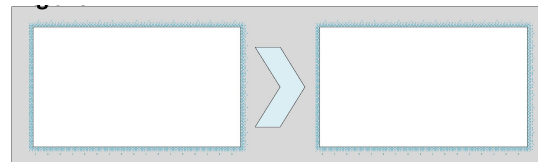
- Misaligned expectations
- Deployment blockers
- Finger pointing
- Slowed adoption
- Sunk services required
- Subscriptions not renewed

Sales Lifecycle

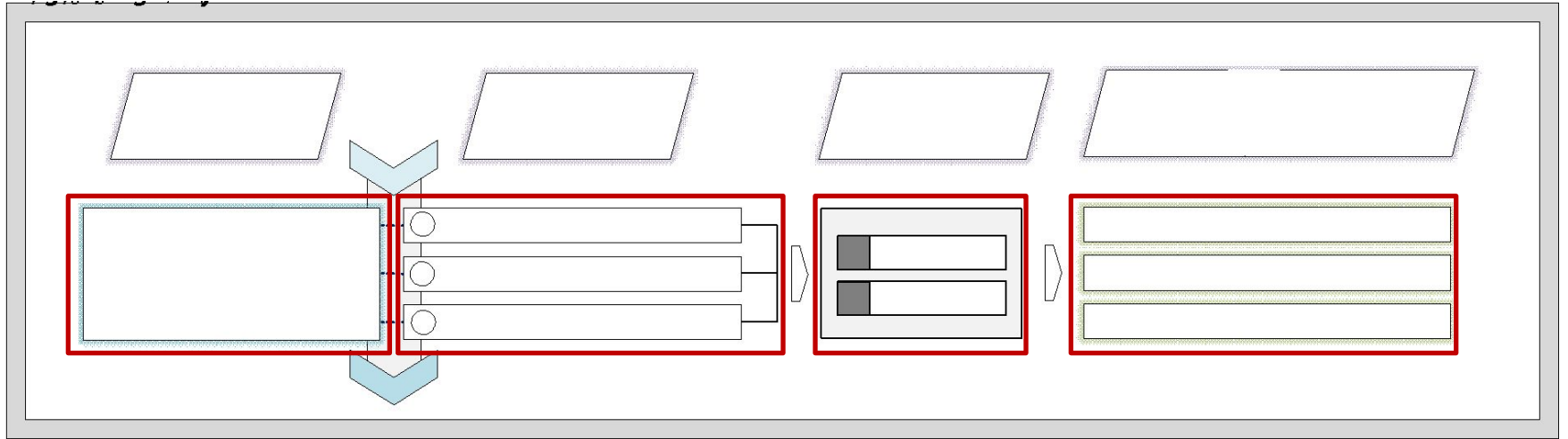


Enables sales team to quickly qualify deals in or out, so sellers can focus on High potential opportunities.

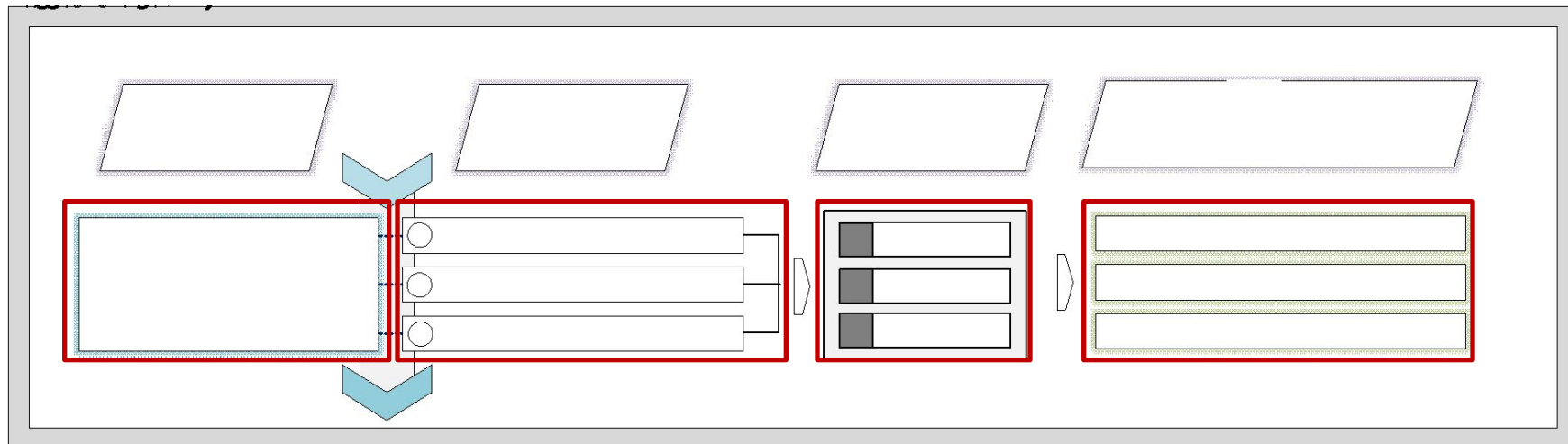
How do we as engineers, ensure we support the opportunity during the initial stages successfully ?



