BASE4 SECURITY

Democratizing Incident Response Tabletop Exercises

FIRST Technical Colloquium 2023

Amsterdam, NL

Federico Pacheco

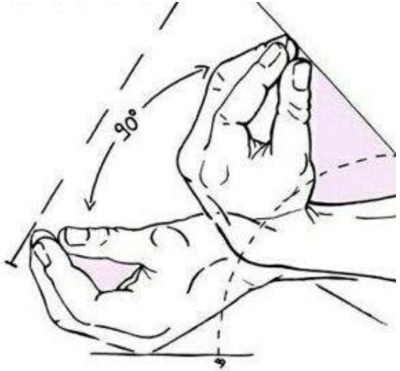
R+D+i Manager

fpacheco@base4sec.com

@FedeQuark

Who is this unknown guy?

- Born in Argentina
- Italian passport
- Living in Spain



Committed to help reducing the gap between industry and academia in cybersecurity

Disclaimer

This presentation may contain excessive amounts of memes in order to bypass cultural barriers

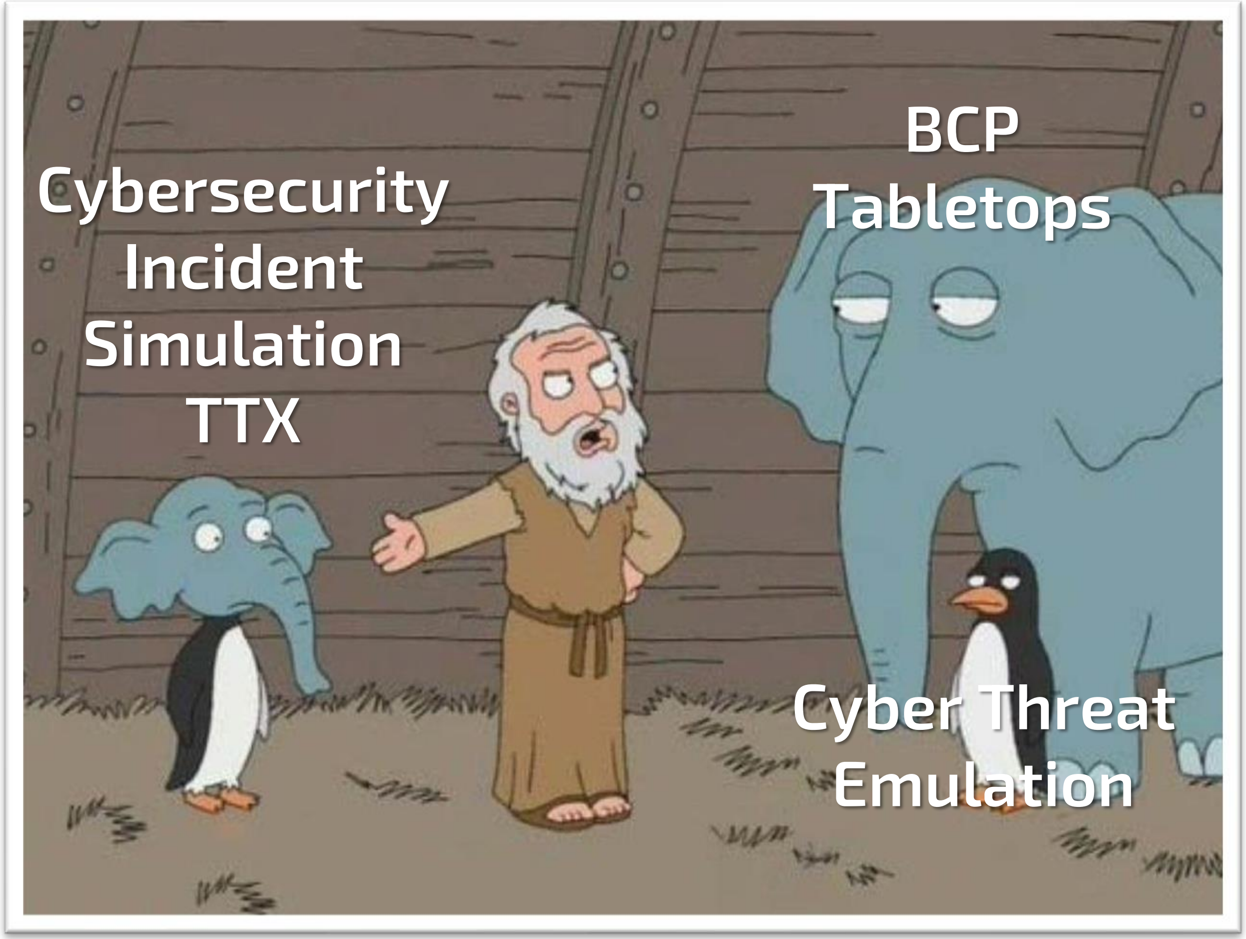
DI MARIA
10

Democratize

Tabletop Exercises (TTX)

Incident Response

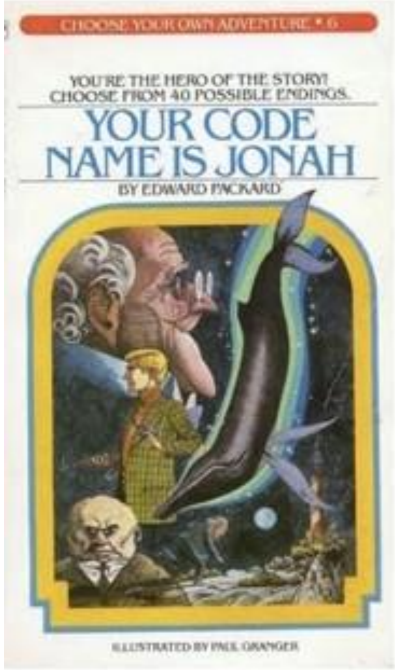
Let's face it

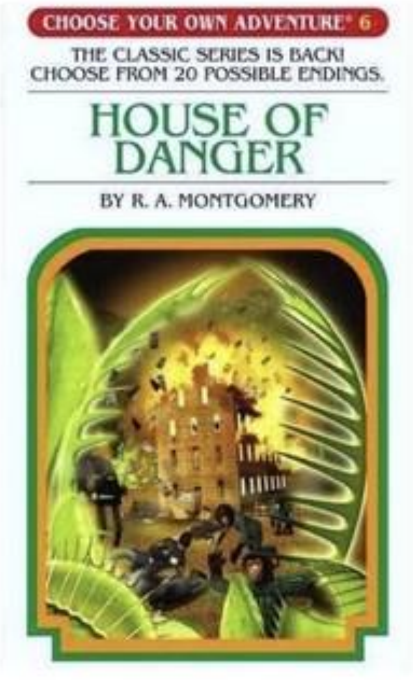

Cybersecurity Incident Simulation TTX
BCP Tabletops
Cyber Threat Emulation

Incident Response

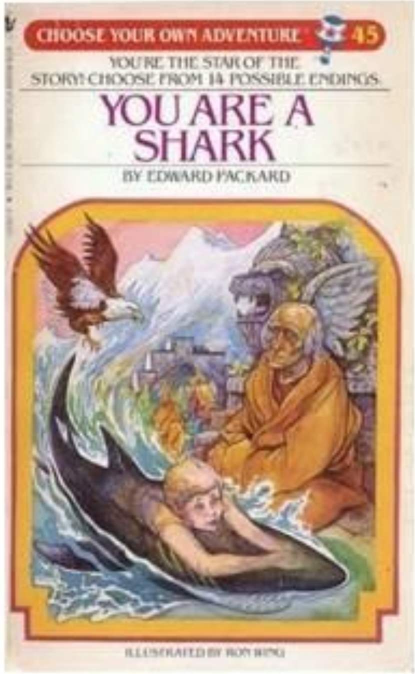
Tabletop Exercises

What it seems to be


CHOOSE YOUR OWN ADVENTURE® 6
YOU'RE THE HERO OF THE STORY! CHOOSE FROM 40 POSSIBLE ENDINGS.
YOUR CODE NAME IS JONAH
BY EDWARD PACKARD
ILLUSTRATED BY PAUL GRANGER


CHOOSE YOUR OWN ADVENTURE® 6
THE CLASSIC SERIES IS BACK! CHOOSE FROM 20 POSSIBLE ENDINGS.
HOUSE OF DANGER
BY R. A. MONTGOMERY

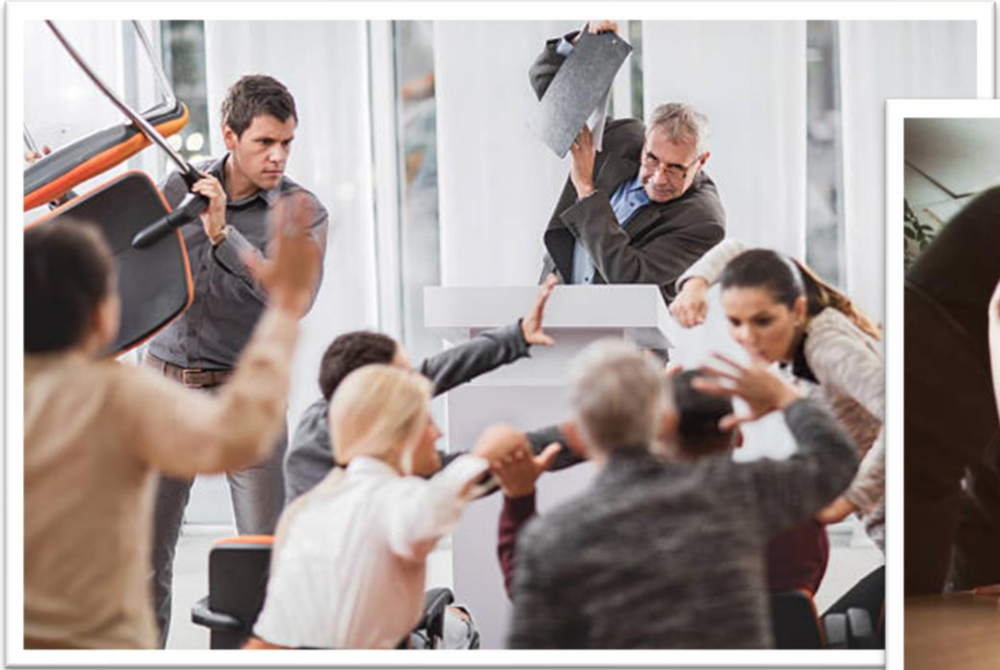
CHOOSE YOUR OWN ADVENTURE® 22
YOU'RE THE STAR OF THE STORY! CHOOSE FROM 26 POSSIBLE ENDINGS.
SPACE PATROL
BY JULIUS GOODMAN
ILLUSTRATED BY RALPH REESE

