Functional Incident Response Plans

2024 and beyond

Tom Arnold, CISSP, ISSMP, GCFE, GBFA, GNFA, GWEB, PCIP, CISA
Lecturer, Digital Forensics and Incident Response, University of Nevada Las Vegas Cybersecurity Graduate Program

University of Nevada Las Vegas

Cybersecurity Graduate Program

- Interdisciplinary
  - Jointly offered between Business and Engineering
  - Focus on both hard and soft skills of cybersecurity
  - Open to all backgrounds
    - Preference given to those with a technical background
- Access to job-ready training
  - Individual mentors from local cyber community
  - Cours projects with real clients
  - Competitions each term of the program
  - Capstone project
  - Online cyber-range via Cyberbit

PCI Security Standards Council

UNLV LEE BUSINESS SCHOOL

UNLV HOWARD R. HUGHES COLLEGE OF ENGINEERING

Agenda

- Challenges
  - Core deficiency inherent in plans and planning
  - New technologies and services
  - Expanded kill chain
  - Staffing and resources
- Elements
- Audit checklist

Core deficiency inherent in plans and planning

During the development of ANY cybersecurity or incident response plan, there's one person not invited and always missing from the room

-- H. Carvey (2024) USSS CFTF session

PCI Security Standards Council

New technologies and services

Starting simple: Consider cloud-hosted applications and services

Company responsible

Cloud responsible

On Prem	IaaS	PaaS	SaaS
Application	Application	Application	Application
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
Operating System	Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Network	Network	Network	Network