Engineering Discovery



Engineering Align - Demo



Use case - Email



**IT leader/SOC
Architect**

Key Responsibilities

- Responsible for efficacy of product
- Management of security tools
- Security Program Stakeholder
- Timely reports to senior management of type and frequency of threats
- Optimize security investments and staff

Current Challenges

- Suspects advanced threats including malware, phishing, site URLs and impersonation attacks are being missed (O365)
- Credential harvesting across the organization despite incumbent solution promise
- Too many false positives and false negatives

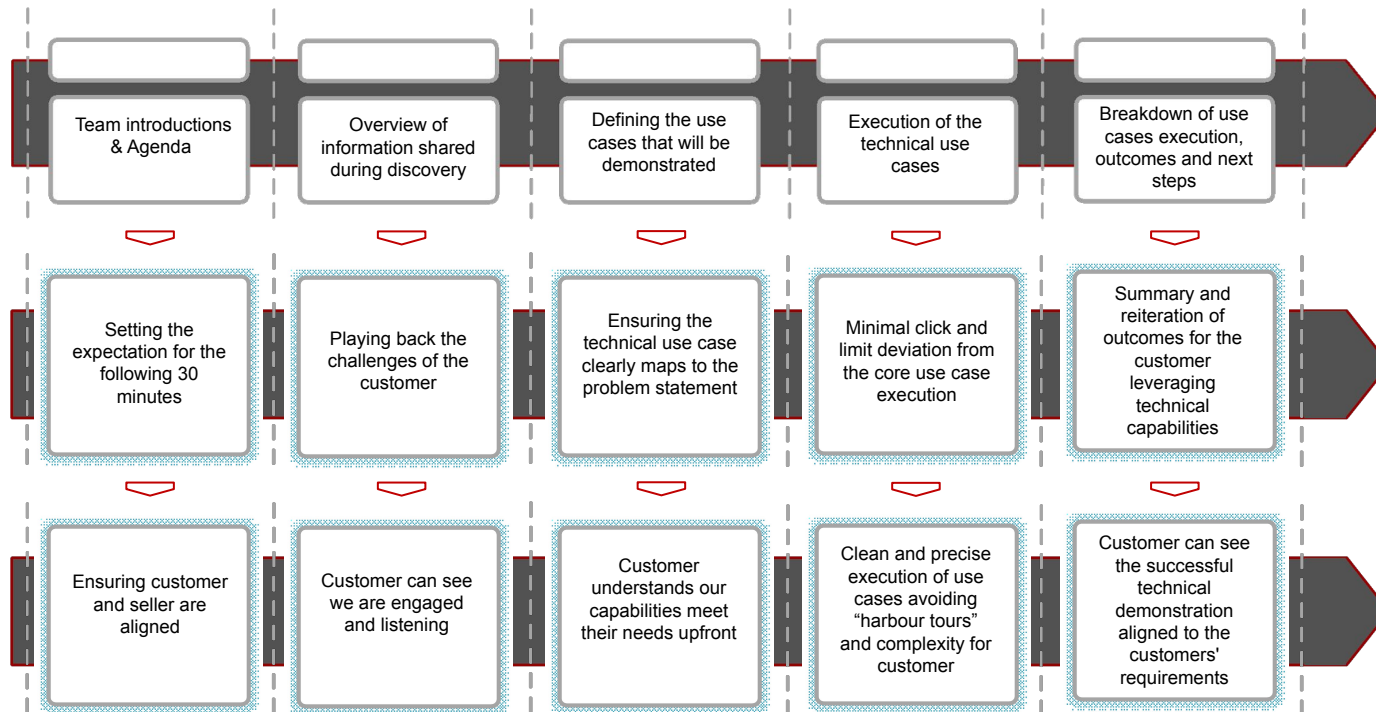
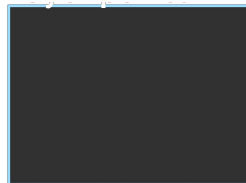
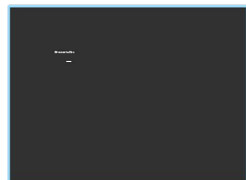
Timelines