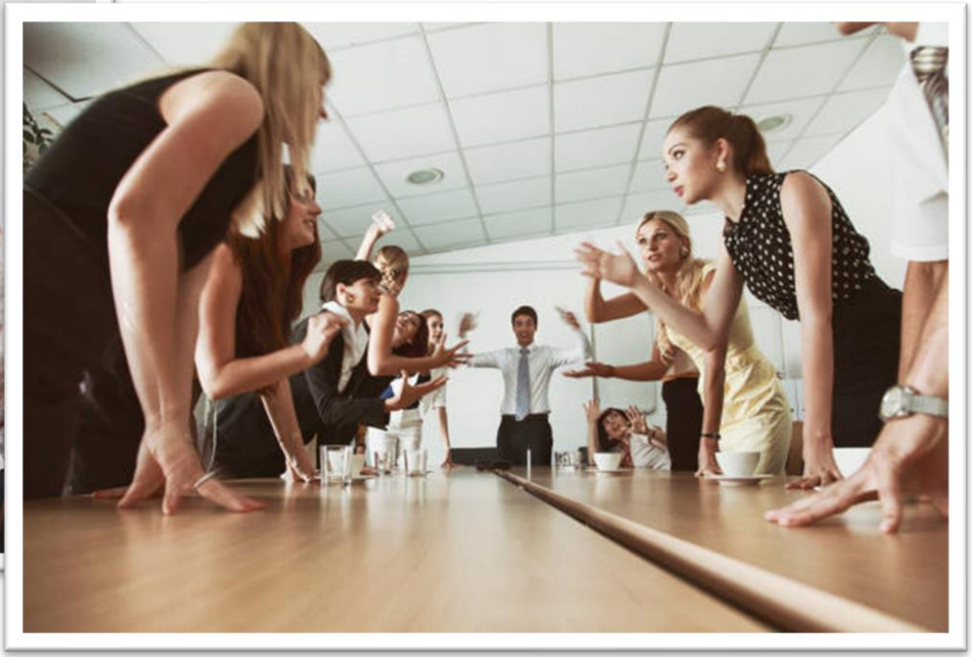

CHOOSE YOUR OWN ADVENTURE® 45
YOU'RE THE STAR OF THE STORY! CHOOSE FROM 14 POSSIBLE ENDINGS.
YOU ARE A SHARK
BY EDWARD PACKARD
ILLUSTRATED BY RON WING

What customers think it is

What we think our approach is

What usually occurs





Exercise Dynamics

Participants → Areas

Scenario → Events

Information → Decisions

Interaction

What for?

Communication

Documentation

Playbooks

Runbooks

Procedures

Operations

Capabilities

Decisions

Coordination

Escalation

Types of participants

Player

Observer

Connector

Coordinator

Scenario creation

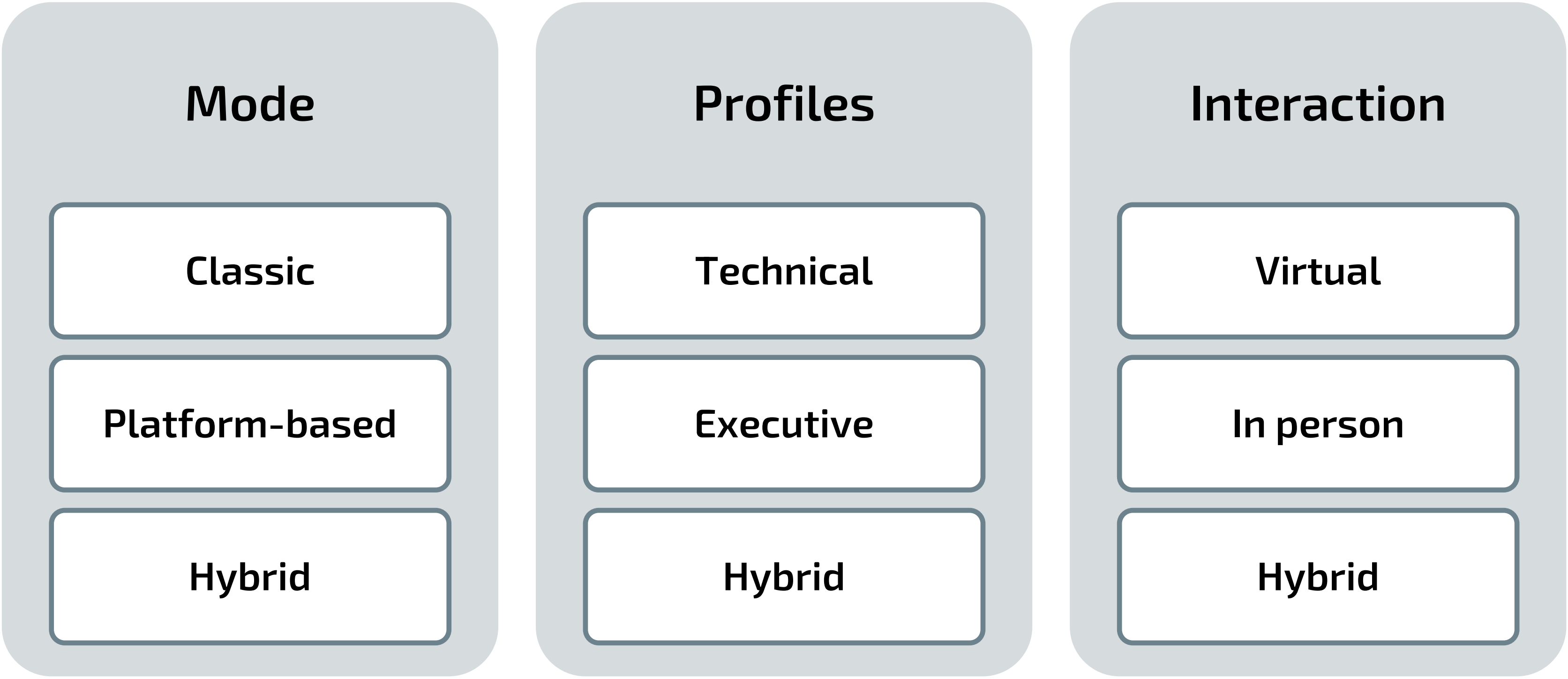
By threat category

- Ransomware
- Denial of Service
- Insiders
- Data Leakeage
- Social Engineering
- Third parties
- Physical disruption

By industry

- Banking & Insurance
- Government
- Critical infrastructure
- Manufacture
- Software Development
- Health

