
MOZDEVZ
The Cyber Security &
Incident Response Use
Cases Workshop
ATHSec | Computer Emergency
Response Team (0xCERT)
Arlindo Cossa Junior @ ATHSec
© Copyright ATHSec | MSSP

Cyber Talk

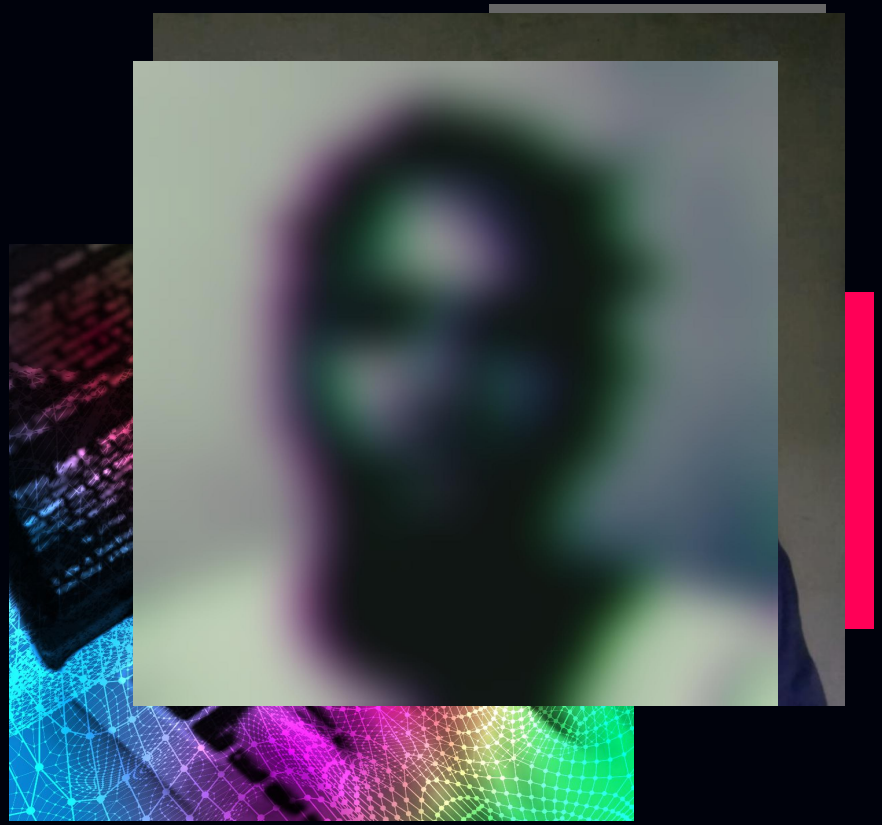
System Owner (T1033)

Arlindo Cossa Junior

@SwagneyCod3

- Head of Security @ ATHSec
- Global Cybersecurity Consultant,
- Specialist & Security Manager @ ATHSec

- **I'm purple wannabe**



Cyber Talk

Your Business Under Our Digital Protection

ATHSec

@athsecacademy

- MSSP | Cyber Security Company
- Managed Detection and Response
- Cyber Security Emergence Response
- Security Operation Center as Service
- Vulnerability Assessments and Penetration Testing
- Information Security Consulting
- etc..