- EOFY – 6 weeks left and requires quantifiable data to support procurement

Use case - Email

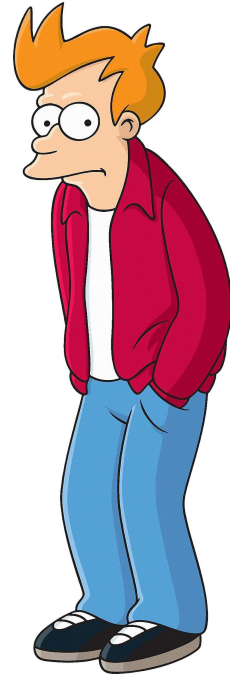
Discover	Customer Business Ask / Requirements	Email based compromises are 2/3 of all incident response engagements – High visibility at C level
	Security Domain Focus	Email Security
	Security Requirements	Detection/Prevention for advanced threats via email / Proactive remediation
3 Whys	Why Anything ?	Email is becoming resource intensive to the SOC / High risk vector to the Enterprise
	Why Trellix ?	High fidelity detections for advanced threats / simple deployment / tangible data
	Why Now ?	Currently open budget but will be absorbed back into the business if not spend by EOFY
Align	Replay Security Requirements	Detection/Prevention for advanced threats via email / Proactive remediation
	Use case / Metrics	O365 Mail Security bypass > Trellix Email Detection > Auto remediation
	Trellix Security Domain / Demo	Pre-prepared Use case in Trellix Crossfire

Demonstration Flow



Technical Considerations

- Stop performing Harbour tour style demos
- Build a vision that the customer could do this themselves
- Avoid complication for the sake of innovation unless in scope of the use case
- Do the last things first ! – Engagement and Impact



Summary



- Great **discovery** will always lead to a fantastic well **aligned** demonstrations
- Operational efficiencies and gain metrics are often more valuable than the number of features and functions available (No Harbour Tours)
- Allow for the customer to “peel back the layers” , no need to offer up information that has not been asked
- Hold off on giving a demo until they have sufficient evidence of the customer’s business pains and outcomes

Trellix

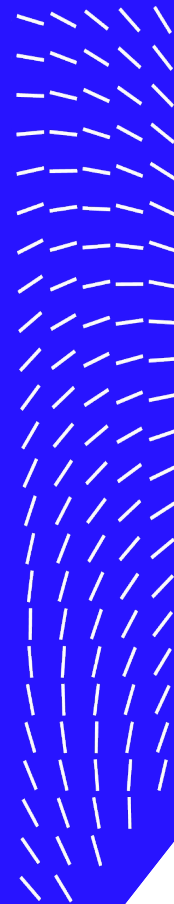
Trellix Crossfire Platform

Demonstration Portal – Overview

Trent Bowman

Global Solutions Architect , XDR/SecOps

July 11, 2024



Crossfire Walkthrough

Logging In...

Data requested by the Executive team. Please fill in correctly.

This lab use purpose:

Enter customer and opportunity details:

Name

Opportunity

Products covered:

<input type="checkbox"/> CM	<input type="checkbox"/> NX	<input type="checkbox"/> EX
<input type="checkbox"/> ETP	<input type="checkbox"/> HX	<input type="checkbox"/> PX
<input type="checkbox"/> IA	<input type="checkbox"/> AX	<input type="checkbox"/> FX
<input type="checkbox"/> FSO	<input type="checkbox"/> Cloudvisory	<input type="checkbox"/> MSV
<input type="checkbox"/> iSight	<input type="checkbox"/> SSLi	<input type="checkbox"/> Helix

Data requested by the Executive team. Please fill in correctly.