Design Decisions



Mode

- Classic
- Platform-based
- Hybrid

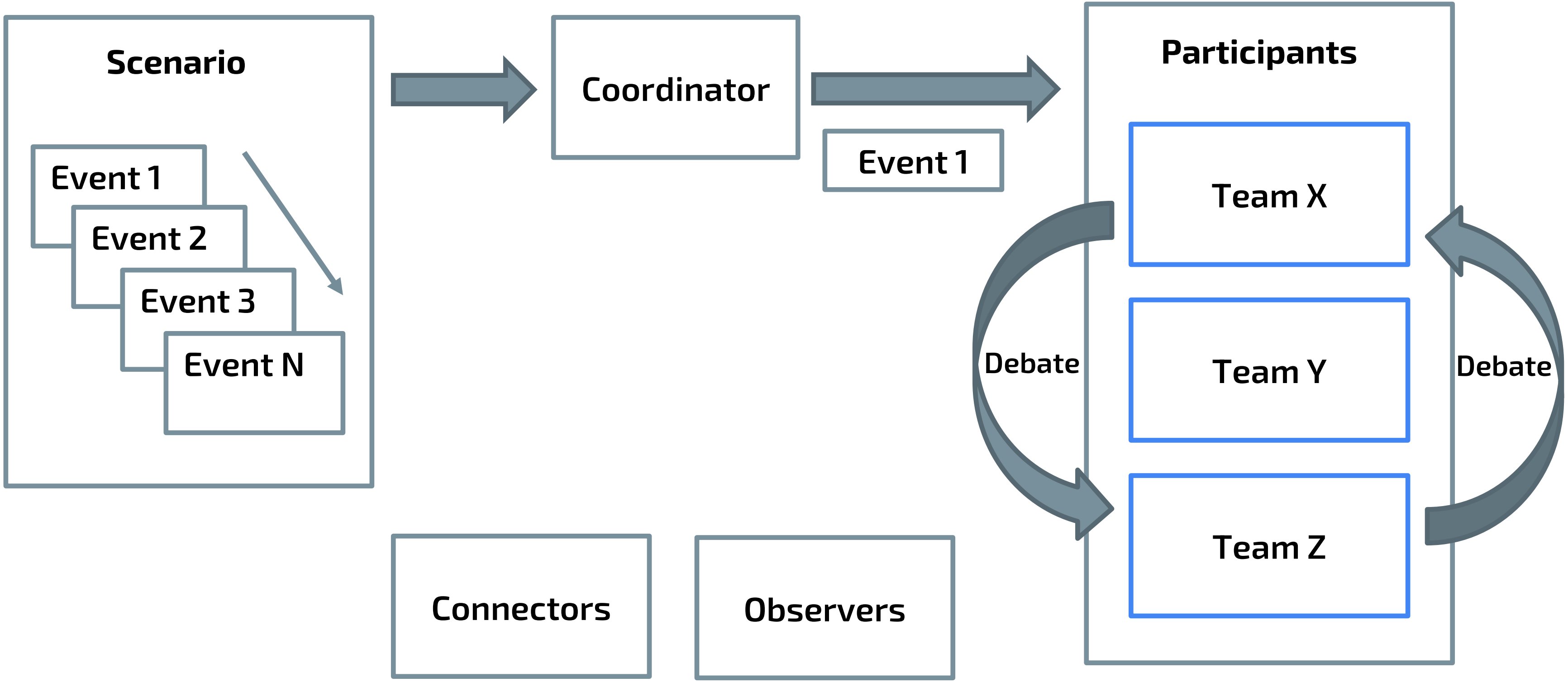
Profiles

- Technical
- Executive
- Hybrid

Interaction

- Virtual
- In person
- Hybrid

Classic Mode



Scenario

Event 1

Event 2

Event 3

Event N

Coordinator

Event 1

Participants

Team X

Team Y

Team Z

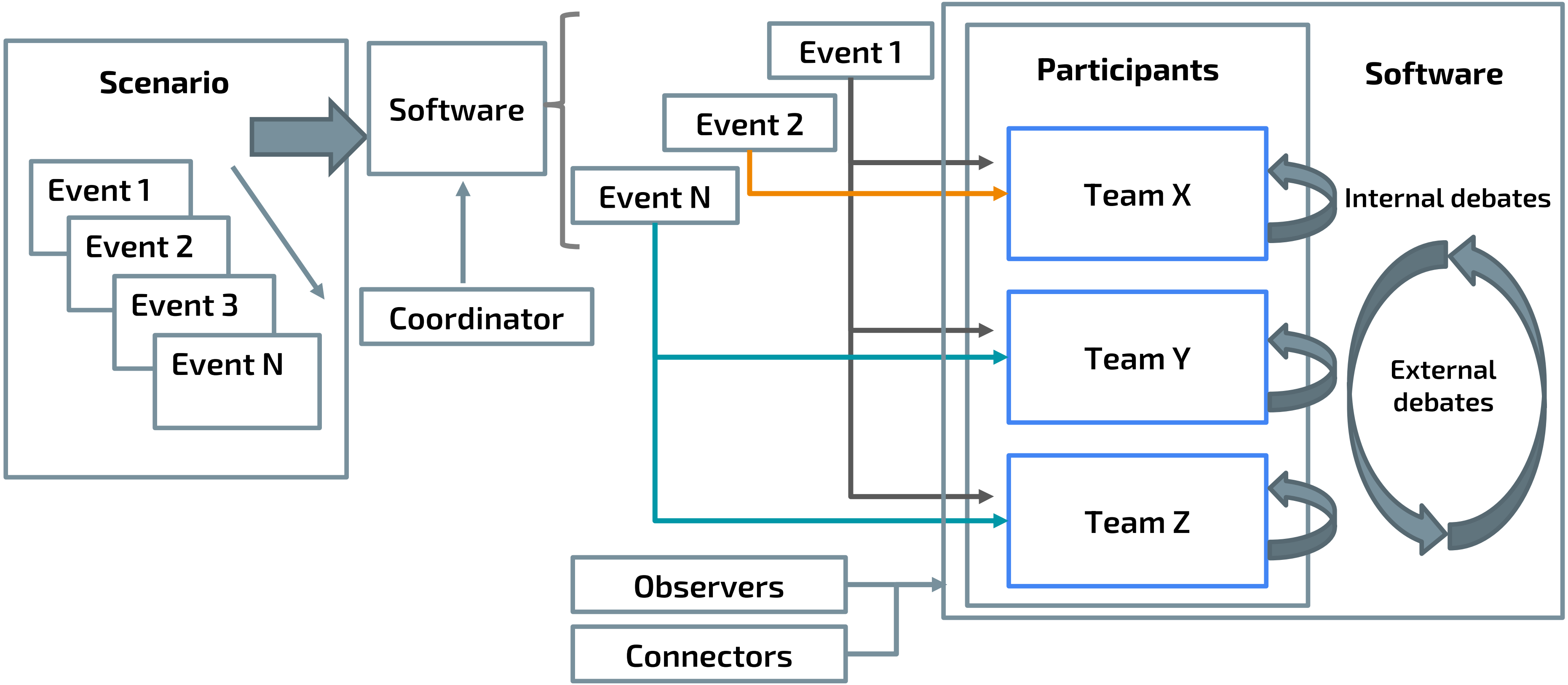
Debate

Debate

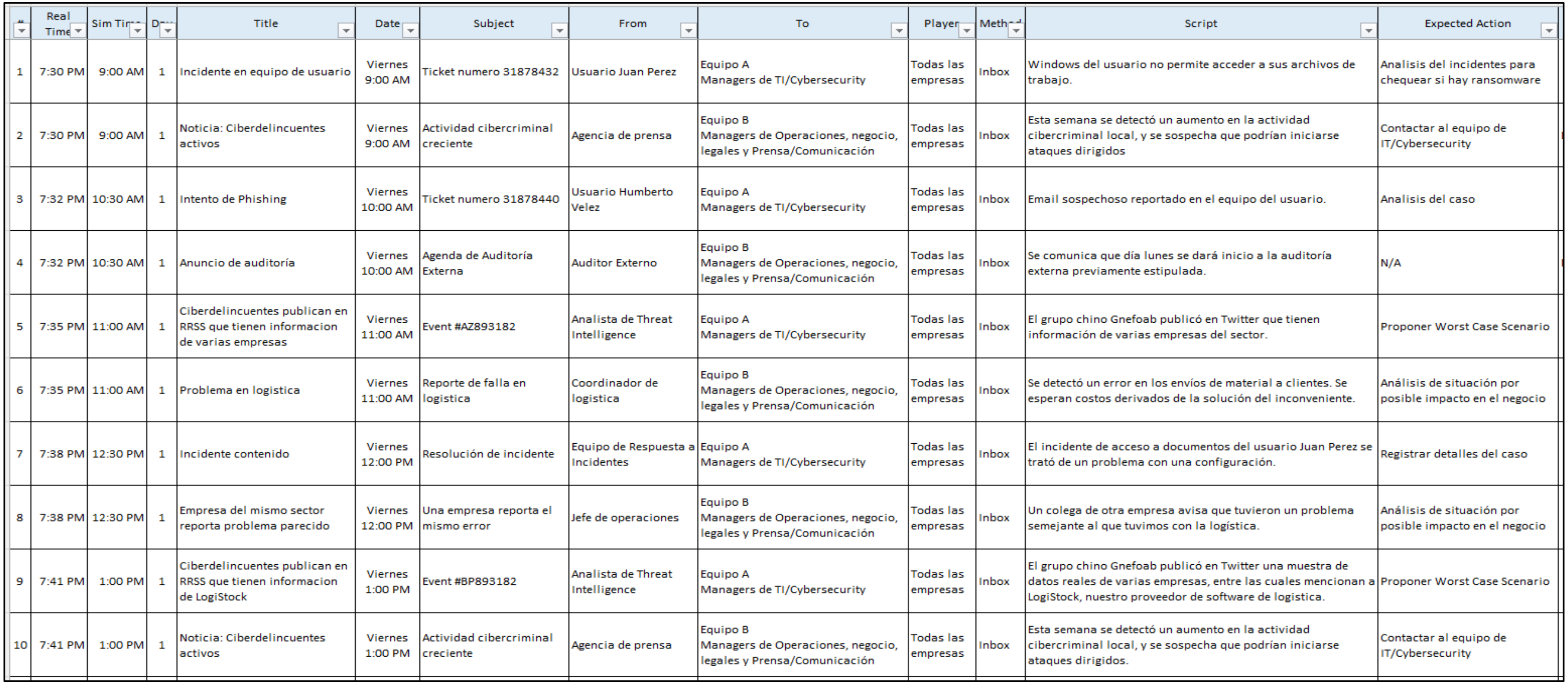
Connectors

Observers

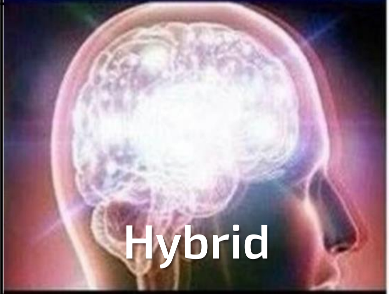
Platform-based mode



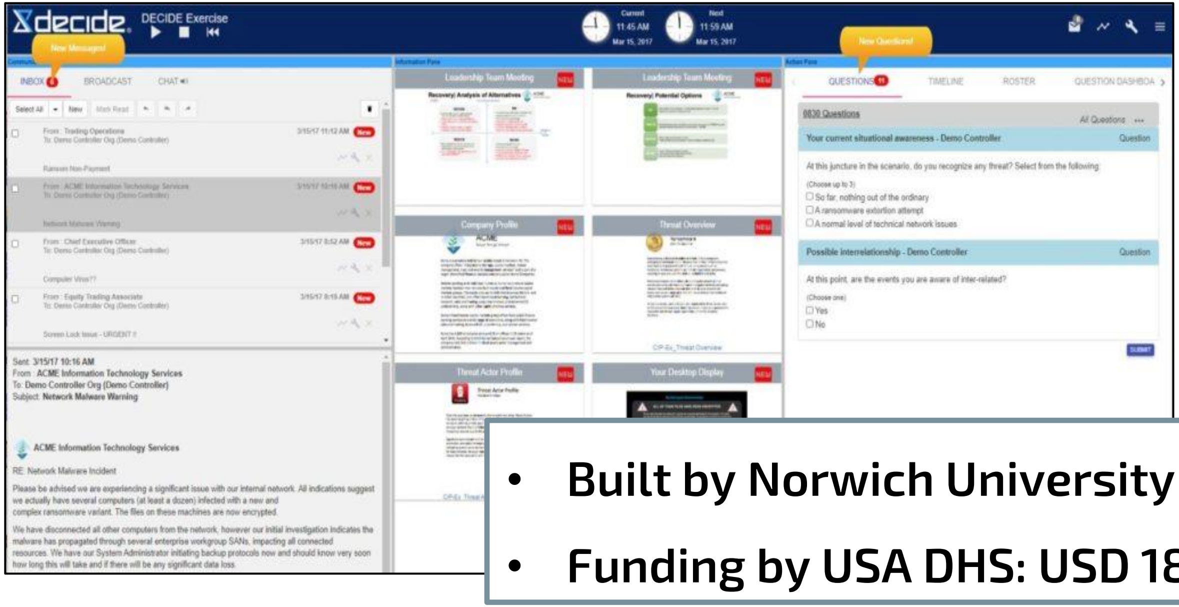
MSEL (Master Scenario Events List)



#	Real Time	Sim Ti	D	Title	Date	Subject	From	To	Player	Meth	Script	Expected Action
1	7:30 PM	9:00 AM	1	Incidente en equipo de usuario	Viernes 9:00 AM	Ticket numero 31878432	Usuario Juan Perez	Equipo A Managers de TI/Cybersecurity	Todas las empresas	Inbox	Windows del usuario no permite acceder a sus archivos de trabajo.	Analisis del incidentes para chequear si hay ransomware
2	7:30 PM	9:00 AM	1	Noticia: Ciberdelincuentes activos	Viernes 9:00 AM	Actividad cibercriminal creciente	Agencia de prensa	Equipo B Managers de Operaciones, negocio, legales y Prensa/Comunicación	Todas las empresas	Inbox	Esta semana se detectó un aumento en la actividad cibercriminal local, y se sospecha que podrían iniciarse ataques dirigidos	Contactar al equipo de IT/Cybersecurity
3	7:32 PM	10:30 AM	1	Intento de Phishing	Viernes 10:00 AM	Ticket numero 31878440	Usuario Humberto Velez	Equipo A Managers de TI/Cybersecurity	Todas las empresas	Inbox	Email sospechoso reportado en el equipo del usuario.	Analisis del caso
4	7:32 PM	10:30 AM	1	Anuncio de auditoría	Viernes 10:00 AM	Agenda de Auditoría Externa	Auditor Externo	Equipo B Managers de Operaciones, negocio, legales y Prensa/Comunicación	Todas las empresas	Inbox	Se comunica que día lunes se dará inicio a la auditoría externa previamente estipulada.	N/A
5	7:35 PM	11:00 AM	1	Ciberdelincuentes publican en RRSS que tienen informacion de varias empresas	Viernes 11:00 AM	Event #AZ893182	Analista de Threat Intelligence	Equipo A Managers de TI/Cybersecurity	Todas las empresas	Inbox	El grupo chino Gnefoab publicó en Twitter que tienen información de varias empresas del sector.	Proponer Worst Case Scenario
6	7:35 PM	11:00 AM	1	Problema en logistica	Viernes 11:00 AM	Reporte de falla en logistica	Coordinador de logistica	Equipo B Managers de Operaciones, negocio, legales y Prensa/Comunicación	Todas las empresas	Inbox	Se detectó un error en los envíos de material a clientes. Se esperan costos derivados de la solución del inconveniente.	Análisis de situación por posible impacto en el negocio
7	7:38 PM	12:30 PM	1	Incidente contenido	Viernes 12:00 PM	Resolución de incidente	Equipo de Respuesta a Incidentes	Equipo A Managers de TI/Cybersecurity	Todas las empresas	Inbox	El incidente de acceso a documentos del usuario Juan Perez se trató de un problema con una configuración.	Registrar detalles del caso
8	7:38 PM	12:30 PM	1	Empresa del mismo sector reporta problema parecido	Viernes 12:00 PM	Una empresa reporta el mismo error	Jefe de operaciones	Equipo B Managers de Operaciones, negocio, legales y Prensa/Comunicación	Todas las empresas	Inbox	Un colega de otra empresa avisa que tuvieron un problema semejante al que tuvimos con la logística.	Análisis de situación por posible impacto en el negocio
9	7:41 PM	1:00 PM	1	Ciberdelincuentes publican en RRSS que tienen informacion de LogiStock	Viernes 1:00 PM	Event #BP893182	Analista de Threat Intelligence	Equipo A Managers de TI/Cybersecurity	Todas las empresas	Inbox	El grupo chino Gnefoab publicó en Twitter una muestra de datos reales de varias empresas, entre las cuales mencionan a LogiStock, nuestro proveedor de software de logística.	Proponer Worst Case Scenario
10	7:41 PM	1:00 PM	1	Noticia: Ciberdelincuentes activos	Viernes 1:00 PM	Actividad cibercriminal creciente	Agencia de prensa	Equipo B Managers de Operaciones, negocio, legales y Prensa/Comunicación	Todas las empresas	Inbox	Esta semana se detectó un aumento en la actividad cibercriminal local, y se sospecha que podrían iniciarse ataques dirigidos.	Contactar al equipo de IT/Cybersecurity

Mode	Pros	Cons
Classic	- Live continuous debate - Timing according to interaction	- Same info for everyone - Biased towards the most talkative
Platform-based	- Different info by teams - More realistic (chat/calls)	- Fixed timing according to design - No continuous interaction
 Hybrid	- Best of both worlds - Fully realistic	- Higher complexity - Needs maturity

The pioneers: DECIDE



From : Trading Operations
To: Demo Controller Org (Demo Controller) 3/15/17 11:12 AM New
Ransom Non-Payment

From : ACME Information Technology Services
To: Demo Controller Org (Demo Controller) 3/15/17 10:16 AM New
Network Malware Warning

From : Chief Executive Officer
To: Demo Controller Org (Demo Controller) 3/15/17 8:52 AM New
Computer Virus??