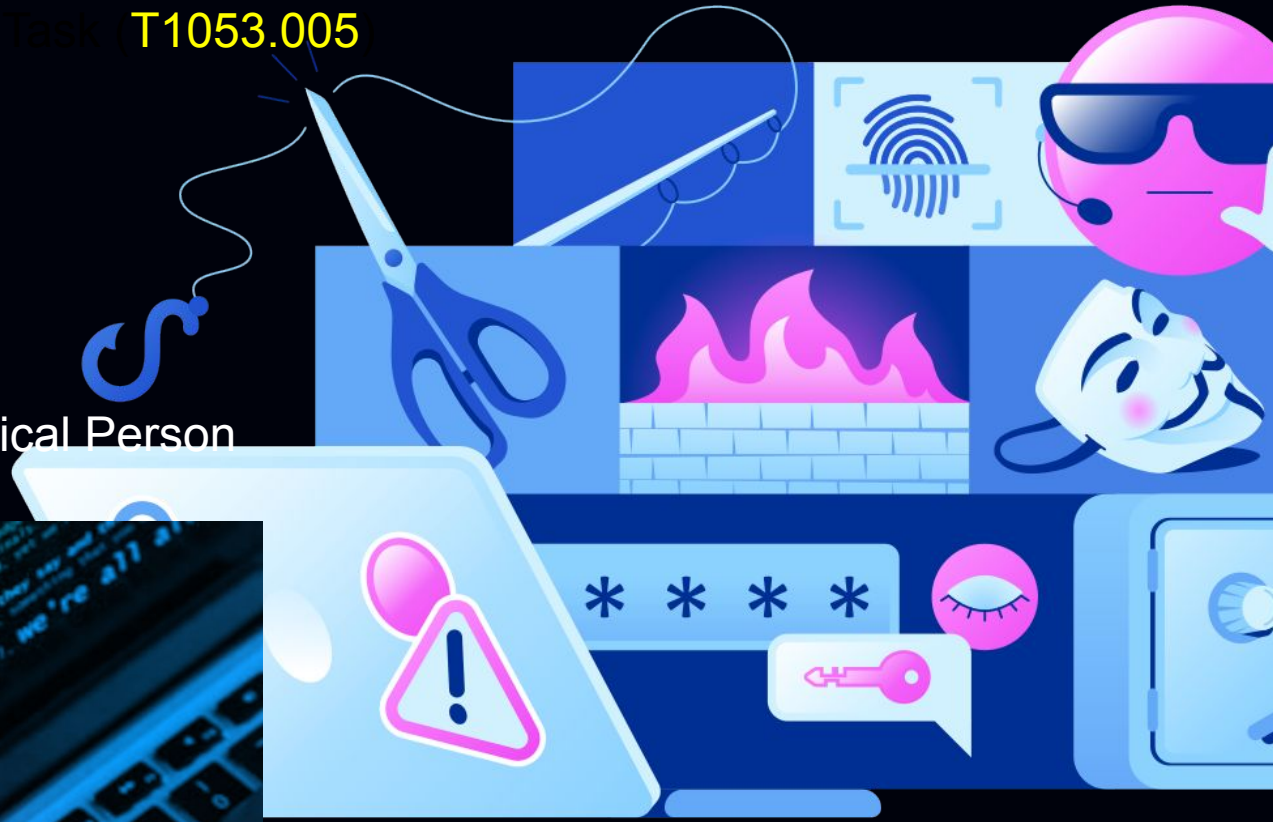
Cyber Talk

ScheduledTask/Job: Scheduled Task (T1053.005)

Agenda

@SwagneyCod3

- Let’s tell about cybersec
- Incident Response Process
- The Use Cases for non Technical Person

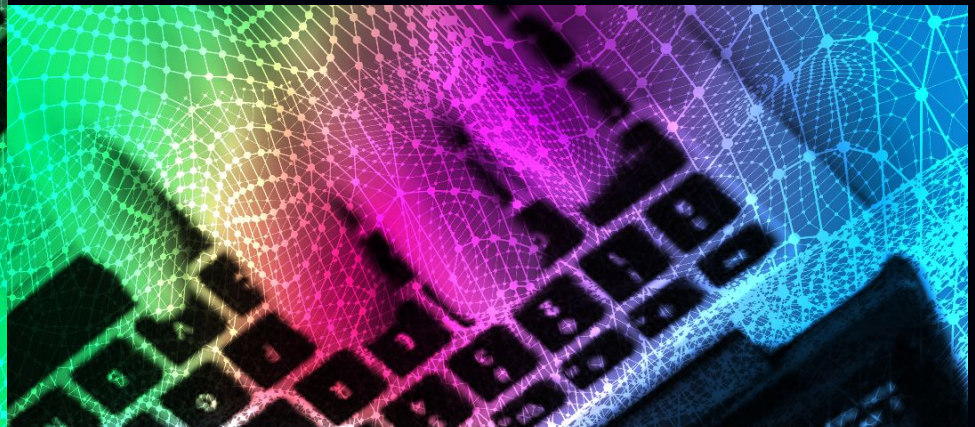


Cyber Talk

Cyber Security is about:

@SwagneyCod3

- Understand the environment
- Reduce the risk
- Reduce the impact
- Etc...



