MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

# BEWARE THE RANSOMWARE: AN INTERACTIVE TABLETOP


**Diana Kelley**
Cybersecurity Field CTO
Microsoft
@dianakelley14

**Ed Moyle**
Director, Research
ISACA
@securitycurve

# IMPORTANT NOTE

Warning: This is a group activity.  You will be expected to participate.

# TIMED AGENDA

| Time (minutes) | Item |
|---|---|
| 0 - 20 | Introduction and Overview |
| 20 – 35 | Backgrounder and Detection |
| 35 – 45 | Analysis |
| 45 – 65 | Injection! |
| 65 – 75 | Containment |
| 75 – 90 | Injection! |
| 90 – 100 | Recovery |
| 100 – 120 | Post-Incident and Wrap-Up |

# WHAT IS A TABLETOP?

- Real-world SIM
- Facilitated and mostly scripted
- Participants play roles of key stakeholders

# WHY DO A TABLETOP?

- Test process/plan
  - Note: NIST Special Publication 800-61 is a good resource for developing a plan*
- Expose gaps
- Identify areas for improvement
- Practice makes perfect

*http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

# OTHER OPTIONS

Hybrid

- Some scripting
- Live scans/hunting
- ~6 mos planning/5 days run

Full-Live

- Real and scripted
- Sims with physical and logical aspects
- ~12 mos planning/1-2 weeks run

# SOME LINGO

- Red Team/Blue Team/White Team
- Master Scenario Event List (MSEL)
- Rules of Engagement (ROE)
- Inject
- Range/CyberRange
- Hotwash and After Action Review (AAR)