From : Equity Trading Associate
To: Demo Controller Org (Demo Controller) 3/15/17 8:19 AM New
Screen Lock Issue - URGENT !!

Sent: 3/15/17 10:16 AM
From : ACME Information Technology Services
To: Demo Controller Org (Demo Controller)
Subject: Network Malware Warning

ACME Information Technology Services

RE: Network Malware Incident

Please be advised we are experiencing a significant issue with our internal network. All indications suggest we actually have several computers (at least a dozen) infected with a new and complex ransomware variant. The files on these machines are now encrypted.

We have disconnected all other computers from the network, however our initial investigation indicates the malware has propagated through several enterprise workgroup SANs, impacting all connected resources. We have our System Administrator initiating backup protocols now and should know very soon how long this will take and if there will be any significant data loss.

0830 Questions — All Questions

Your current situational awareness - Demo Controller — Question

At this juncture in the scenario, do you recognize any threat? Select from the following:

(Choose up to 3)
☐ So far, nothing out of the ordinary
☐ A ransomware extortion attempt
☐ A normal level of technical network issues

Possible Interrelationship - Demo Controller — Question

At this point, are the events you are aware of inter-related?

(Choose one)
☐ Yes
☐ No

Homeland Security

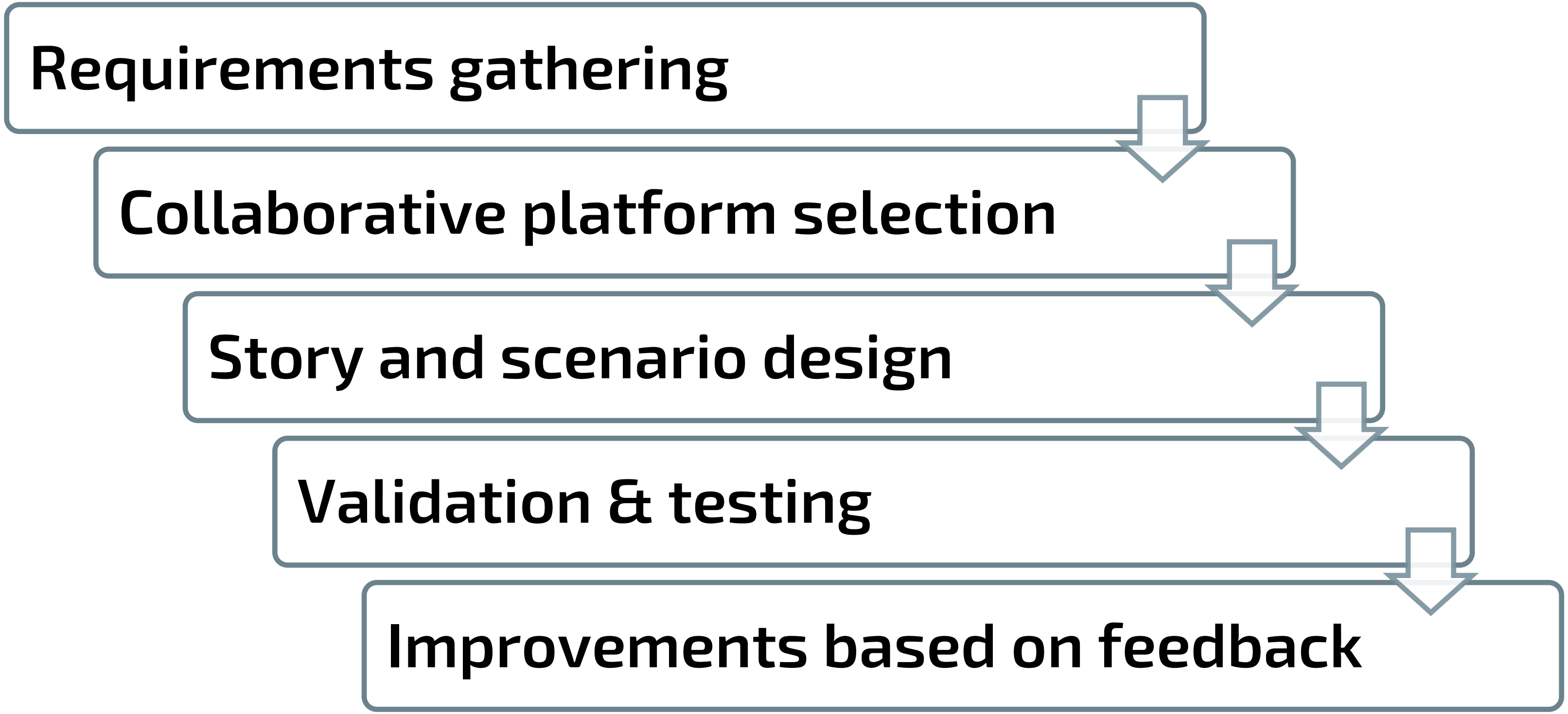
ARMY CYBER INSTITUTE AT WEST POINT

NATIONAL CYBERSECURITY PREPAREDNESS CONSORTIUM

- Built by Norwich University Applied Research Institute
- Funding by USA DHS: USD 18.7 million in 12 years

The Big4 have their own platform → pwc EY Deloitte. KPMG

What about a low-cost version?