Cyber Talk

Cyber Talk

Technology

Implementation of Technology will depend on people, processes and their strategies

People

Humans are critical to interpreting and acting on technology's advice, which is why they're a huge part of what we do for you.

Process

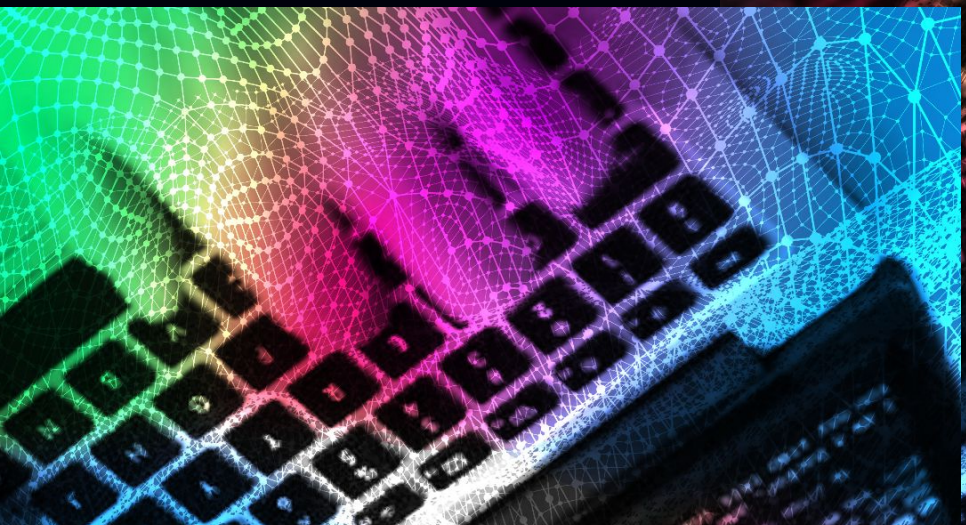
Without implementing sustainable and effective processes, the investments you make in people and technology will only cause more complexity.

Cyber Talk

Incident Response is about:

@SwagneyCod3

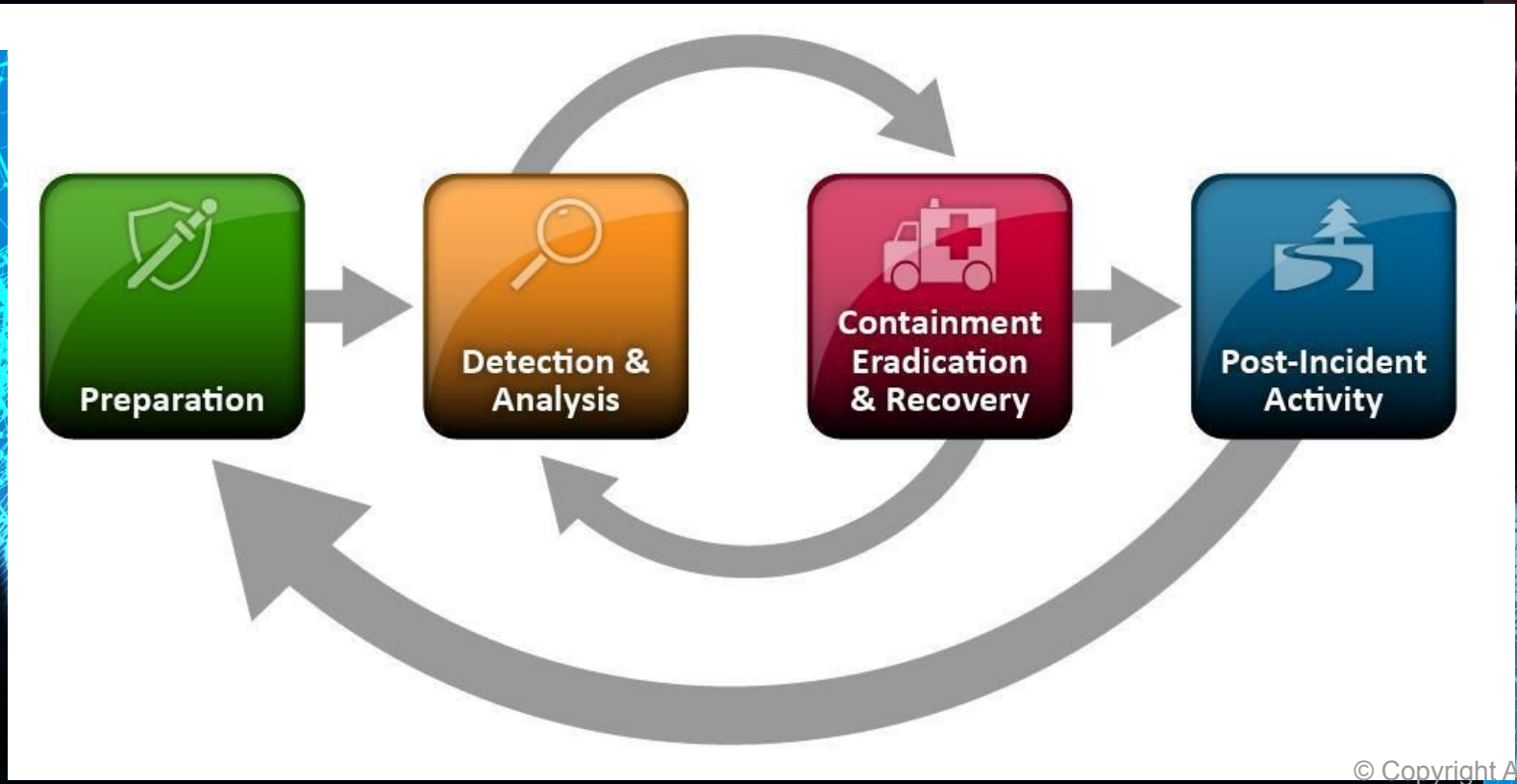
- How do I prepare
- How do I respond
- Mitigate incidents after they happen



Cyber Tall

NIST - Incident Response Life Cycle

@SwagneyCod3



Cyber Talk

How do I prepare ?