# BUILDING A PLAN

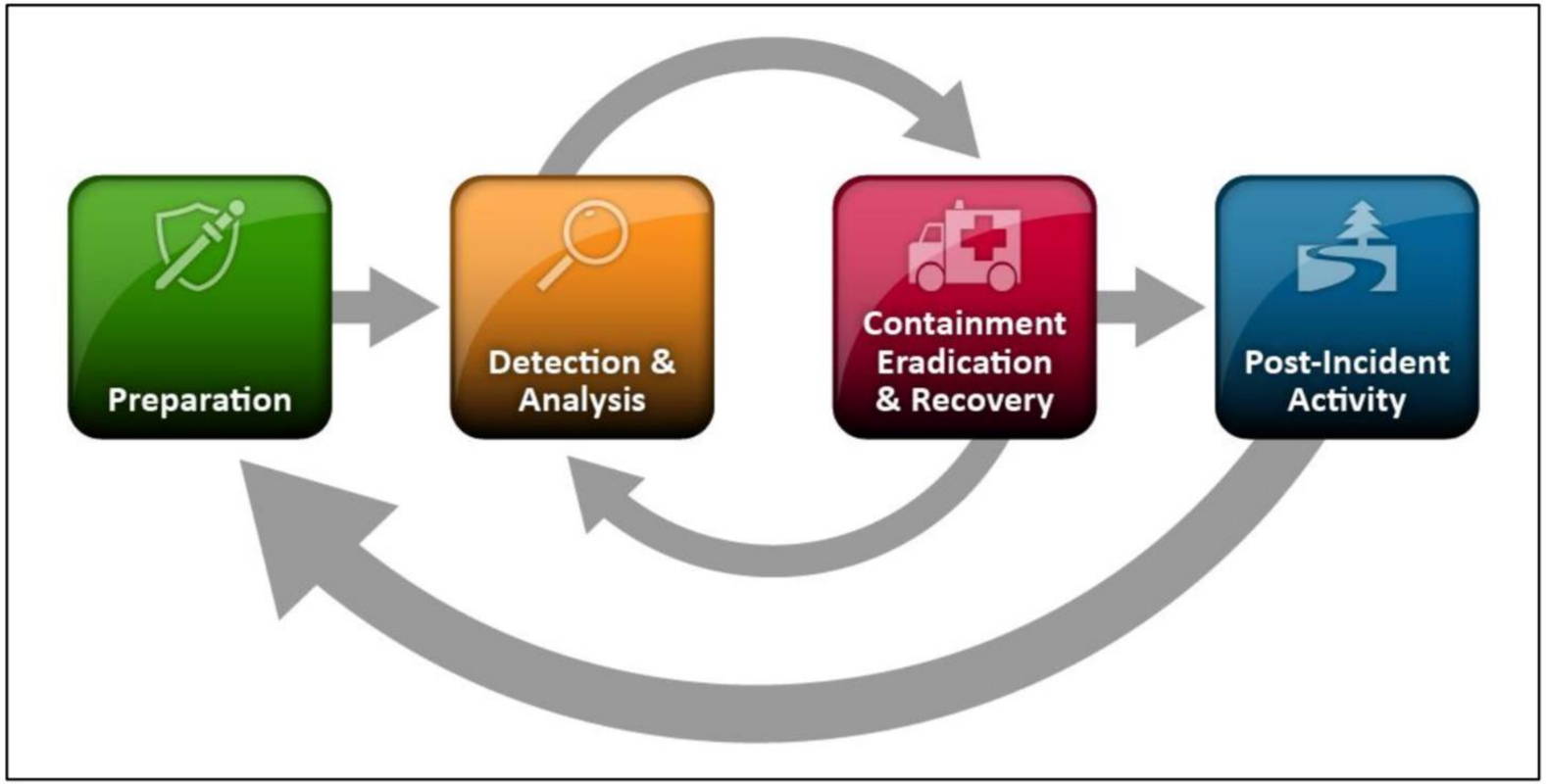



**Figure 3-1. Incident Response Life Cycle**

# TABLETOP

# ENTERPRISE BACKGROUNDER

## John R. Brinkley Memorial Health System

- Large, non-profit, multi-state health system
- Please take 5 minutes to review background handouts

# STAKEHOLDERS

- CxO
- Public Relations
- Legal
- Compliance
- CyberSecurity/SOC

- *For larger SIMs (not used today)*
  - *HR*
  - *Operations/NOC*
  - *Audit*
  - *Physical/Facilities*
  - *Business Continuity*

# GETTING STARTED

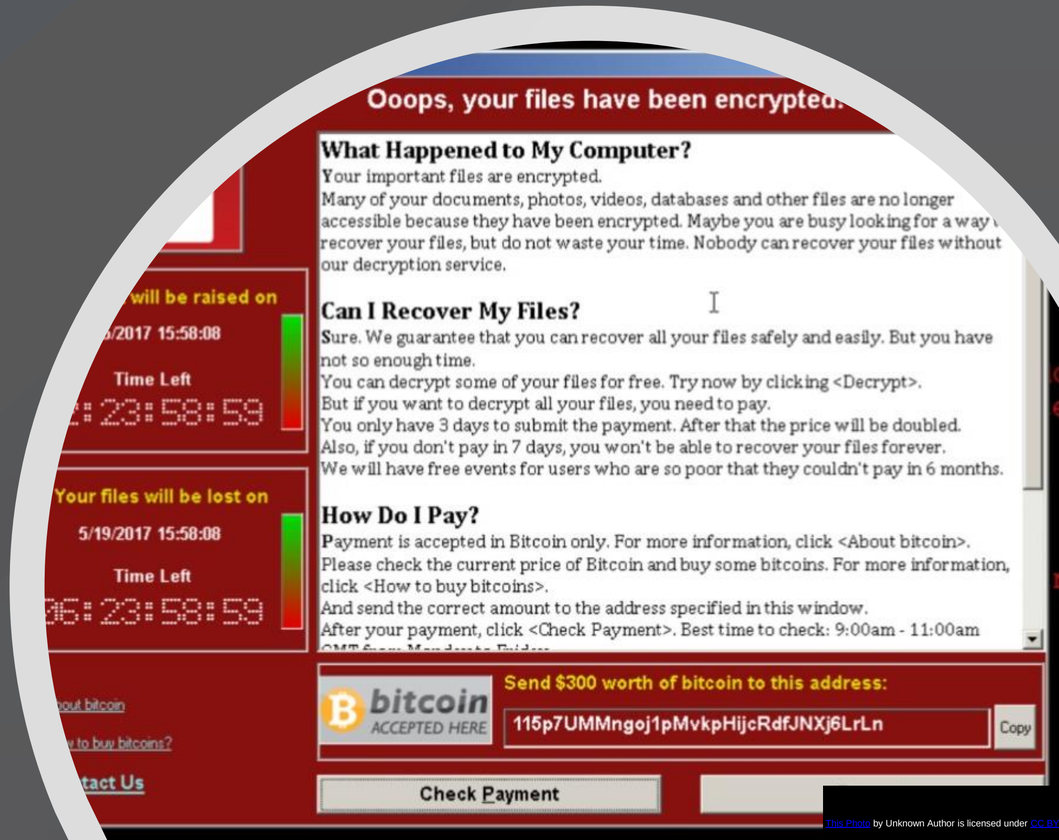
- Open background information envelope
- Envelope contains motivations, goals, and other relevant information about your role
- Do not share background information outside your team

# INCIDENT RESPONSE

- Incident response process initiated
- Ransomware discovered on clinical systems

Instructions:

- Timed: 20 minutes
- Open Envelope One
  - Review information, but do not offer it unless requested
- Focus on the objective
  - Analyze what's going on
  - What do you need to know?

