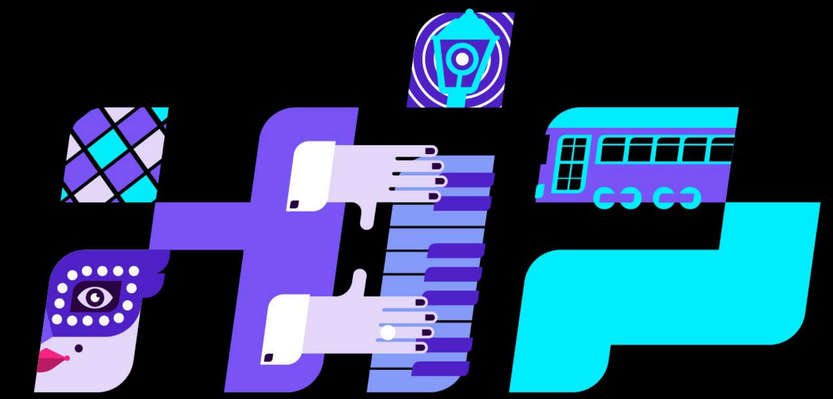
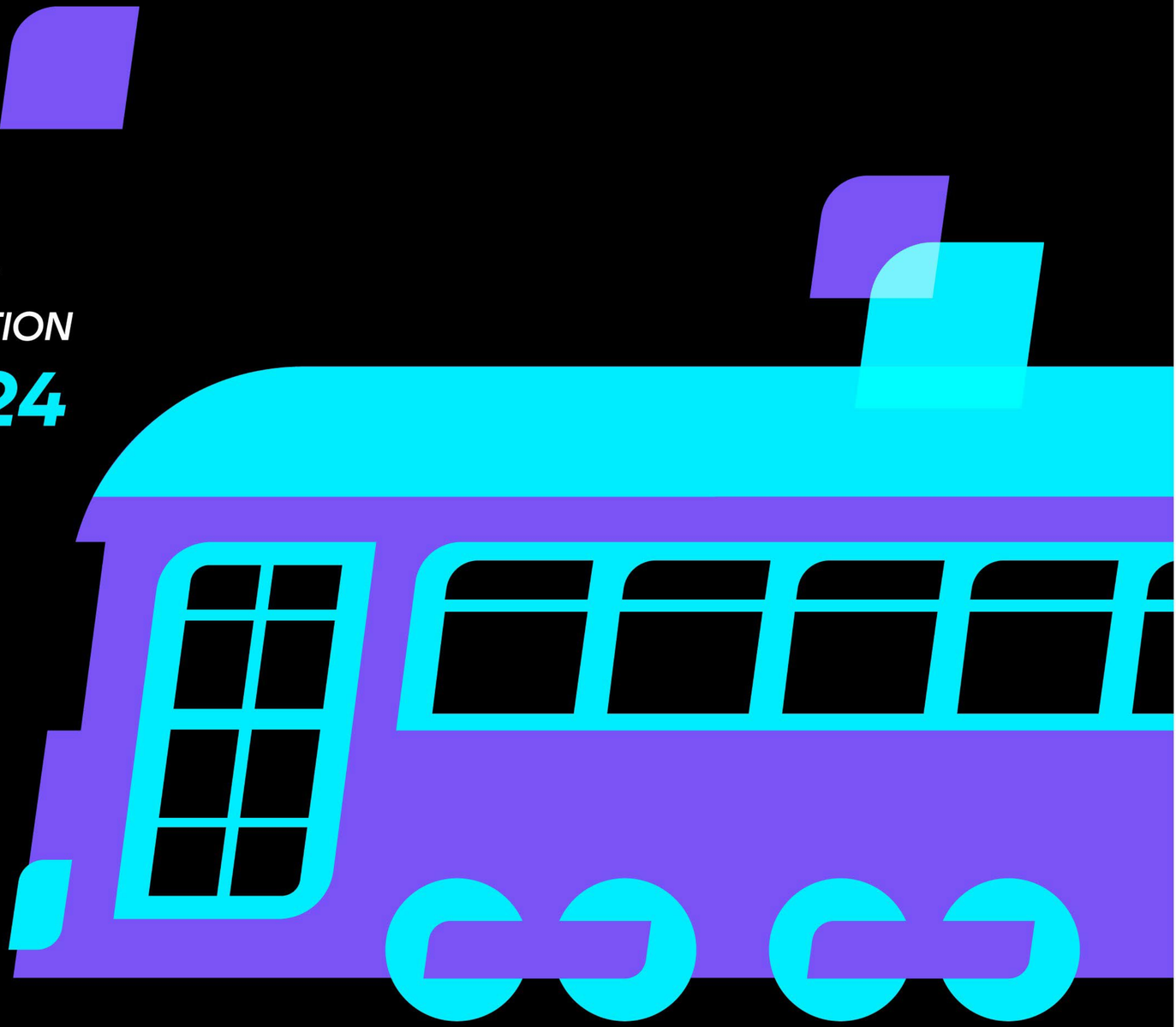