Cyber Talk

1.Preparation

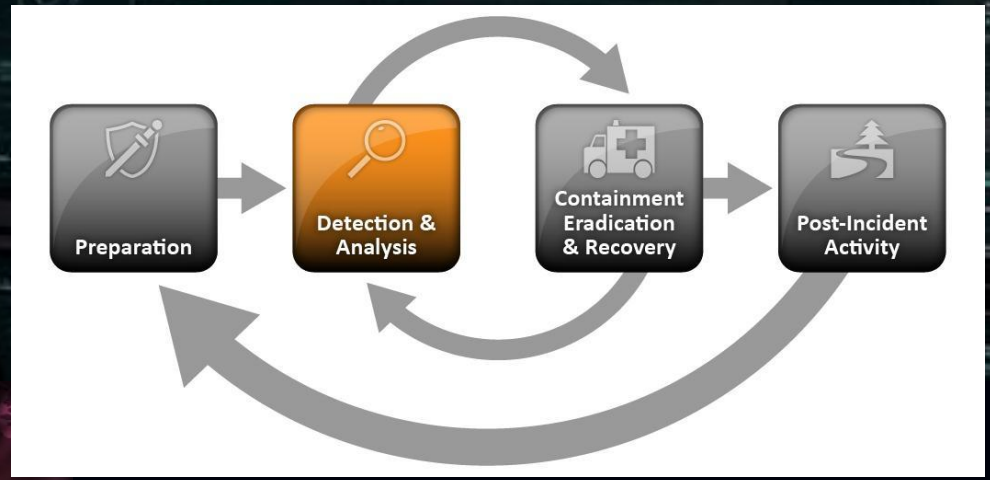
@SwagneyCod3

- Specify the purpose, scope, goals and objectives of incident response plan

Cyber Talk

2.Detect & Analysis

- Setup the monitoring system and Read logs
- Analysis when something's happened

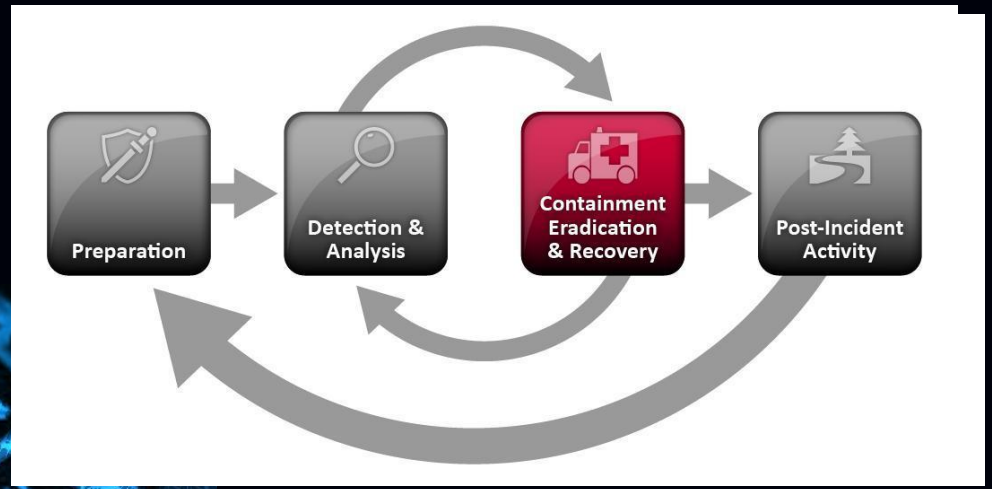


Cyber Talk

3.Containment, Eradication and Recovery

@SwagneyCod3

- Who
- Remove or correct the system
- Operate the system again

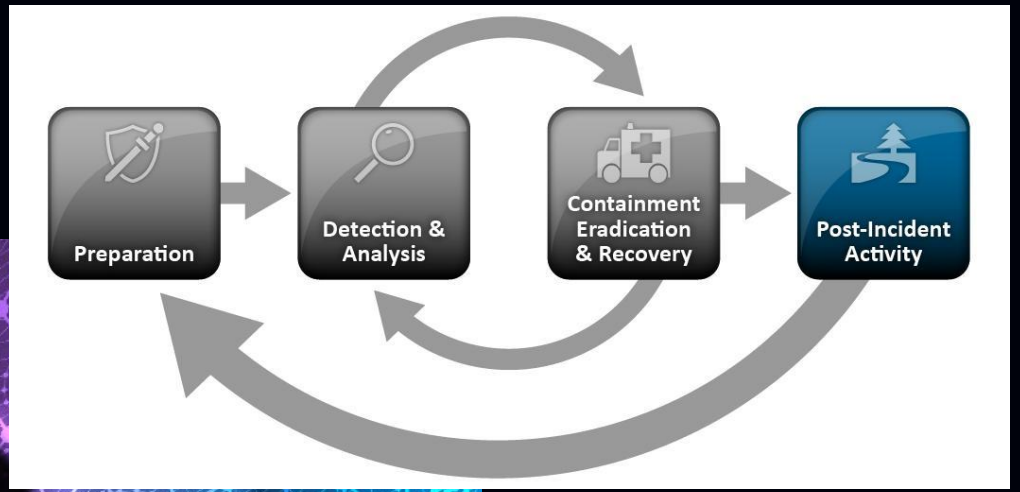


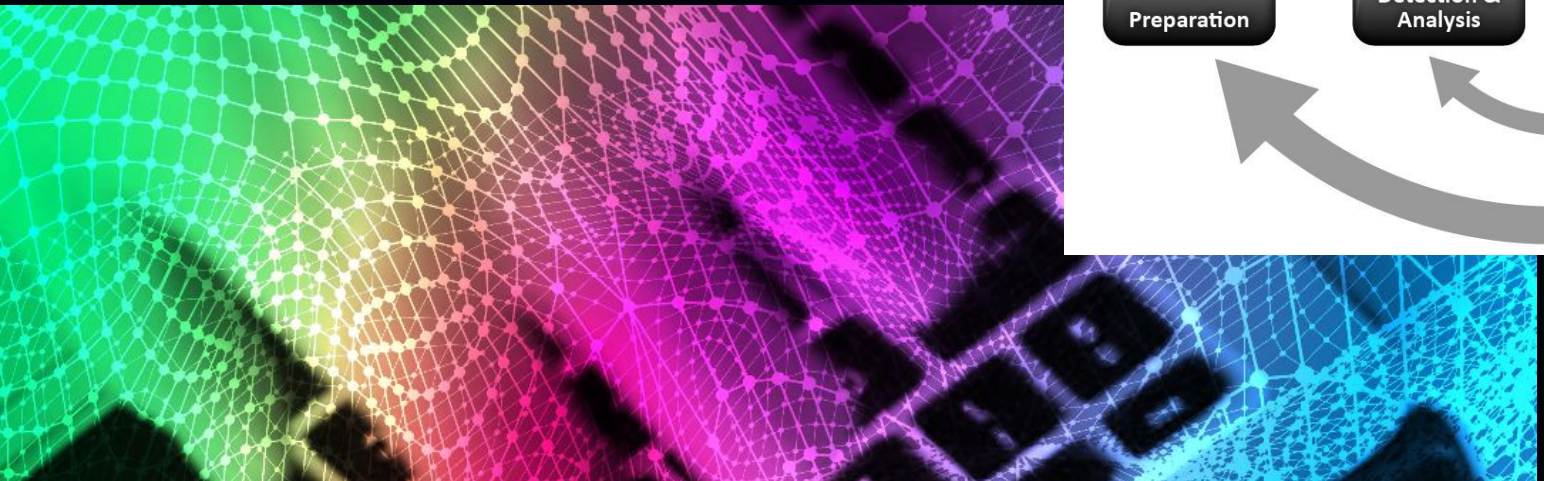
Cyber Talk

4.Post-Incident Activity