This lab use purpose:

Crossfire Walkthrough

Dashboard...

XFire Lab (ASH) :: Dashboard

Lab user: trent.bowman@trellix.com [Show password](#)

Lab Systems

Appliances labeled as "02" provide Admin access

Special Projects

DOCUMENT_SHARE				
----------------	--	--	--	--

Crossfire Lab Guide

Trellix Platform

Trellix XDR Xconsole				
----------------------	--	--	--	--

Security Operations and Analytics

Trellix XDR EPO

Trellix EPO Cloud				
-------------------	--	--	--	--

Helix Demo1 (Prod)

Helix Demo 3 (prod)

Endpoint Security

Trellix EDR				
-------------	--	--	--	--

hx01	HX 2502	5.3.3		
hx02	HX 2502	5.3.3		
hx03	HX 2502	5.3.3		
HXTools v4				
HX Demo 1				
HX Demo 2				
HX Demo 3				

Network Security

IPS Manager				
-------------	--	--	--	--

nx01	NX 4500	10.0.0	all	inline	
nx-xdr-d2	NX 1500	10.0.1	all	span	
nx11v-demo01	NX 2500	10.0.0	all	span	

Virtual Machines

VM name: Win7x64

Lab Mailbox: trent.bowman@ash.selabs.freeye.com

Inbox is empty.

Trellix

Crossfire Walkthrough

Lab Systems...

Appliances labeled as "02" provide Admin access	
Special Projects	
DOCUMENT_SHARE	
Crossfire Lab Guide	
Trellix Platform	
Trellix XDR Xconsole	
Security Operations and Analytics	
Trellix XDR EPO	
Trellix EPO Cloud	
Helix Demo1 (Prod)	
Helix Demo 3 (prod)	
Endpoint Security	
Trellix EDR	
hx01	HX 2502 5.3.3
hx02	HX 2502 5.3.3
hx03	HX 2502 5.3.3
HXTools v4	
HX Demo 1	
HX Demo 2	
HX Demo 3	
Network Security	
IPS Manager	
nx01	NX 4500 10.0.0 inline
nx-xdr-d2	NX 1500 10.0.1 span
nx11v-demo01	NX 2500 10.0.0 span



Globe = Go To Lab Environment
CMD = Go To Command Line
Lock = Credentials for Lab

Crossfire Walkthrough

Virtual Machines...

The screenshot displays the Trellix Virtual Machines management interface. A dropdown menu is open, showing a list of operating system images. The 'Create' button is highlighted in green. Below the dropdown, a table lists existing virtual machines.

Virtual Machines

VM name: Win7x64 [Create]

Lab Mailbox: trent.bowman@ash.selabs.fireeye.com
Inbox is empty.

Virtual Machines

Name	Role/image	IP address	State	Actions
APJ Summit	Win7x64	no ip	creating	[Power] [Refresh] [Delete]

Crossfire Walkthrough

Scenarios...

XFIRE Lab (ASH) :: Scenarios Trellix

Create Scenario

Trellix XDR Solutions - Extended Detection and Response Create

- Trellix XDR Xconsole
- Trellix XDR EPO
- Helix Demo1 (Prod)
- Trellix EDR
- HX Demo 1
- NX1500
- CMS Demo 2
- EX5500
- ETP

XDR Workbench

- EPO-ONPREM
- Marketing
- Finance
- Accounting

Trellix XDR Solutions - Extended Detection and Response

- Blackhat_XDR_demo_WIP.pdf

Trellix Data Protection - Prevention and Monitoring Create

- EPO-Prevent
- dlp-prevent-01
- dlp-monitor-01

DLP-WORKBENCH

- Finance
- Marketing
- Accounting

Trellix Data Protection

Clandestine Wolf 2.0 Create

- Helix Demo1 (Prod)
- HX2502
- HX Demo 1
- NX4500
- CM2500
- CMS Demo 1

Attacker

- Research-1
- Research-2
- Research-3
- Research-6

Clandestine Wolf 2.0 Setup and Demo Guide

- CW_2.0_Setup_and_Demo_Guide.pdf

FireEye Platform Create

- HX2502
- NX4500
- CM2500
- EX5500
- ETP

Attacker

- Victim
- Lateral

FCP Introduction

- FireEye Platform Scenario Guide (8/21)
- FireEye_Platform_Scenario_Guide.pdf

Crossfire Walkthrough

Scenarios...