HYBRID
IDENTITY
PROTECTION

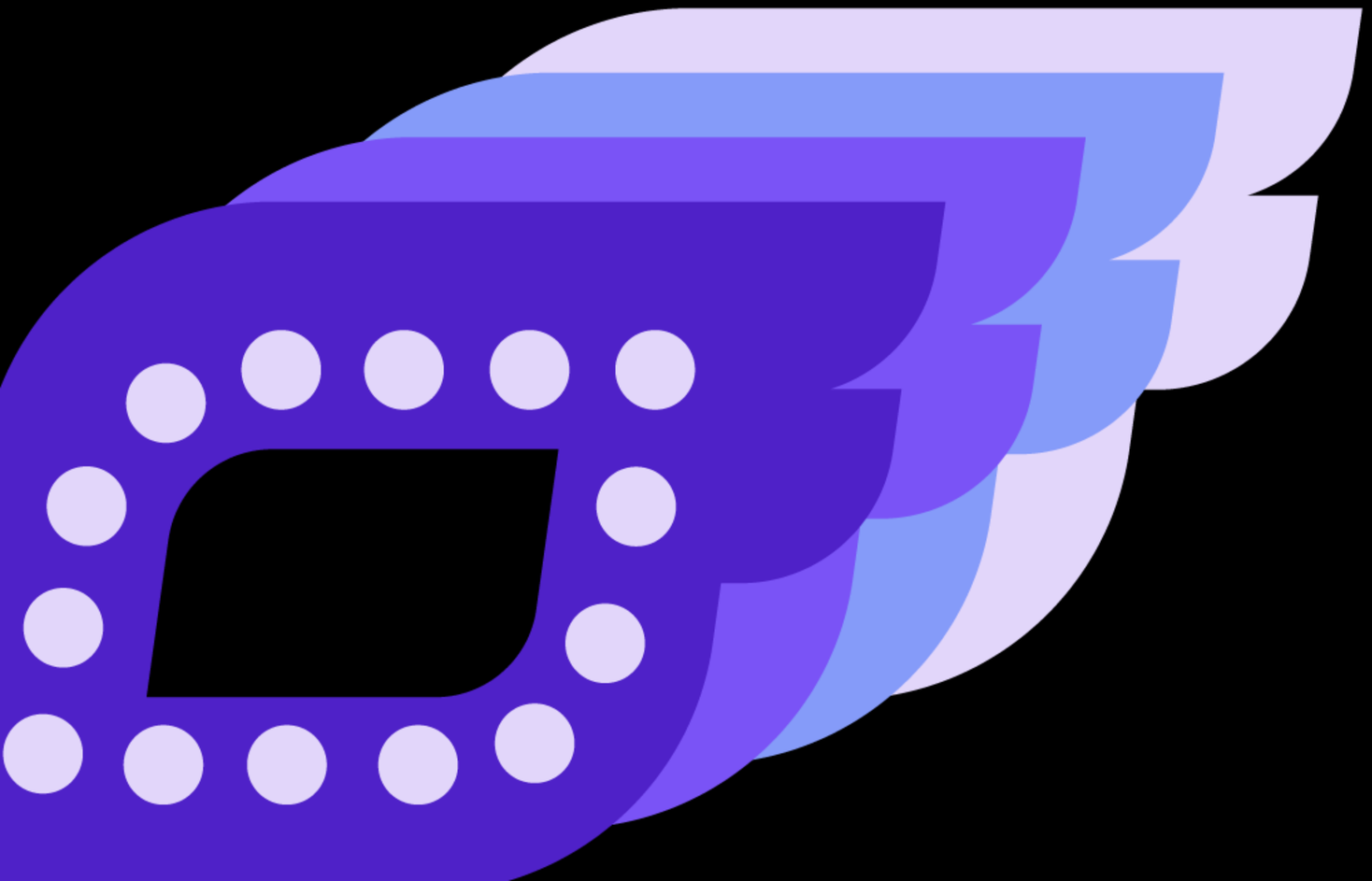
conf24

NEW ORLEANS



HYBRID IDENTITY PROTECTION conf24

NEW ORLEANS



Resisting Ransomware

Real-Life Lessons to Help You Fight Back

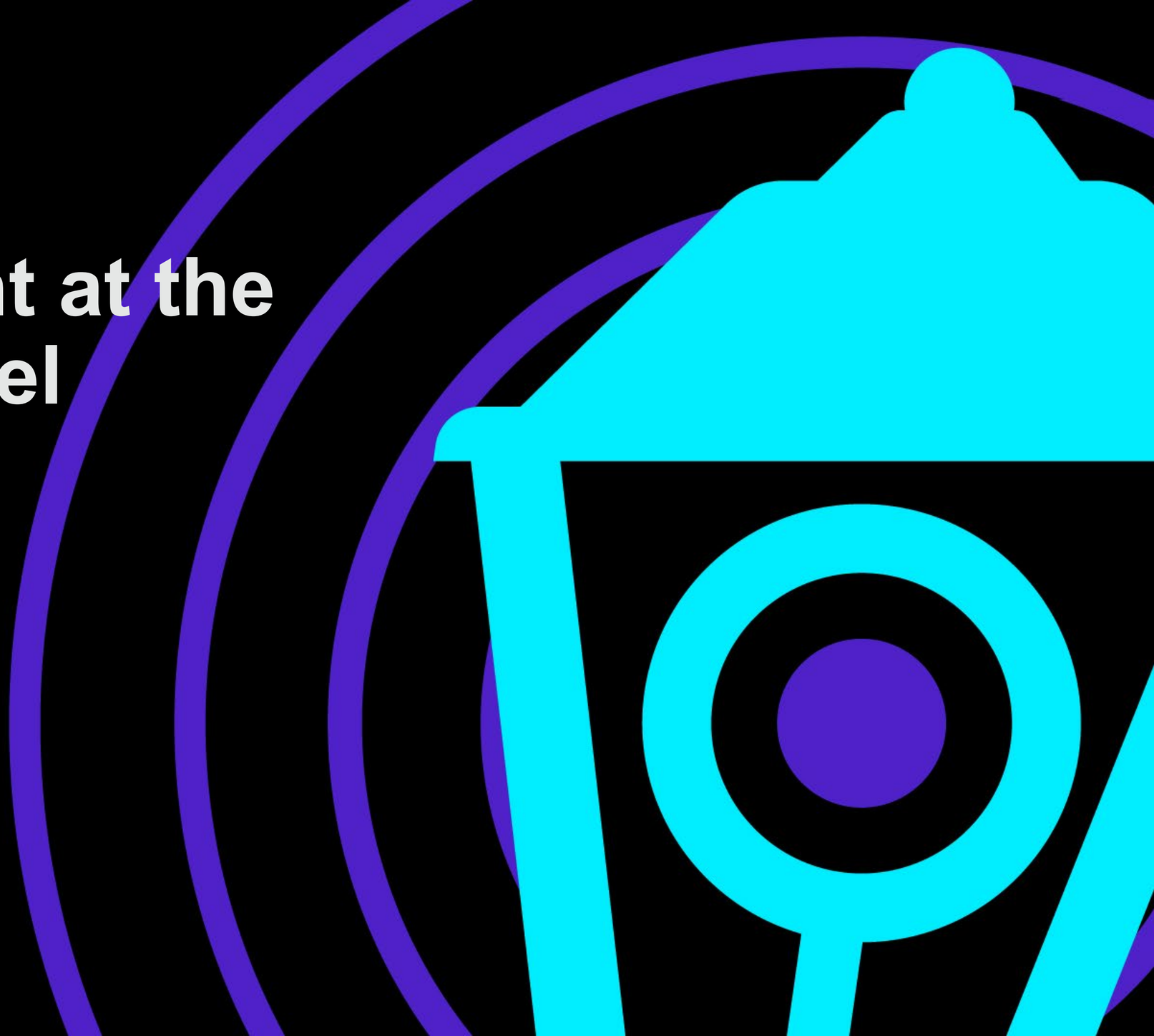
Jeff Wichman

Director of Breach Preparedness and Response

Marty Momdjian

GM – Semperis Ready1

There is *no* light at the end of the tunnel



HYBRID IDENTITY PROTECTION conf24 NEW ORLEANS

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

Lessons Learned

- Detection
- Response
- Recovery
- Ransomware negotiations

HYBRID IDENTITY PROTECTION conf24 NEW ORLEANS

Detection Considerations

- Every company says they are ready for a ransomware attack, until they are attacked.

- What do you want to detect?
- When?
- How?

- Detect for Tier 0 abuse! It is game over if Tier 0 is compromised.