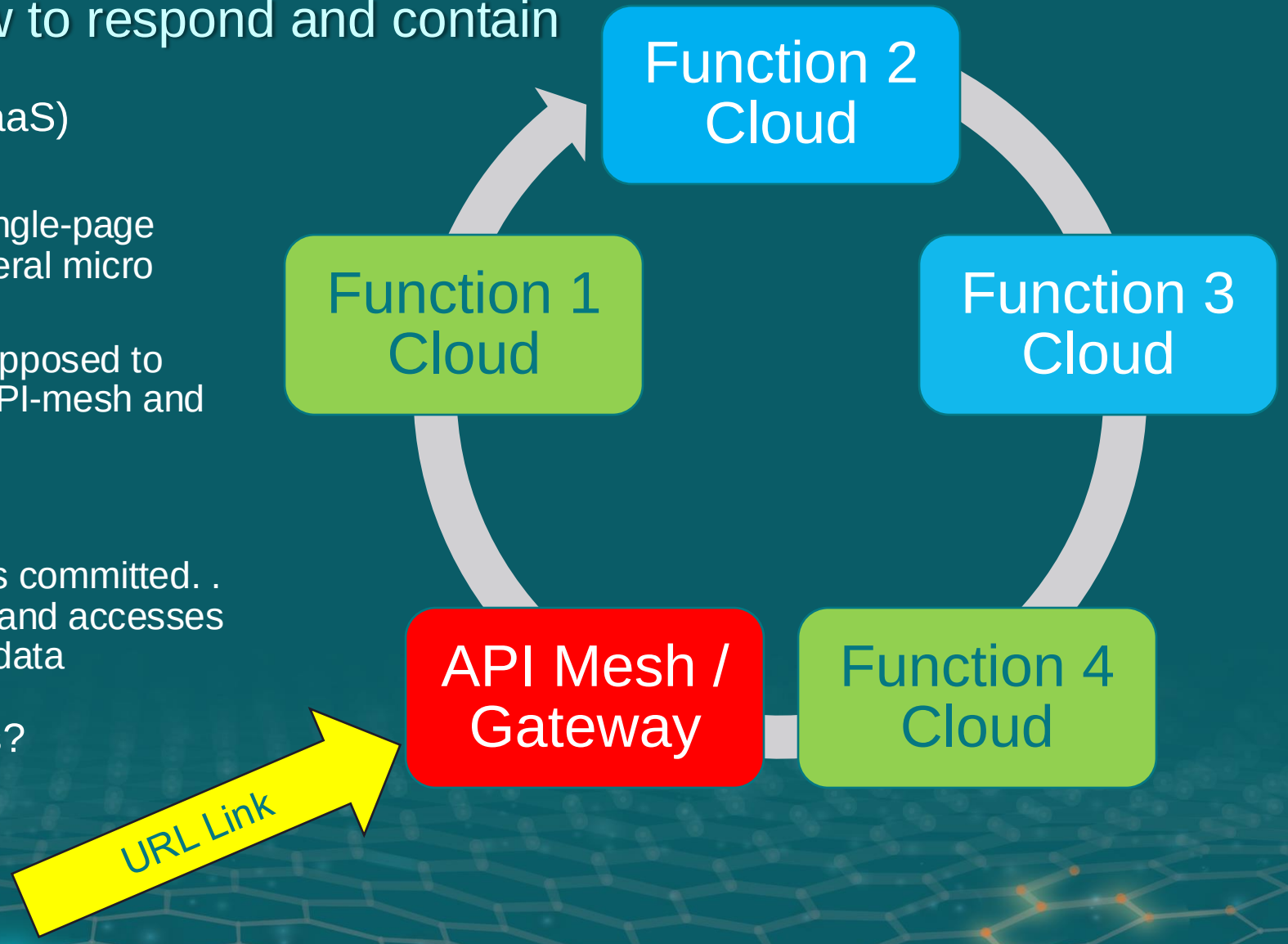
PCI Security Standards Council

New technologies and services

Much tougher: Consider how to respond and contain

- Cloud **Function as a Service** (FaaS)
  - Multiple cloud providers
  - Developed high-performance, single-page application deployed across several micro services
  - Application and site access is supposed to have security enabled through API-mesh and use of API-Gateway
- Scenario

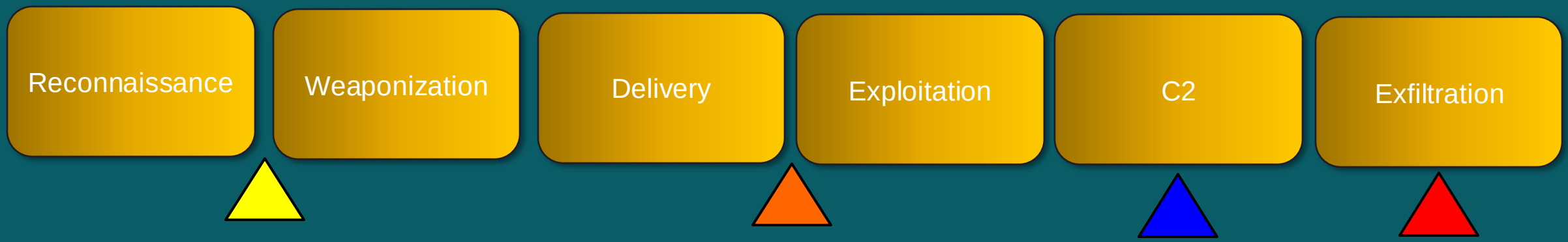
  Find bad guy and how the attack was committed. . Did attacker bypasses API-Gateway and accesses individual service to steal consumer data
- Now What? How can you do this?



PCI Security Standards Council

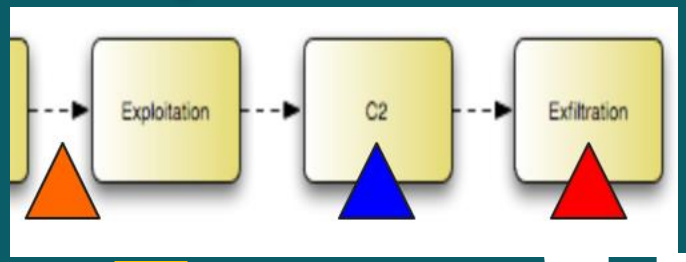
Expanded kill chain

We start here. . .



"Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains" Lockheed-Martin, August 2011

Expanded kill chain



Carrier, Brian Proceedings of ResponderCon, Basis Technologies, 2022

Initial Access

Install Primary C2

Install Secondary C2

Privilege Escalation / Credential Access

Infrastructure Discovery

Data Discovery / Exfiltration

Propagate Ransomware

Encrypt data

PCI Security Standards Council

Elements

Basic: From frameworks and compliance requirements

NIST computer security incident handling guide (SP 800-61)