@SwagneyCod3

- Lessons Learned
- Prepare the protections
- How to improve



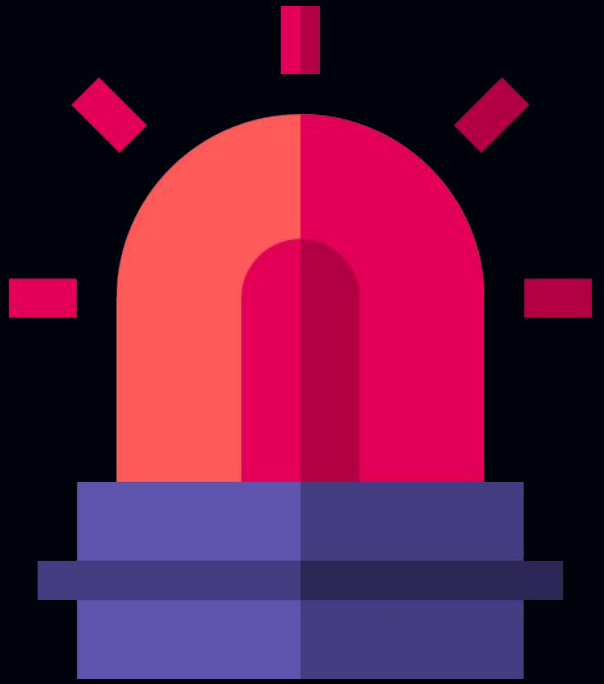


Cyber Talk

5.Communications

@SwagneyCod3

- Define circumstances when employees, customers and partners may or may not be informed of the issue
- Disclosure of incident information should be limited to a need to know basis
- Establish procedures for controlling communication with the media
- Establish procedure for communicating securely during an incident
- Have contact information for the SIRT, vendors contracted to help during a security emergency