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

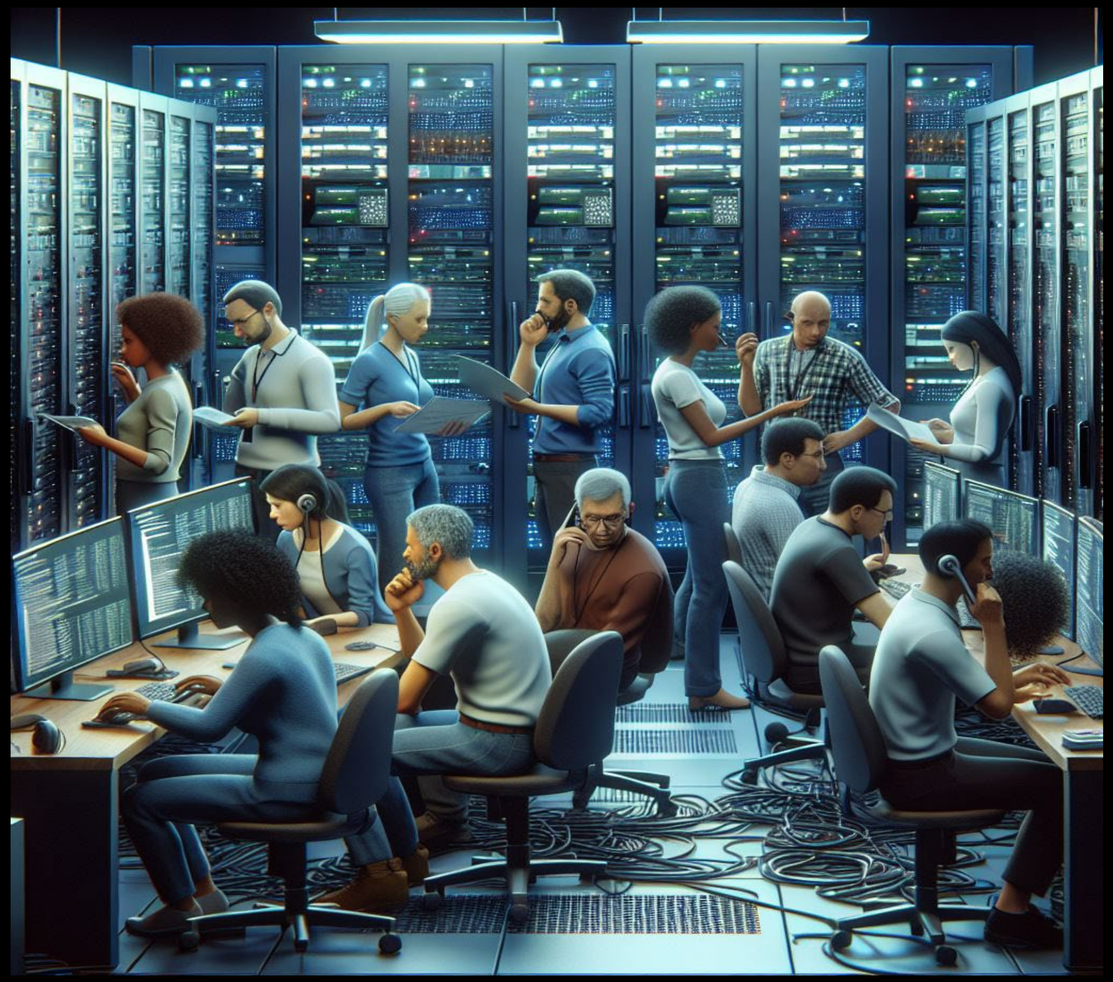
Incident Response

- What do you need?
- Escalation Points?
  - Internal
  - External
  - Legal
- Work with your partners
  - Who calls the shots?
    - Insurance
    - Legal
    - IR/Forensics
    - Ransomware Negotiator

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

Recovery

- Protect what is alive
- Where possible recover in isolation
- Be prepared for extended downtime
- Keep your team hydrated, fed and rested
- Forensic copy and evidence retention



HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

Ransomware Negotiations

- Do NOT contact the threat actor
- Follow direction of your legal counsel
- Engage a professional negotiator
- Be prepared for a 2 – 3-week process

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

Ask your self and others

Pre

- How fast can you really respond and press the red button?
- Does everyone know their role when an event occurs outside of IR team?
- Communications? Who, How, What?
- Forensics data and evidence storage?
- Exceptions (a **temporary** bypass of a security policy, procedure, or control for business reasons?)

Post

- Incident reporting – reg and compliance?
- Post backup restoration – remediation?
- Tech refresh and retooling…?
- Lessons learned?
- Cyber insurance (Before an event, ask what they will need post-event)

Questions

HYBRID IDENTITY PROTECTION conf24

NEW ORLEANS

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

Jeff Wichman

Director Breach Preparedness & Response, Semperis

Over 20 years in IT, Incident Response, Digital Forensics, and Ransomware Negotiations.

jeffw@semperis.com

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

Marty Momdjian

GM – Semperis Ready1

Incident Preparedness, Response, Recovery

DoD – Healthcare – Cyber

Generally… an all around fun guy

martym@semperis.com