Requirements gathering

Collaborative platform selection

Story and scenario design

Validation & testing

Improvements based on feedback

Idea validation

Education

- Students in university courses

Cybersecurity community

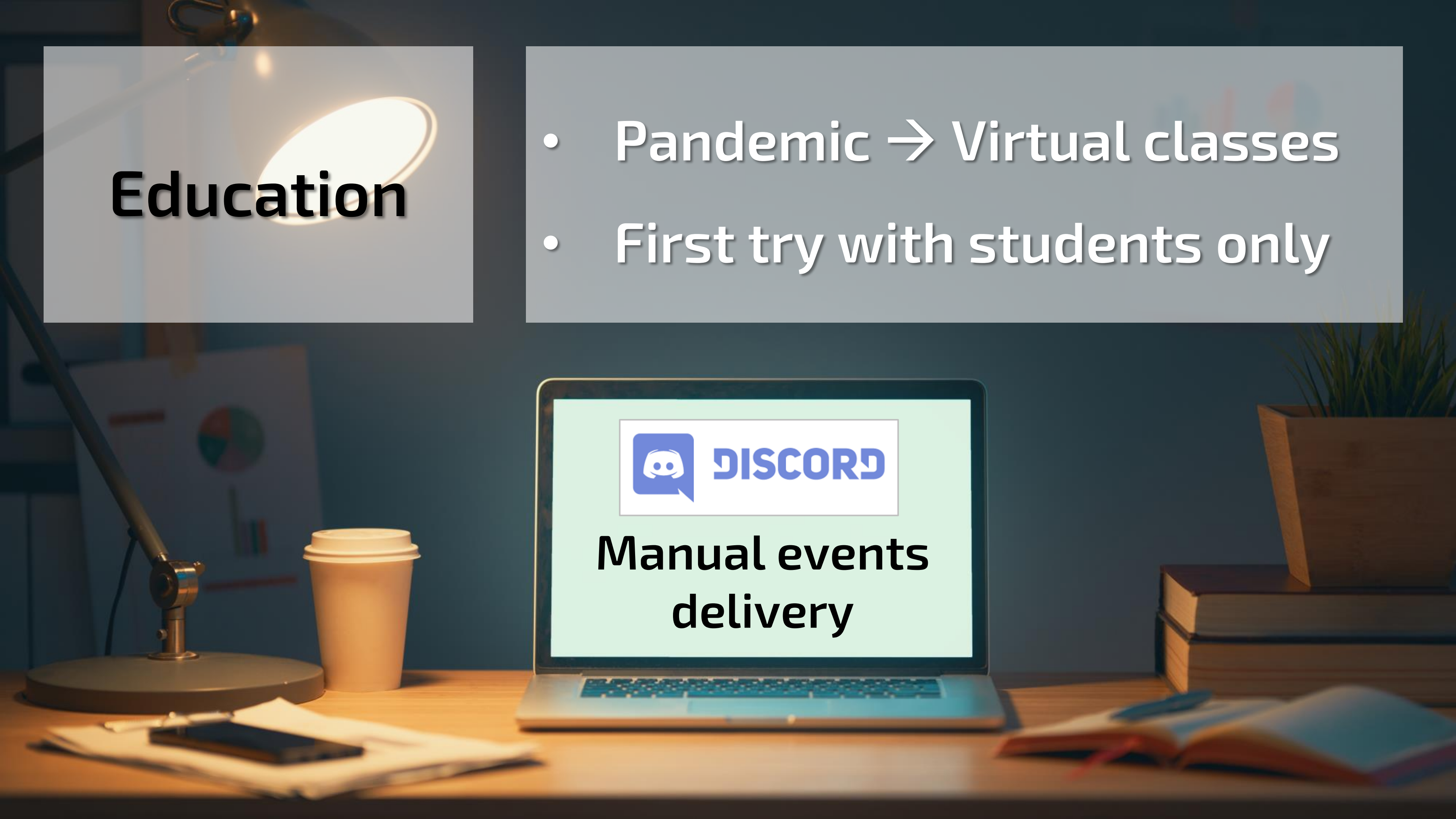
- Colleagues and alumni

Cybersecurity industry

- International companies

Education

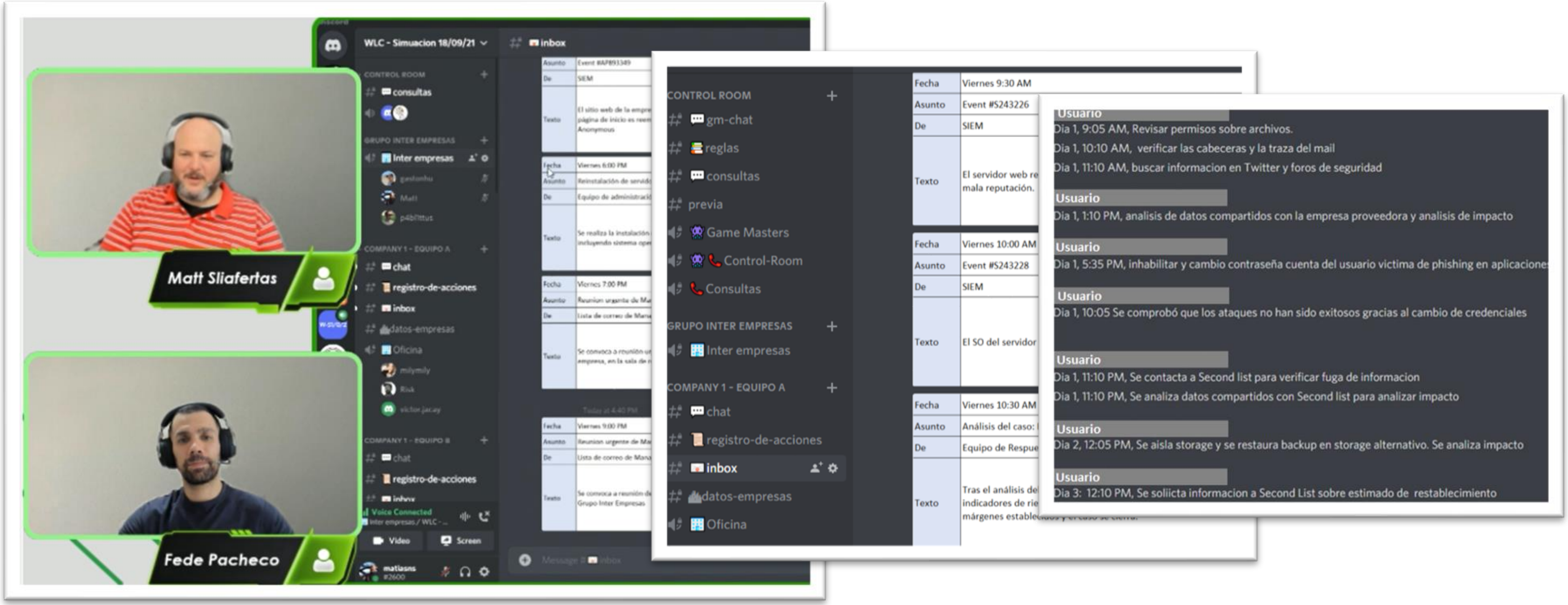
- Pandemic → Virtual classes
- First try with students only



DISCORD

Manual events delivery

Cybersecurity Community



Asunto	Event #AP893349
De	SIEM
Texto	El sitio web de la empre página de inicio es reem Anonymous

Fecha	Viernes 6:00 PM
Asunto	Reinstalación de servid
De	Equipo de administració
Texto	Se realiza la instalación incluyendo sistema ope

Fecha	Viernes 7:00 PM
Asunto	Reunion urgente de Ma
De	Lista de correo de Mana
Texto	Se convoca a reunión u empresa, en la sala de r

Today at 4:40 PM

Fecha	Viernes 9:00 PM
Asunto	Reunion urgente de Ma
De	Usta de correo de Mana
Texto	Se convoca a reunión d Grupo Inter Empresas

Fecha	Viernes 9:30 AM
Asunto	Event #S243226
De	SIEM
Texto	El servidor web re mala reputación.

Fecha	Viernes 10:00 AM
Asunto	Event #S243228
De	SIEM
Texto	El SO del servidor

Fecha	Viernes 10:30 AM
Asunto	Análisis del caso:
De	Equipo de Respue
Texto	Tras el análisis de indicadores de rie márgenes establecidos y el caso se cierra.

Usuario

Dia 1, 9:05 AM, Revisar permisos sobre archivos.

Dia 1, 10:10 AM, verificar las cabeceras y la traza del mail

Dia 1, 11:10 AM, buscar informacion en Twitter y foros de seguridad

Usuario

Dia 1, 1:10 PM, analisis de datos compartidos con la empresa proveedora y analisis de impacto

Usuario

Dia 1, 5:35 PM, inhabilitar y cambio contraseña cuenta del usuario victima de phishing en aplicaciones

Usuario

Dia 1, 10:05 Se comprobó que los ataques no han sido exitosos gracias al cambio de credenciales

Usuario

Dia 1, 11:10 PM, Se contacta a Second list para verificar fuga de informacion

Dia 1, 11:10 PM, Se analiza datos compartidos con Second list para analizar impacto

Usuario

Dia 2, 12:05 PM, Se aisla storage y se restaura backup en storage alternativo. Se analiza impacto

Usuario

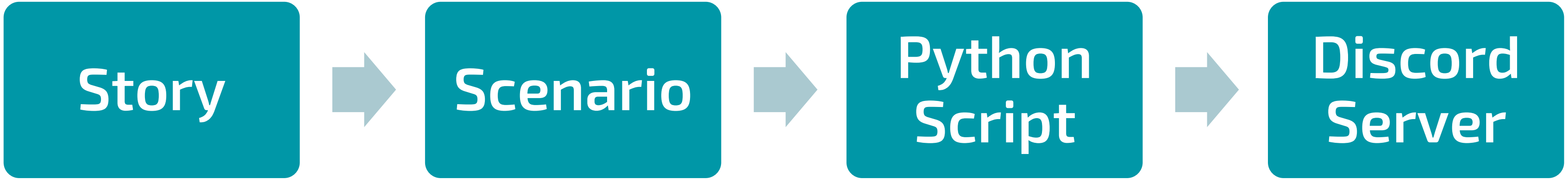
Dia 3: 12:10 PM, Se soliicta informacion a Second List sobre estimado de restablecimiento

Full session (in Spanish): www.twitch.tv/videos/1152676115

Automated events delivery

BORIS

(Bot para Orquestación de Respuesta a Incidentes de Seguridad)



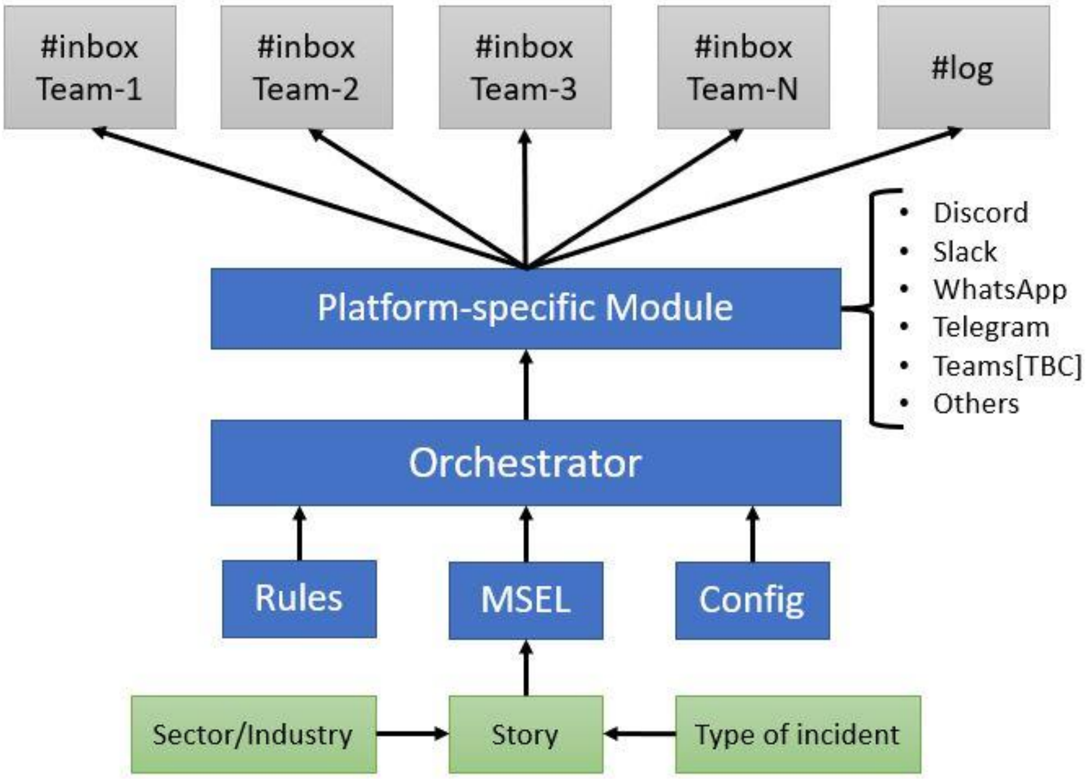
Story → Scenario → Python Script → Discord Server

v1.0: multiplatform orchestration

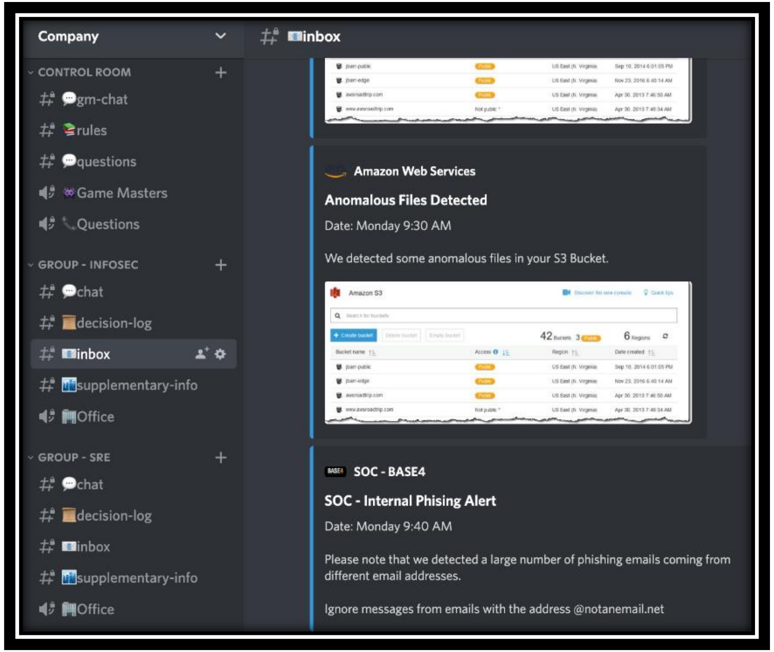
BASE4 SECURITY

T3SF

- **Technical**
- **Table**
- **Top**
- **Simulation**
- **Framework**



Example: Discord and Slack



Amazon Web Services

Anomalous Files Detected

Date: Monday 9:30 AM

We detected some anomalous files in your S3 Bucket.

