



Good Morning!

Weathering the Storm

An Incident Response Tabletop Exercise



Learn about the different **teams** in
information security and **how they**
work together in an interactive exercise.



Company Profile

Apptastic.io

Headquartered in New York, NY

890 Employees


Goal is to build a fully immersive experience in a futuristic cityscape in the metaverse. Users connect to the experience using Hololens™ technology and interact with each other using social credits.

Company wants to rebrand to better align name with mission. It's technology stack is hosted primarily in the cloud on AWS.

Introducing a new immersive virtual
experience by *Apptastic.io*



Meet The Team



Picture of the teacher here

[Teacher's Name]

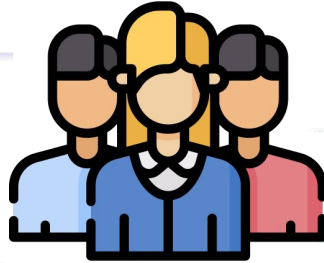
Chief Information Security Officer

Apptastic

Meet The Team



Security Operations



Security Engineering



**Governance, Risk
and Compliance**

Guidelines for the Exercise

- 1) Please stop me and ask questions. We are here to learn.
- 2) After each event (“inject”), we will have a certain number of turns.
- 3) Talk amongst yourselves and share information on your cards.
- 4) Ask questions and have fun!

Are we ready??



Nov 23, 2023 @ 20:03:00 UTC

Security Operations receives an email from AWS Support.

Nov 23, 2023 @ 20:03:00 UTC - The AWS Email

Dear AWS Customer,

As part of our AWS Shield Advanced offering, we noticed a significant volume of traffic against your public Elastic IPs in 226692608800. This is usually indicative of a DDOS attack. We recommend you block all IP addresses identified in the WAF logs.

109.201.133.100

109.70.100.65

185.220.100.243

Please create an AWS Support ticket if you would like to chat with an agent in real time.

Nov 23, 2023 @ 21:15:00 UTC

Security Operations receives an alert from one of the company's Intrusion Detection System (IDS).

Nov 24, 2023 @ 06:02:44 UTC

Several teams notify security@apptastic.io saying that several applications are non-responsive. Application Security team also receives alerts from PagerDuty.

Nov 24, 2023 @ 12:05:30 UTC

More teams notify security@apptastic.io saying that many of the company's internal and external applications are non-responsive. There are some trending topics on social media that report the same.

Nov 24, 2023 @ 12:10:43 UTC

```

cat \\|\\|\\| Warning \\|\\|\\|
!!! Your network is infected by the RTM Locker command!!!
All your documents, photos, reports, customer and employee data, databases and other
important files are encrypted and you cannot decrypt them yourself. They are also on
our servers! But don't worry, we will help you recover all your files!
The only way to recover your files is to buy our dedicated software. Only we can prov
ide you with this software, and only we can recover your files!
We value our reputation. If we do not fulfill our work and obligations, no one will p
ay us. It's not in our interest.
All of our decryption software is perfectly tested and will decrypt your data. We wil
l also provide support in case of problems.

```

To contact us, you need to install TOX (<https://tox.chat/download.html>), write to our support.
Contact: A0FE105A82525ECB94DD2977B4A1F8A5A7CF82F12D720D08C8D9CCA3F98B6F52D911126AC1D