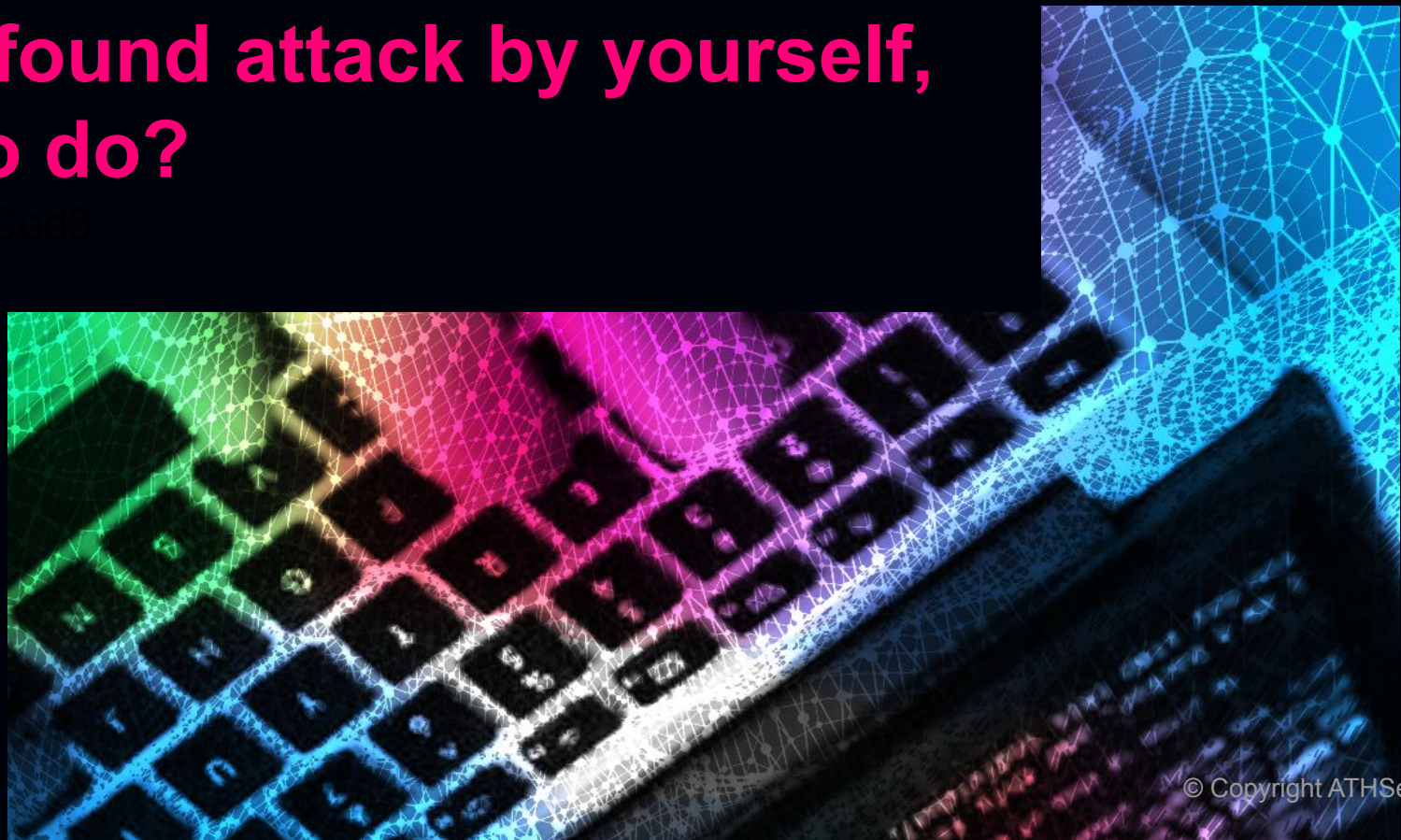

Cyber
Talk
The Use Cases
for non
Technical Person
© Copyright ATHSec | MSSP

What will we do, when incident is occurred?

@SwagneyCod3

If you found attack by yourself, How to do?