Amazon S3

Bucket name	Access	Region	Date created
jbarr-public	Public	US East (N. Virginia)	Sep 10, 2014 6:01:05 PM
jbarr-edge	Public	US East (N. Virginia)	Nov 23, 2016 6:40:14 AM
awsroadtrip.com	Public	US East (N. Virginia)	Apr 30, 2013 7:46:50 AM
www.awsroadtrip.com	Not public *	US East (N. Virginia)	Apr 30, 2013 7:49:34 AM

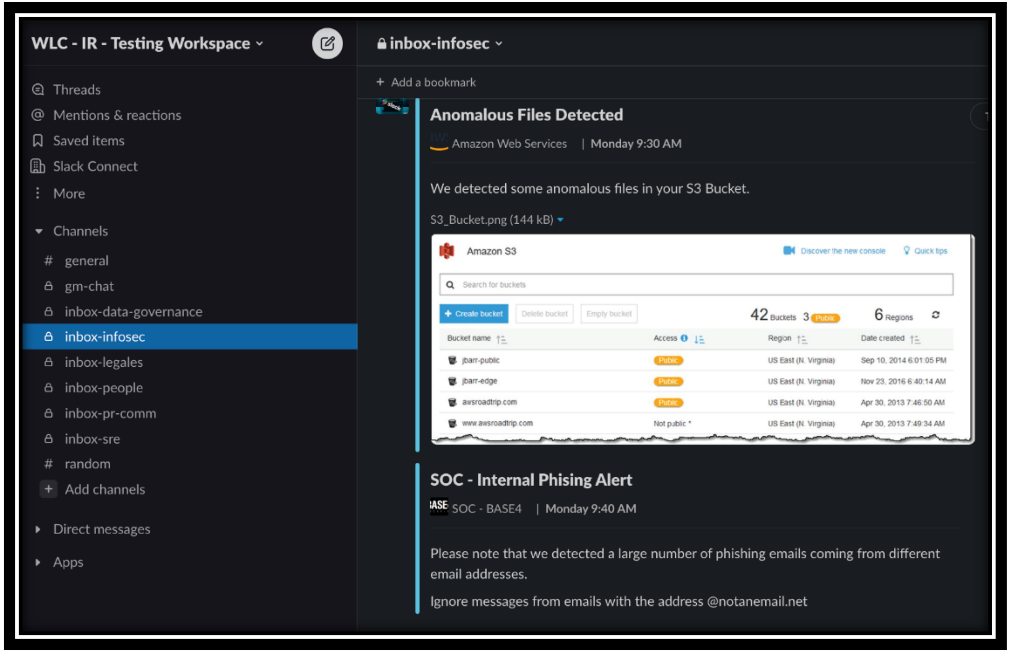
SOC - BASE4

SOC - Internal Phising Alert

Date: Monday 9:40 AM

Please note that we detected a large number of phishing emails coming from different email addresses.

Ignore messages from emails with the address @notanemail.net



Anomalous Files Detected

Amazon Web Services | Monday 9:30 AM

We detected some anomalous files in your S3 Bucket.

S3_Bucket.png (144 kB)

Amazon S3

Bucket name	Access	Region	Date created
jbarr-public	Public	US East (N. Virginia)	Sep 10, 2014 6:01:05 PM
jbarr-edge	Public	US East (N. Virginia)	Nov 23, 2016 6:40:14 AM
awsroadtrip.com	Public	US East (N. Virginia)	Apr 30, 2013 7:46:50 AM
www.awsroadtrip.com	Not public *	US East (N. Virginia)	Apr 30, 2013 7:49:34 AM

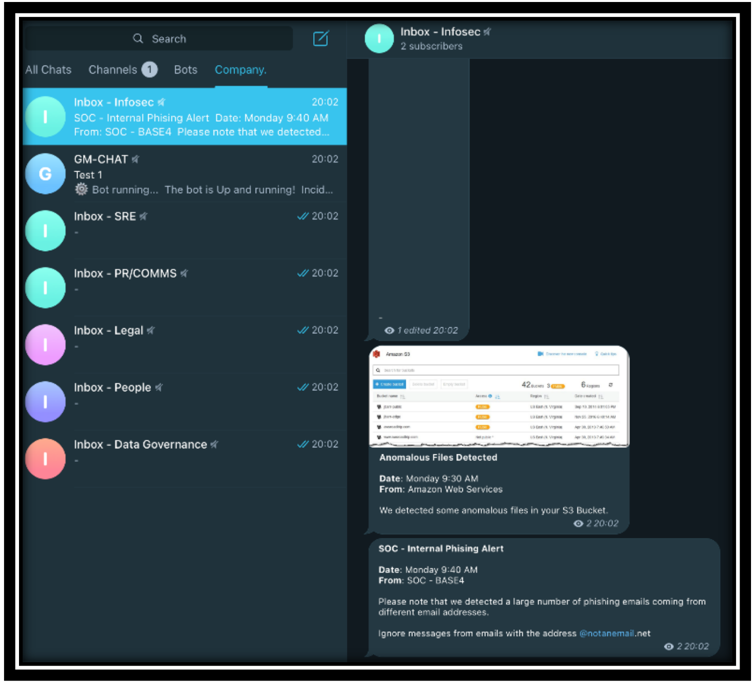
SOC - Internal Phising Alert

SOC - BASE4 | Monday 9:40 AM

Please note that we detected a large number of phishing emails coming from different email addresses.

Ignore messages from emails with the address @notanemail.net

Example: Telegram and WhatsApp



Inbox - Infosec 20:02
SOC - Internal Phising Alert Date: Monday 9:40 AM From: SOC - BASE4 Please note that we detected...

GM-CHAT 20:02
Test 1
⚙ Bot running... The bot is Up and running! Incid...

Inbox - SRE ✓✓ 20:02
-

Inbox - PR/COMMS ✓✓ 20:02
-

Inbox - Legal ✓✓ 20:02
-

Inbox - People ✓✓ 20:02
-

Inbox - Data Governance ✓✓ 20:02
-

Inbox - Infosec
2 subscribers

1 edited 20:02

Anomalous Files Detected

Date: Monday 9:30 AM
From: Amazon Web Services

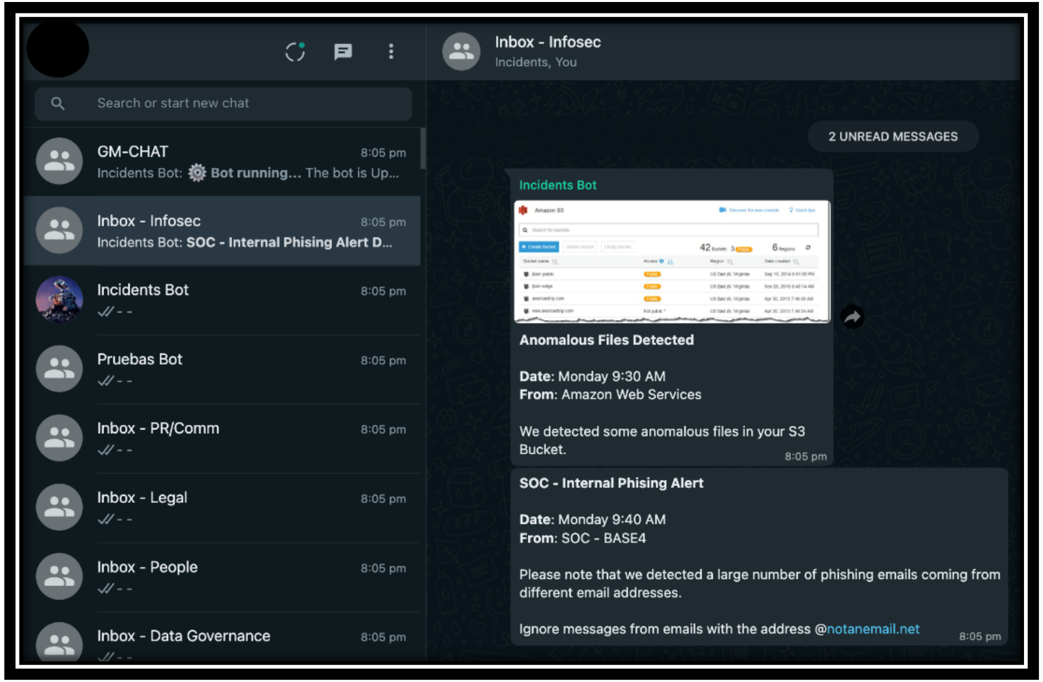
We detected some anomalous files in your S3 Bucket.
2 20:02

SOC - Internal Phising Alert

Date: Monday 9:40 AM
From: SOC - BASE4

Please note that we detected a large number of phishing emails coming from different email addresses.

Ignore messages from emails with the address @notanemail.net
2 20:02



GM-CHAT 8:05 pm
Incidents Bot: ⚙ **Bot running...** The bot is Up...

Inbox - Infosec 8:05 pm
Incidents Bot: **SOC - Internal Phising Alert D...**

Incidents Bot 8:05 pm
✓✓ - -

Pruebas Bot 8:05 pm
✓✓ - -

Inbox - PR/Comm 8:05 pm
✓✓ - -

Inbox - Legal 8:05 pm
✓✓ - -

Inbox - People 8:05 pm
✓✓ - -

Inbox - Data Governance 8:05 pm
✓✓ - -

Inbox - Infosec
Incidents, You

2 UNREAD MESSAGES

Incidents Bot

Anomalous Files Detected

Date: Monday 9:30 AM
From: Amazon Web Services

We detected some anomalous files in your S3 Bucket.
8:05 pm

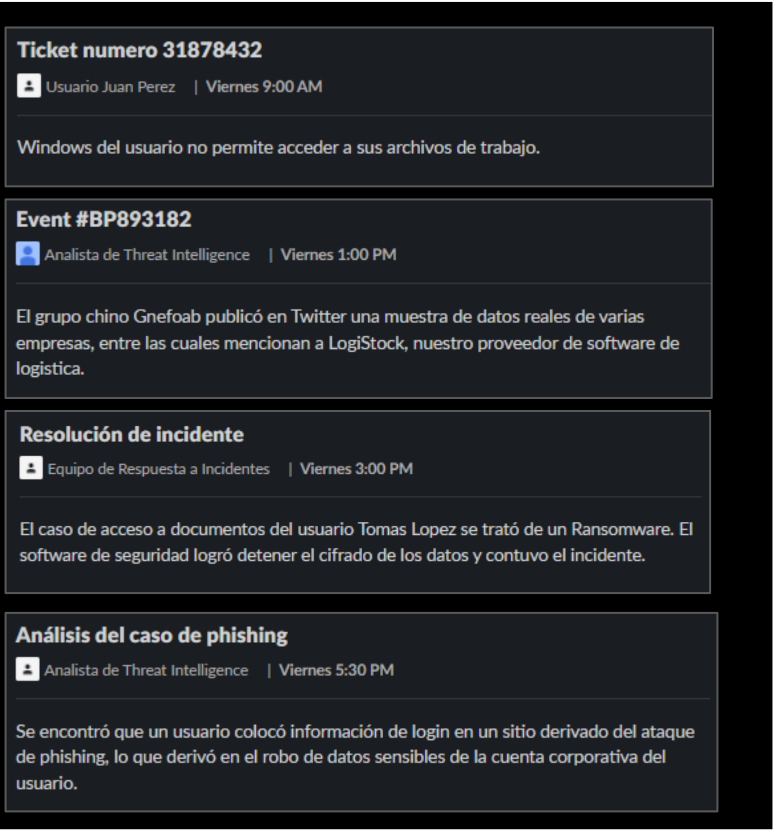
SOC - Internal Phising Alert

Date: Monday 9:40 AM
From: SOC - BASE4

Please note that we detected a large number of phishing emails coming from different email addresses.

Ignore messages from emails with the address @notanemail.net
8:05 pm

#inbox-Cybersecurity



Ticket numero 31878432

Usuario Juan Perez | Viernes 9:00 AM

Windows del usuario no permite acceder a sus archivos de trabajo.