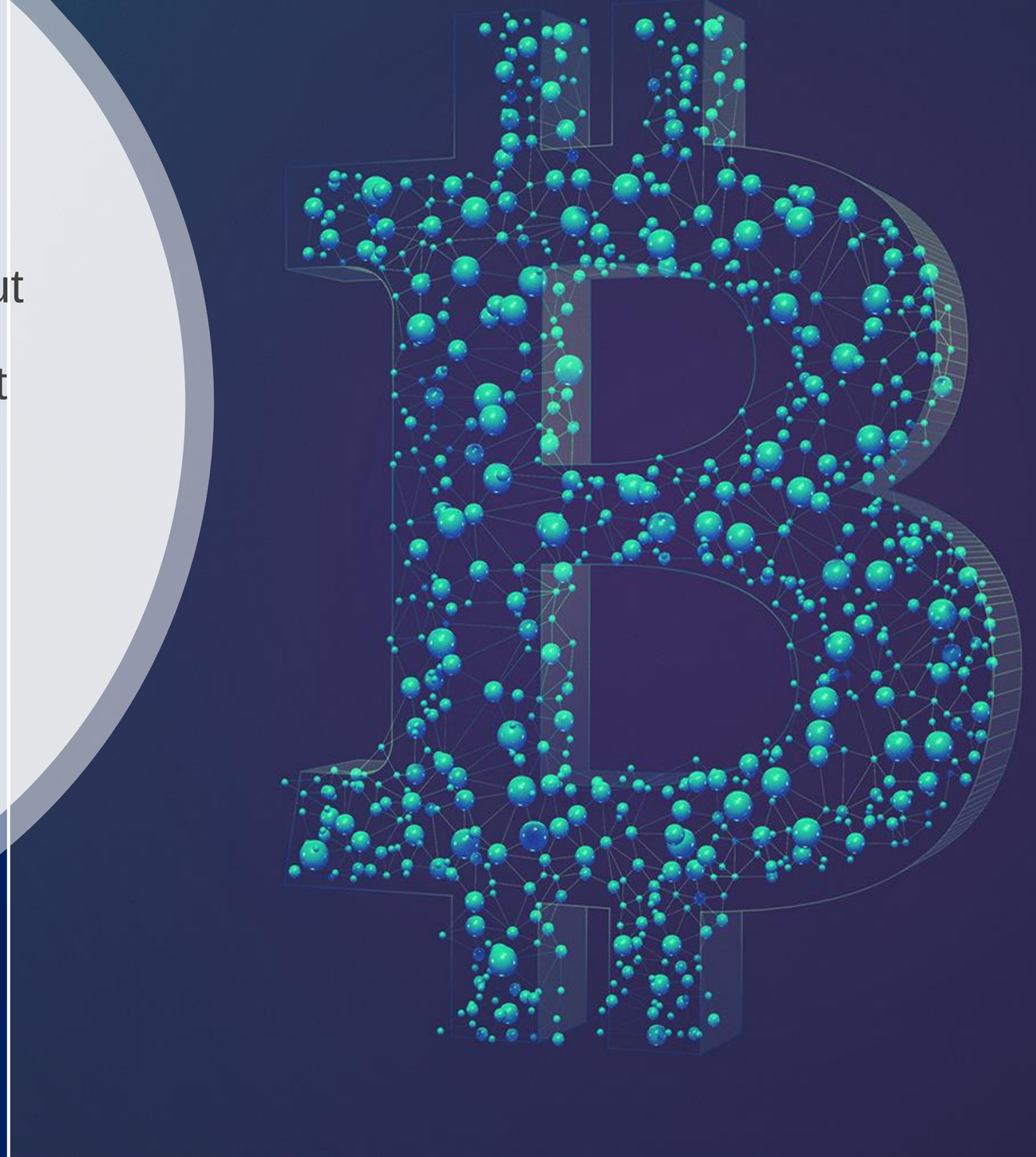



# QUESTIONS

# CONTAINMENT

- Multiple parties asking about payment as an option
- Containment proves difficult

- Instructions:
- Timed: 20 minutes
- Open Envelope Two
  - Review information, but do not offer it unless requested
- Focus on the objective
  - Containment
  - What do you need to do?



Containment
Eradication
& Recovery

# QUESTIONS

# RECOVERY

- Infection vector discovered
- Event fallout and recovery

- Timed: 20 minutes
- Open Envelope Three
  - Meet the Press: Interview Prep
  - Mock Interview


# QUESTIONS

# Post-Incident Activity

## WIND DOWN

- Timed: 10 minutes
- Open Envelope Four
  - Review information, but do not offer it unless requested
- Focus on the objective
  - Recovery
  - What needs to be done to close the incident out?

# QUESTIONS

# HOTWASH


- How do you feel?
- Surprises?
- Biggest “ahas”?

# AFTER-ACTION REVIEW


- What did you learn?
- What would you do differently?
- Are additional tools/resources needed?
- Where can the IR plan be optimized?
- Plans for future runs?
- Metrics to prove value and measure improvement?

# RESOURCES

- Mitre, CyberExercise Playbook, https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf
- NIST, SP 800-61 Rev2, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- Organizational Models for Computer Security Incident Response Teams (CSIRTs), http://www.cert.org/archive/pdf/03hb001.pdf

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

# THANK YOU

## PLEASE FILL OUT YOUR EVALUATIONS!

**Diana Kelley**
Cybersecurity Field CTO
Microsoft
@dianakelley14

**Ed Moyle**
Director, Research
ISACA
@securitycurve