@SwagneyCod3



Cyber Talk

ATHSec | Our Global Team Of Security Experts

0xGIST

cyberXforce Information Security Team

0xGERT

cyberXforce Emergency Response Team

0xGTRAT

cyberXforce Threat Research and Analyse Team

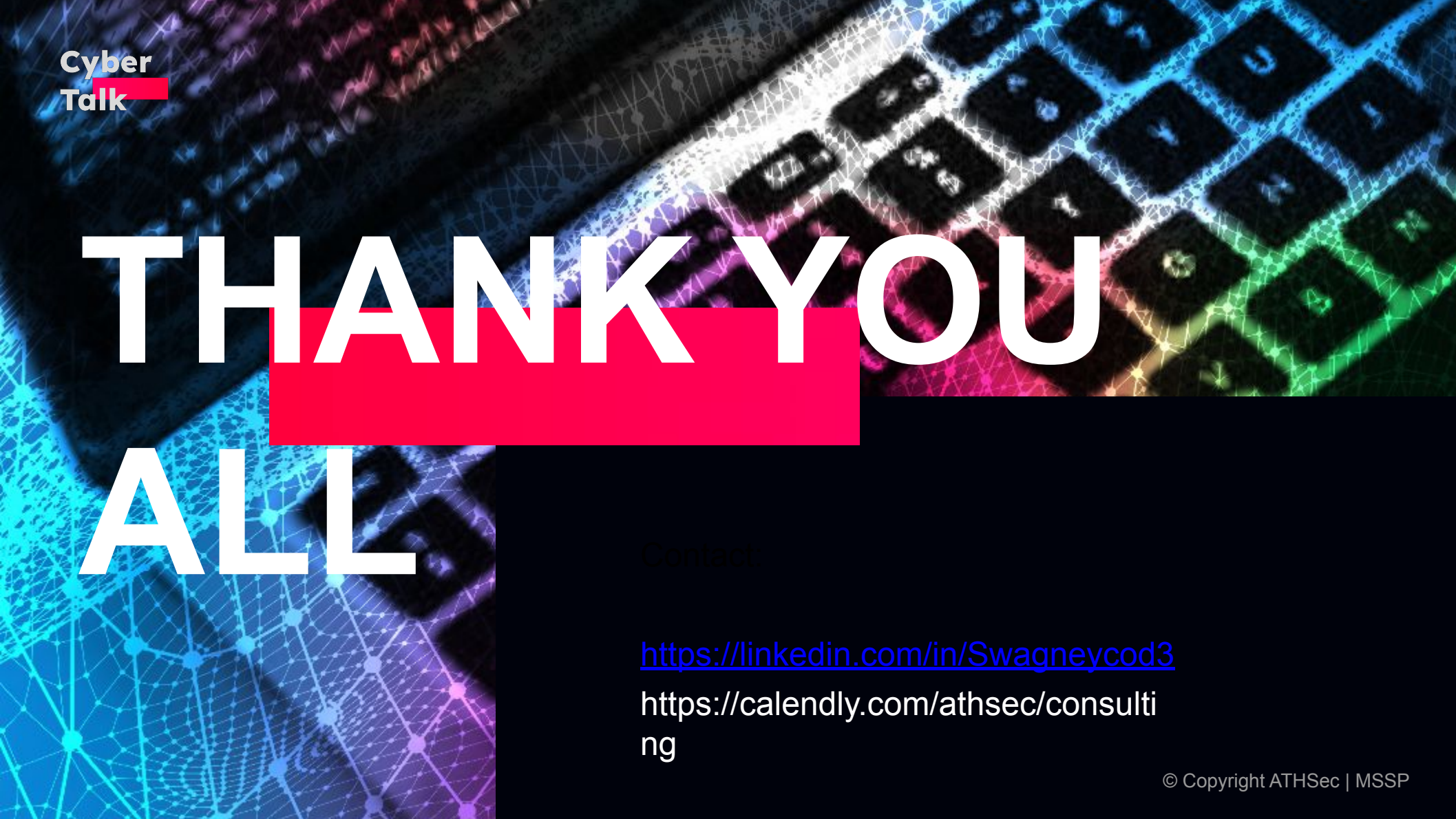
0xGTF

cyberXforce Threat Feed

Cyber Talk

Network Time

MOZDEVZ



THANK YOU ALL

Contact:

https://linkedin.com/in/Swagneycod3

https://calendly.com/athsec/consulting

Cyber Talk

Emergency Response Team

ATHSec | Experiencing an incident? Contact us.

ATHSec | DFIR-CERT

CALL 24h x 7days
| +258 87 272 5433