Event #BP893182

Analista de Threat Intelligence | Viernes 1:00 PM

El grupo chino Gnefoab publicó en Twitter una muestra de datos reales de varias empresas, entre las cuales mencionan a LogiStock, nuestro proveedor de software de logistica.

Resolución de incidente

Equipo de Respuesta a Incidentes | Viernes 3:00 PM

El caso de acceso a documentos del usuario Tomas Lopez se trató de un Ransomware. El software de seguridad logró detener el cifrado de los datos y contuvo el incidente.

Análisis del caso de phishing

Analista de Threat Intelligence | Viernes 5:30 PM

Se encontró que un usuario colocó información de login en un sitio derivado del ataque de phishing, lo que derivó en el robo de datos sensibles de la cuenta corporativa del usuario.

#chat-Cybersecurity

Ernesto: this does not seem like a normal incident. I suggest we investigate further

Federico: I agree, let's see what the infrastructure people tell us

.

.

Ernesto: ok, who can ask?

Ana: I’m on it

.

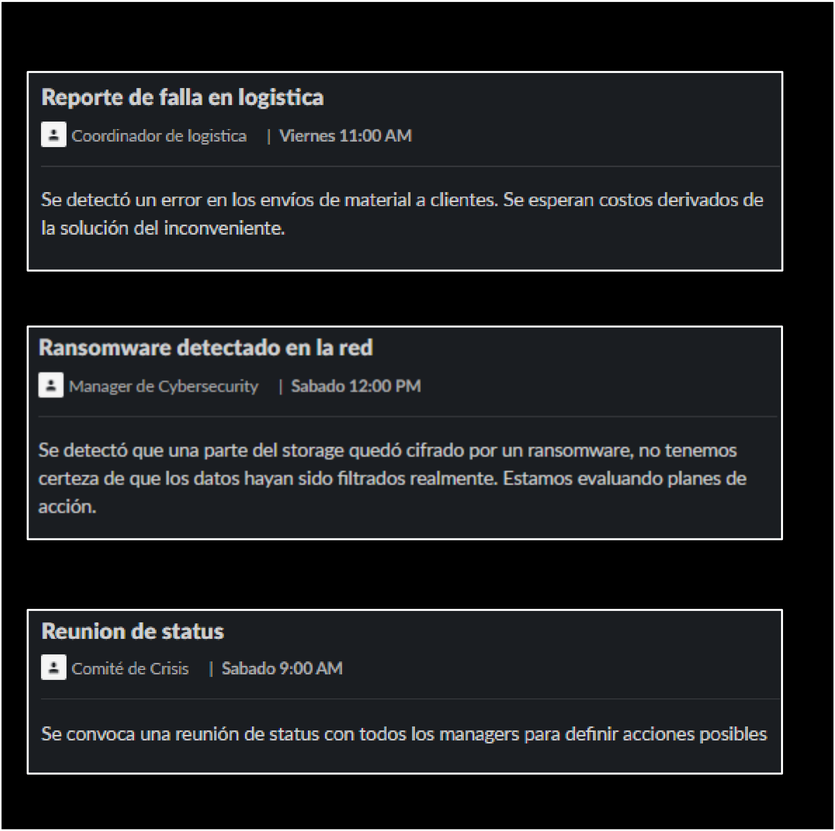
.

.

Joaquin: I think we have a problem

Ana: we must talk to Legal

#inbox-Legal&Compliance



Reporte de falla en logistica

Coordinador de logistica | Viernes 11:00 AM

Se detectó un error en los envíos de material a clientes. Se esperan costos derivados de la solución del inconveniente.

Ransomware detectado en la red

Manager de Cybersecurity | Sabado 12:00 PM

Se detectó que una parte del storage quedó cifrado por un ransomware, no tenemos certeza de que los datos hayan sido filtrados realmente. Estamos evaluando planes de acción.

Reunion de status

Comité de Crisis | Sabado 9:00 AM

Se convoca una reunión de status con todos los managers para definir acciones posibles

#chat-Legal&Compliance

Vanesa: Can this cause a bigger issue?

Carlos: We will be exposed to regulatory risk if we don’t act quickly

Cristina: Let’s ask about the technical scope to cybersecurity

Carlos: let’s see if PR can make a formal communication

Vanesa: yes, that’s the right choice

Cristina: we can’t waste more time

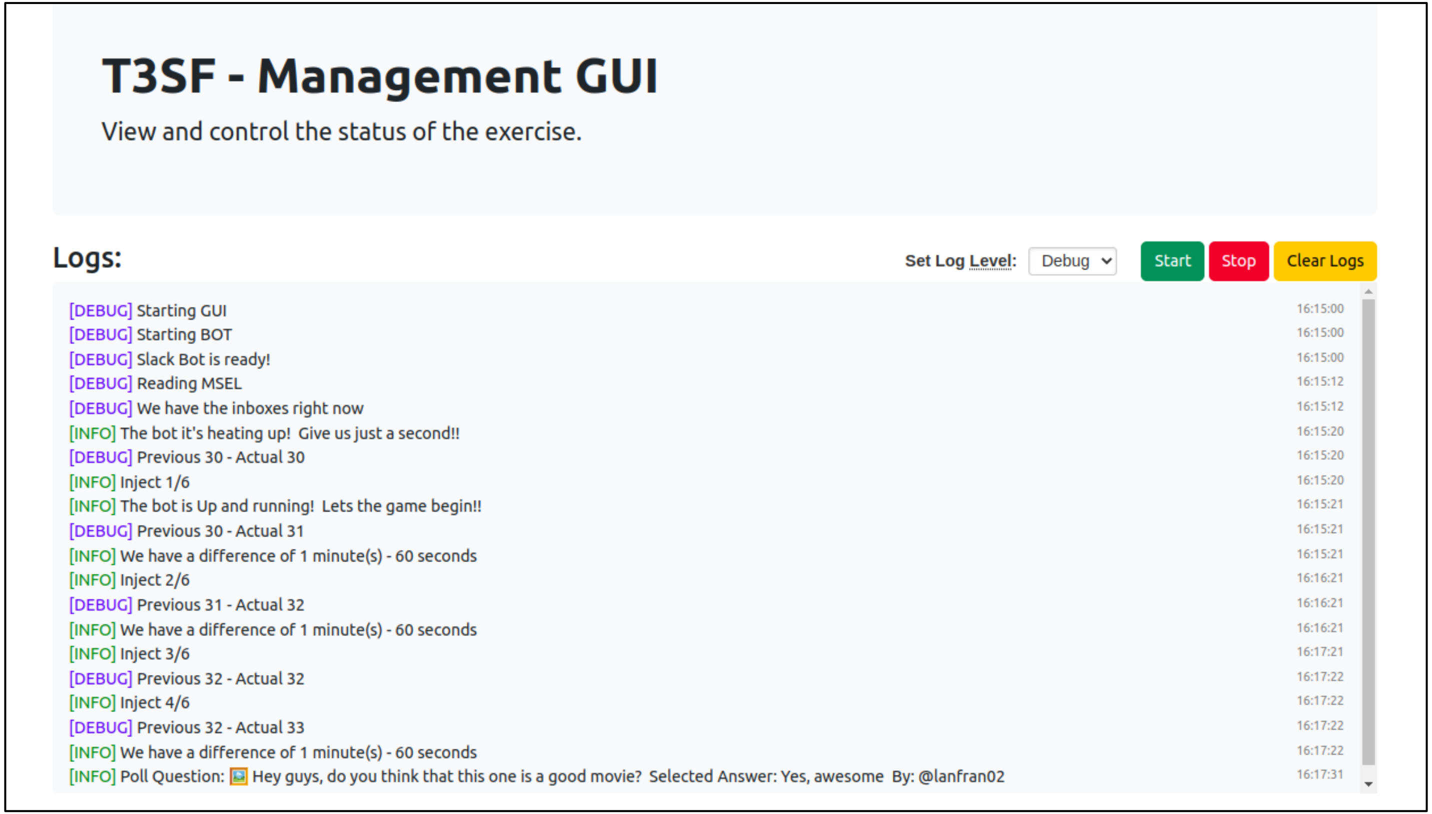
Vanesa: let’s take this to the committee

Open TTX in Hybrid mode

EKOPARTY
ENTER THE METAVERSE
2022

Ekoparty Security Conference 2022

v1.2: GUI + more features



T3SF - Management GUI

View and control the status of the exercise.

Logs:

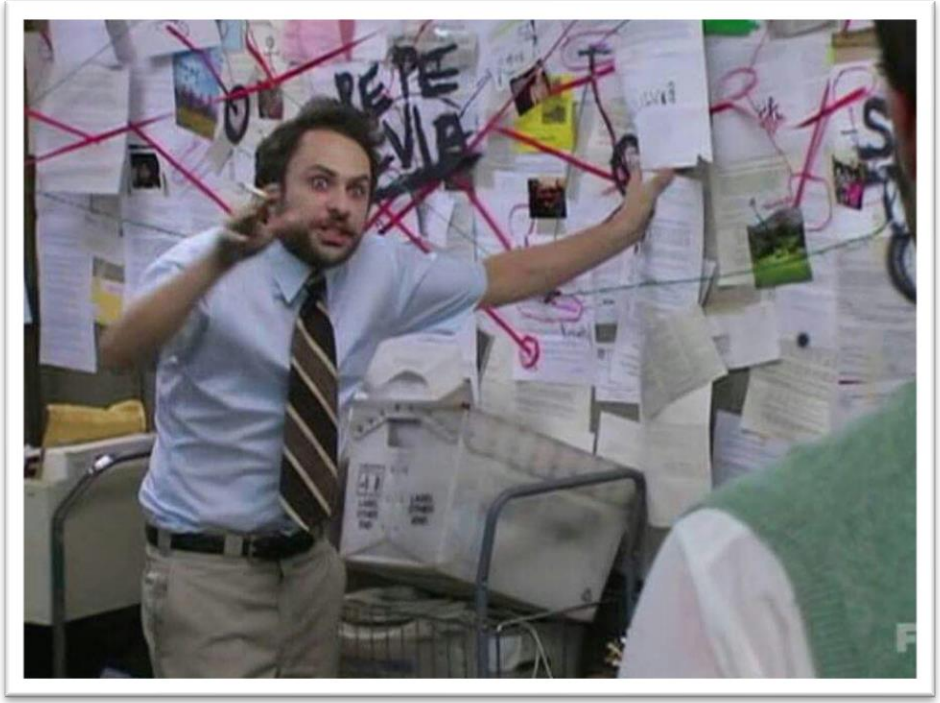
Set Log Level: Debug

```
[DEBUG] Starting GUI                                                                          16:15:00
[DEBUG] Starting BOT                                                                          16:15:00
[DEBUG] Slack Bot is ready!                                                                   16:15:00
[DEBUG] Reading MSEL                                                                          16:15:12
[DEBUG] We have the inboxes right now                                                         16:15:12
[INFO] The bot it's heating up!  Give us just a second!!                                      16:15:20
[DEBUG] Previous 30 - Actual 30                                                               16:15:20
[INFO] Inject 1/6                                                                             16:15:20
[INFO] The bot is Up and running!  Lets the game begin!!                                      16:15:21
[DEBUG] Previous 30 - Actual 31                                                               16:15:21
[INFO] We have a difference of 1 minute(s) - 60 seconds                                       16:15:21
[INFO] Inject 2/6                                                                             16:16:21
[DEBUG] Previous 31 - Actual 32                                                               16:16:21
[INFO] We have a difference of 1 minute(s) - 60 seconds                                       16:16:21
[INFO] Inject 3/6                                                                             16:17:21
[DEBUG] Previous 32 - Actual 32                                                               16:17:22
[INFO] Inject 4/6                                                                             16:17:22
[DEBUG] Previous 32 - Actual 33                                                               16:17:22
[INFO] We have a difference of 1 minute(s) - 60 seconds                                       16:17:22
[INFO] Poll Question: 🖼 Hey guys, do you think that this one is a good movie?  Selected Answer: Yes, awesome  By: @lanfran02   16:17:31
```

Not so fast...