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! Warning!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
If you do not contact the support team within 48 hours, your data will be published i
n the public domain, and compromising data will be sent to your competitors, as well
as to the relevant regulatory authorities.
```

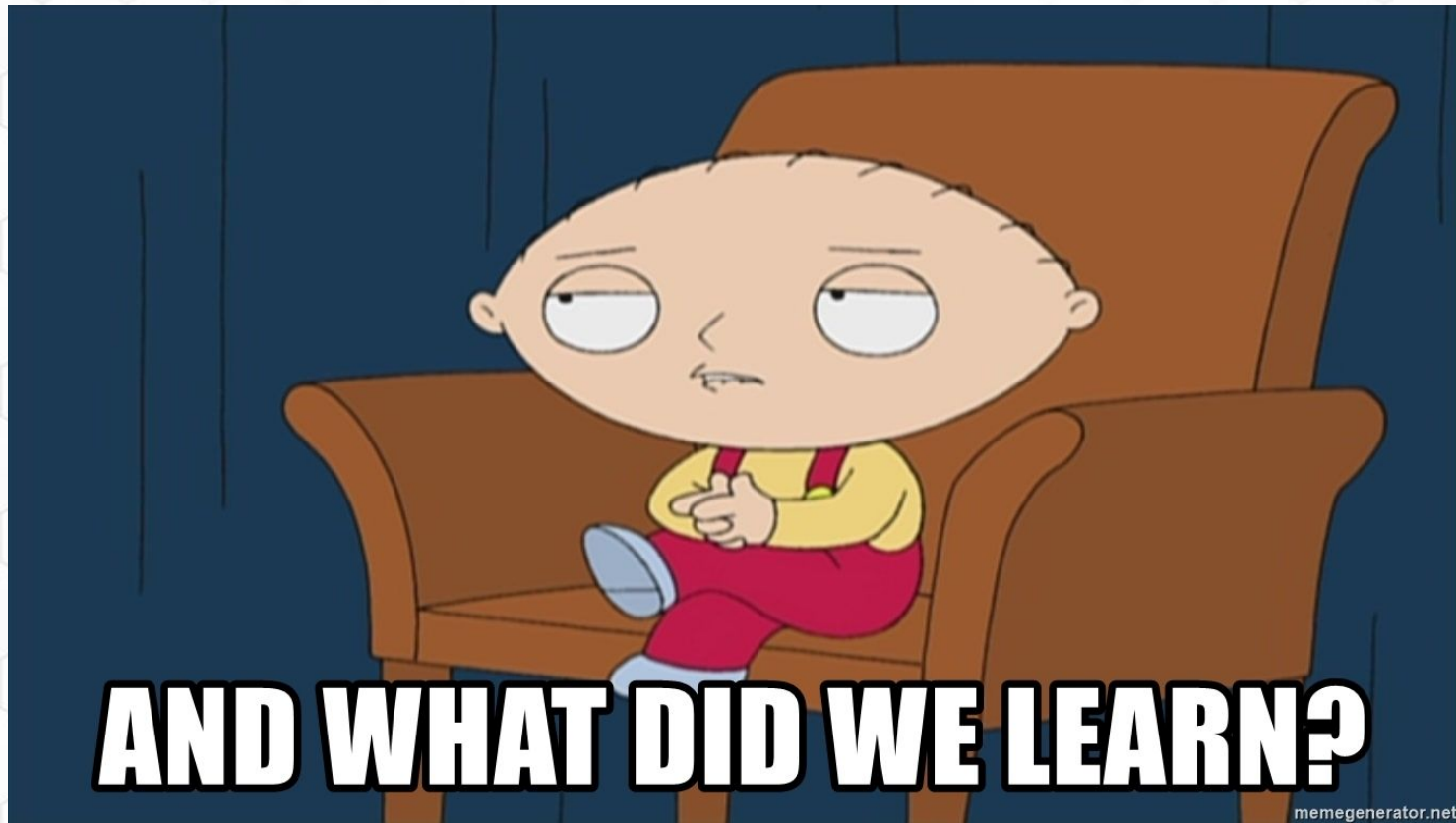
DO NOT ATTEMPT TO RECOVER THE FILES YOURSELF!
DO NOT MODIFY ENCRYPTED FILES!
OTHERWISE YOU MAY LOSE ALL YOUR FILES FOREVER!



EXTRA! EXTRA!

READ ALL ABOUT IT!

**CRISIS
AVERTED**



AND WHAT DID WE LEARN?