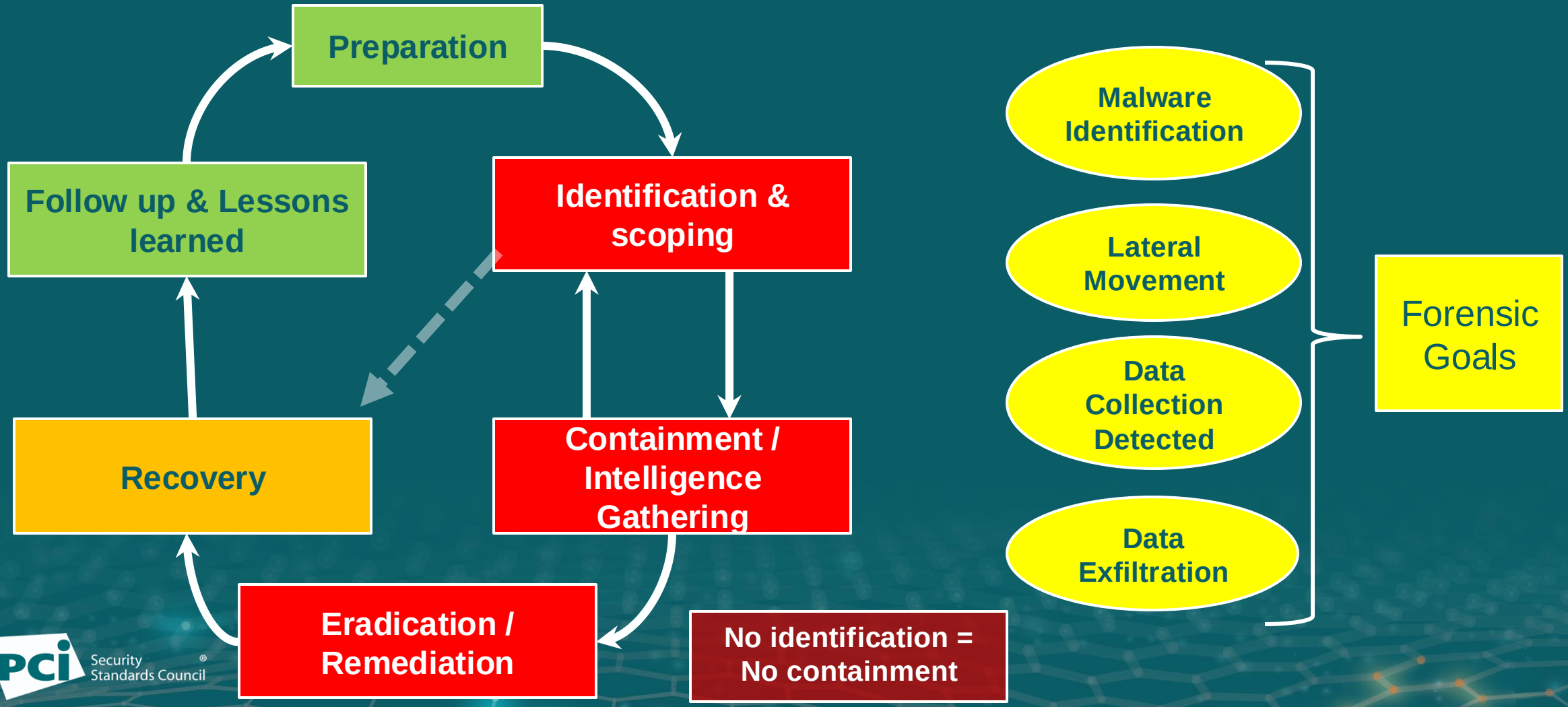
Uses predefined forms to establish response plan, forms include:

- Incident contact list, identification checklists, survey
- Containment checklist, eradication checklist, and communications logs

PCI Security Standards Council

Elements

Process elements that should be covered



PCI Security Standards Council

Staffing and resources

Challenges that need to be identified in advance of “the event”

- Incident team identified
  - Incident leader
  - Technical leader
  - Unit members
  - External resources
  - Staff fatigue and depth
- Legal readiness
  - For all Cloud resources, right to audit and investigate
  - Event log availability
  - External resource agreements in place (response time)
- Basic security team
  - Clear identification and declaration guidelines in the plan
  - Identification and inventory of all 3rd-party resources and assets
  - Identification and classification of assets
  - Network and systemic inventory
  - Location of common evidence artifacts
  - Tools for 4n6 response
- IT
  - Current and accurate network diagrams and inventory
  - Location of all logs

PCI Security Standards Council

Assessment checklist

Basic process and procedures to validate in IR plans

- Elements from compliance standards
- OPSEC
- Personnel are trained, exercised and ready
- Declaration of an incident
  - Category identified and defined
  - Initial notification requirements
- Determine investigative scope
- Perform technical analysis
  - Threat hunt and identification
  - Correlate to CTI
  - Assess operational impact
  - Update scope
- Document timeline
- Identify anomalous activity
  - Assess affected systems & networks
  - Identify deviations from baseline
- Root cause
  - Initial access vectors
  - Defense evasion & persistence
  - Lateral movement & backdoors
  - Adversary TTPs
- Incident indicators
  - Atomic, computed, and behavioral info
  - Document indicators

PCI Security Standards Council

Assessment checklist

The rest

- Analysis of adversary TTPs
  - Initial access techniques
  - Malware
  - Compromised host analysis for persistence
  - Methods for lateral movement
  - Level of credential access
  - Methods for C2
  - Methods for data exfiltration
- 3rd Party analysis support
  - Coordinate response efforts
- Containment
- Eradication and Recovery
- Post-incident
  - Document and report
  - Adjust sensors, alerts and log collection
  - Identify and address operational blind spots
- Final reports
  - Provide post-incident updates as required by law and policies
  - Publish reports to senior leadership
- Perform hotwash
  - Lessons learned analysis and update plans
  - Identify gaps in IR training or security readiness
  - Identify and resolve deficiencies in tools and processes
  - Identify if infrastructure and defenses were appropriate

PCI Security Standards Council

Thank you

thomas.arnold@unlv.edu

PCI Security Standards Council

UNLV LEE BUSINESS SCHOOL

UNLV HOWARD R. HUGHES COLLEGE OF ENGINEERING