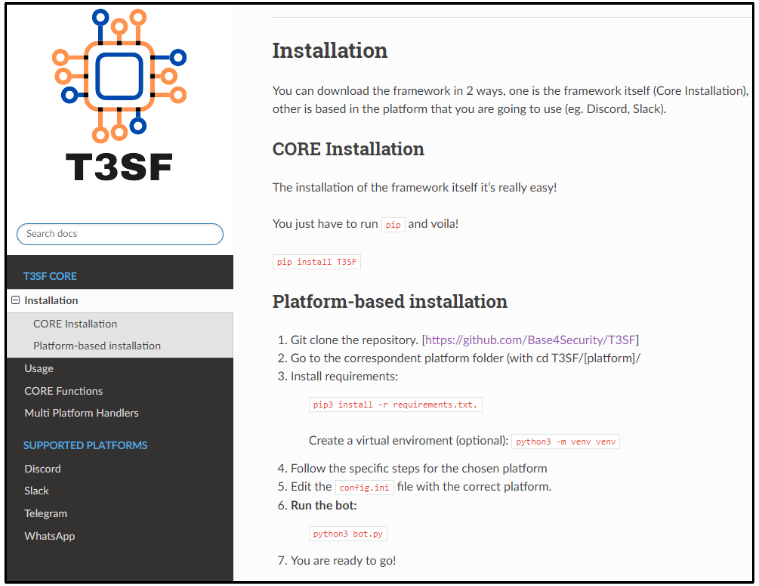
BASE4 SECURITY

How to convince the CEO to make it Open Source



Documentation and Source Code

BASE4 SECURITY



Installation

You can download the framework in 2 ways, one is the framework itself (Core Installation), other is based in the platform that you are going to use (eg. Discord, Slack).

CORE Installation

The installation of the framework itself it's really easy!

You just have to run `pip` and voila!

```
pip install T3SF
```

Platform-based installation

1. Git clone the repository. [https://github.com/Base4Security/T3SF]
2. Go to the correspondent platform folder (with cd T3SF/[platform]/
3. Install requirements:

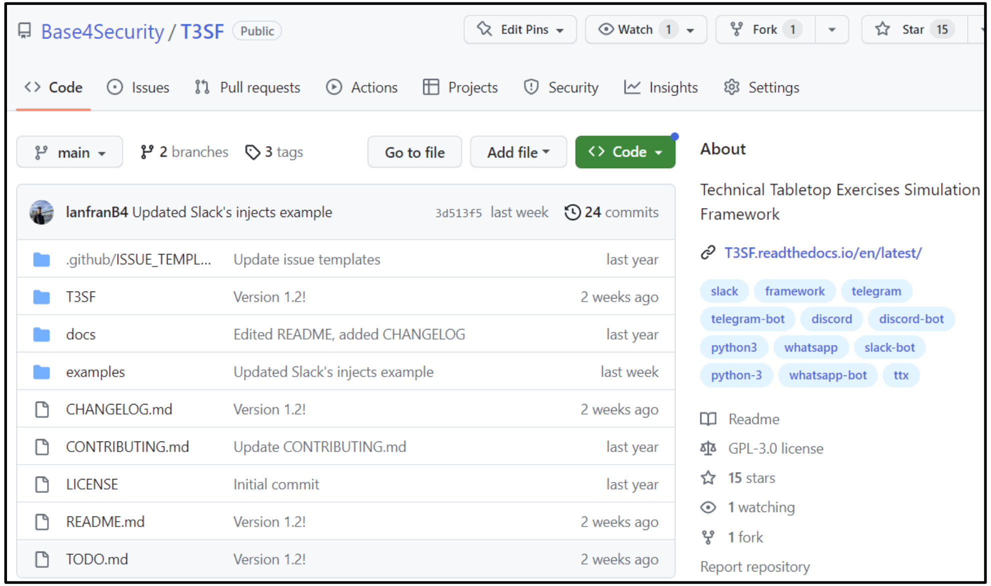
   ```
   pip3 install -r requirements.txt.
   ```

   Create a virtual enviroment (optional): `python3 -m venv venv`

4. Follow the specific steps for the chosen platform
5. Edit the `config.ini` file with the correct platform.
6. **Run the bot:**

   ```
   python3 bot.py
   ```

7. You are ready to go!



lanfranB4 Updated Slack's injects example 3d513f5 last week 24 commits

.github/ISSUE_TEMPL...	Update issue templates	last year
T3SF	Version 1.2!	2 weeks ago
docs	Edited README, added CHANGELOG	last year
examples	Updated Slack's injects example	last week
CHANGELOG.md	Version 1.2!	2 weeks ago
CONTRIBUTING.md	Update CONTRIBUTING.md	last year
LICENSE	Initial commit	last year
README.md	Version 1.2!	2 weeks ago
TODO.md	Version 1.2!	2 weeks ago

About

Technical Tabletop Exercises Simulation Framework

T3SF.readthedocs.io/en/latest/

slack framework telegram telegram-bot discord discord-bot python3 whatsapp slack-bot python-3 whatsapp-bot ttx

Readme

GPL-3.0 license

15 stars

1 watching

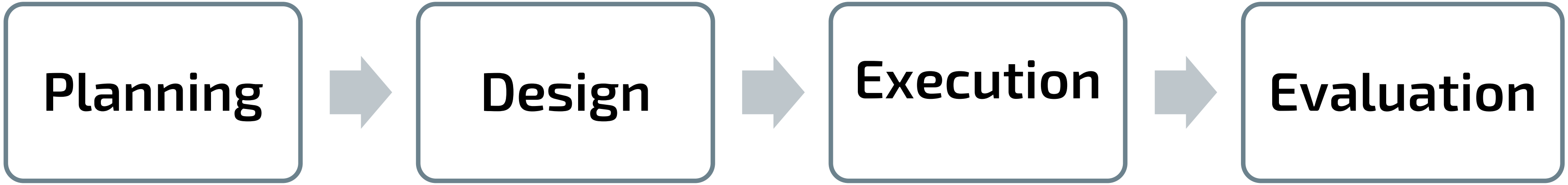
1 fork

Report repository

https://t3sf.readthedocs.io

https://github.com/Base4Security/T3SF

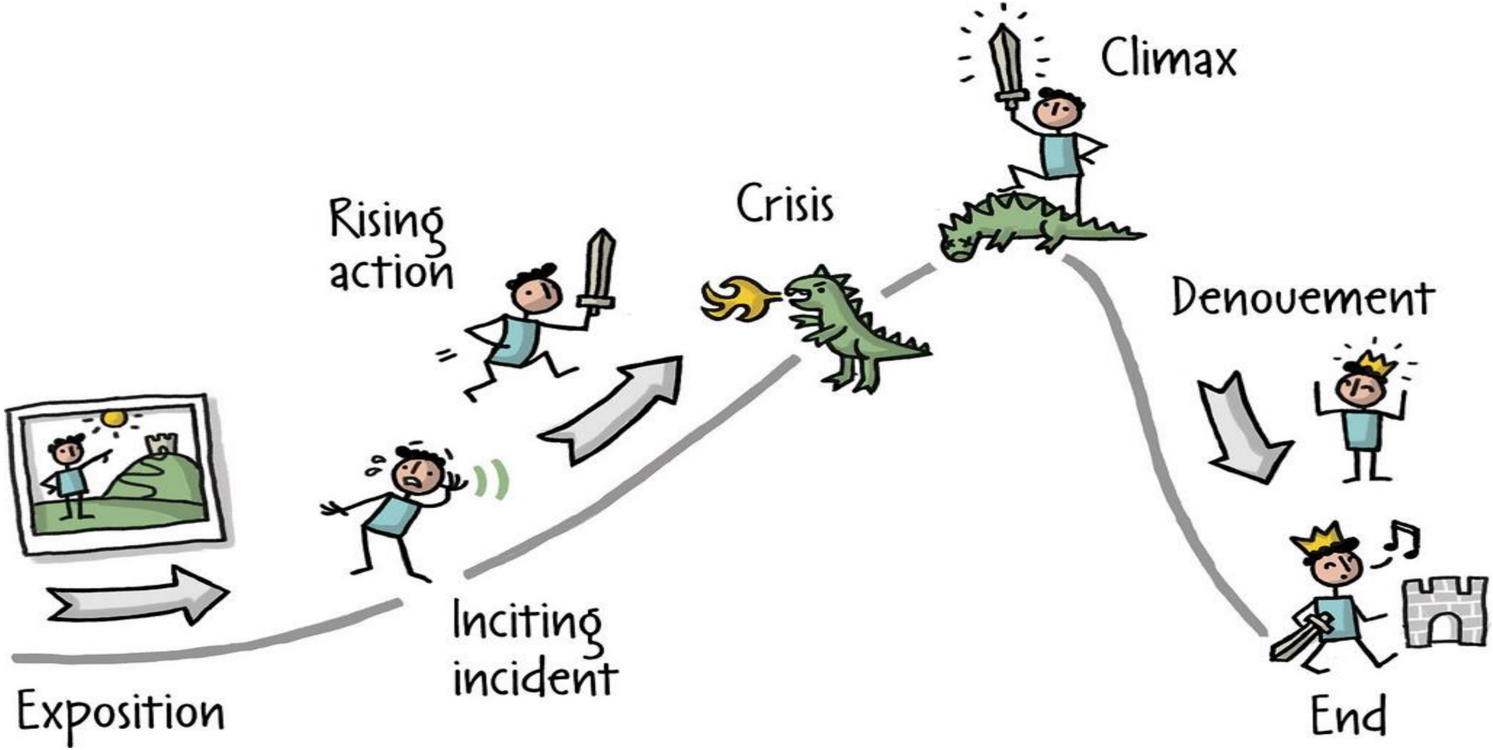
Methodology



Deliverables

- Initial planning
- Welcome Package
- Detailed results report
- Executive summary

The Story: our IR Hero Journey



Upcoming features

BASE4 SECURITY

- GUI for automated platform channels creation
- Scenarios and injects database (based on OpenAI)
- Full compatibility with the main platforms
- Integration with technical emulation tests

Lessons learned

- TTXs proved to help enhance IR capabilities
- TTXs work for (almost) any kind of organization
- Traditional mode is still the most common choice
- TTXs coordination is a fine art
- The human factor is key: Communication problems
- People fight the scenarios (mostly tech guys)
- Open-Source tools can help democratization

BASE4 SECURITY

Thanks for your time

FIRST Technical Colloquium 2023

Amsterdam, NL

Federico Pacheco

R+D+i Manager

fpacheco@base4sec.com

@FedeQuark