XFIRE Lab (ASH) :: Scenarios Trellix

Create Scenario Clandestine Wolf 2.0

Lab user: trent.bowman@trellix.com Show password Stop scenario Delete scenario

Hostname	Model	Version	Access	Role/image	IP address	State	Actions
	Helix Demo1 (Prod)			Attacker	10.14.15.160	running	
hx03	HX2502	5.3.3		Research-1	10.14.21.164	running	
	HX Demo 1			Research-2	10.14.20.245	running	
rx01	NX4500	18.0.0 Inline		Research-3	10.14.20.244	running	
cm01	CM2500	18.0.0		Research-6	10.14.20.243	running	
	CMS Demo 1						

[CW_2.0_Setup_and_Demo_Guide.pdf](#)

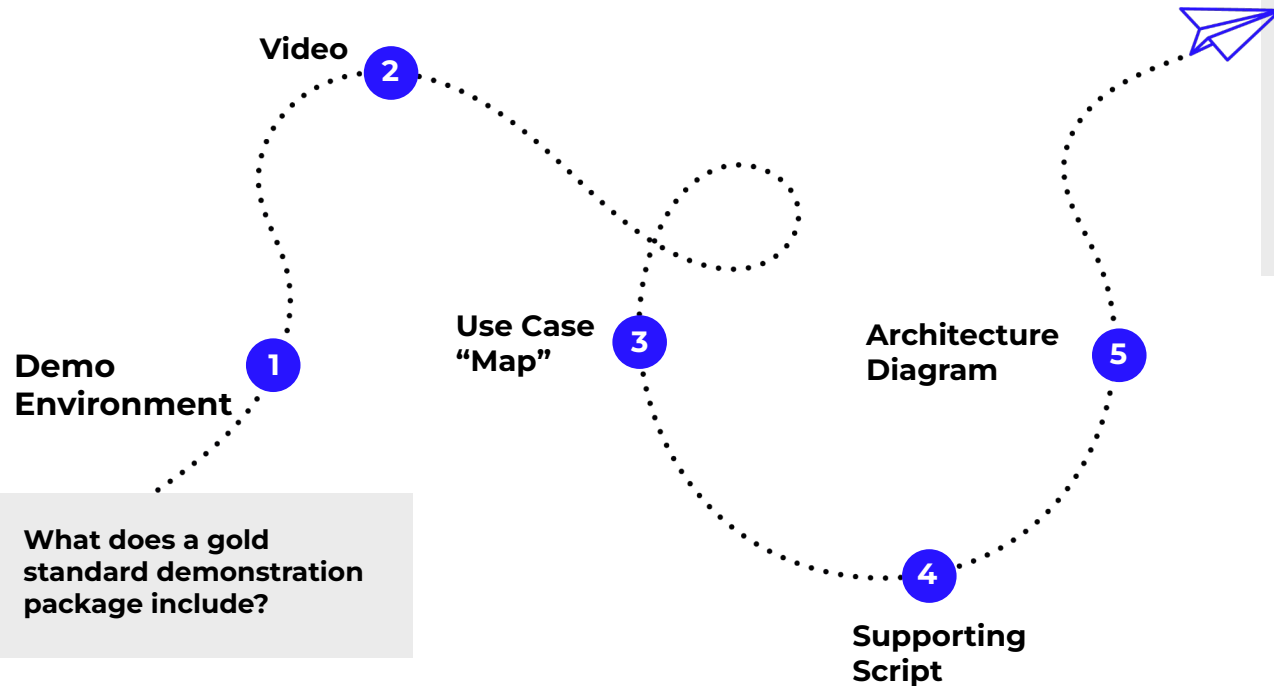
Demo Guide: [Clandestine Wolf 2.0 Setup and Demo Guide](#)

SE Demo Video: [SE Training Webinar and Demo Recording](#)

NOTE: SFO HX03 is a typo, the local agent will bind to ASH HX03 if option #2 is selected on the attacker

XFIRE Lab (ASH) 4.0-20211225 (c) 2015-2023 by the XPFIRE (FATE) Team

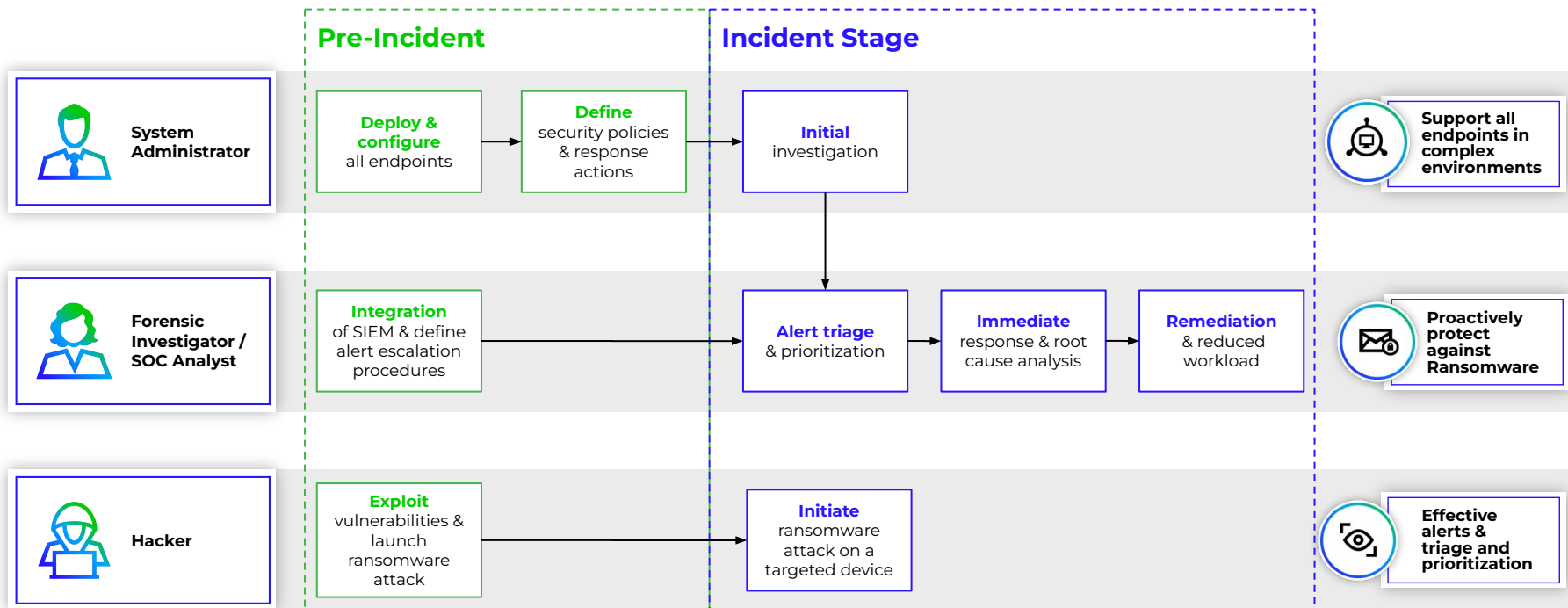
Crossfire Environment Futures



What does a gold standard demonstration package include?

- Top 3 demos per segment will be gold standard.
- All demos will be available in a new Seismic microsite/library.

Use Case Map - Example



Crossfire Summary



In Conclusion...

Demo Support →

Trellix Crossfire Offerings

- Security Operations (Helix, FSO, ePO)
- Endpoint Security (EDR, HX)
- XConsole
- Network Security (NX, IPS, IA, PX, FX, NDR)
- Intelligent Virtual Execution Sandbox (IVX)
- Management Systems (CMS)
- Collaboration Security (EX, ETP)
- Demo Tools (Malware Barn, Illuminator)
- Cloudvisory

Ben Cares	Email	<ul style="list-style-type: none">• Updated ETP demo package.• Make email corpus available for demos.
David Troitino	Endpoint	<ul style="list-style-type: none">• Define “gold demo template”.• Improve user experience .
Wasif Kazi	Network	<ul style="list-style-type: none">• New IVX env and demo.• NDR demo script development.
	XDR	<ul style="list-style-type: none">• Add more products to XConsole. (Forensics, Email, IVX)
Tarisha Bhimta	Data	<ul style="list-style-type: none">• Publish updated Database Security demo.• Update 3rd party integrations with DLP.

Thankyou

