

# The Response-Ready Infrastructure

Justin Hall, Senior Security Architect  
CBTS



# **/usr/bin/whoami**

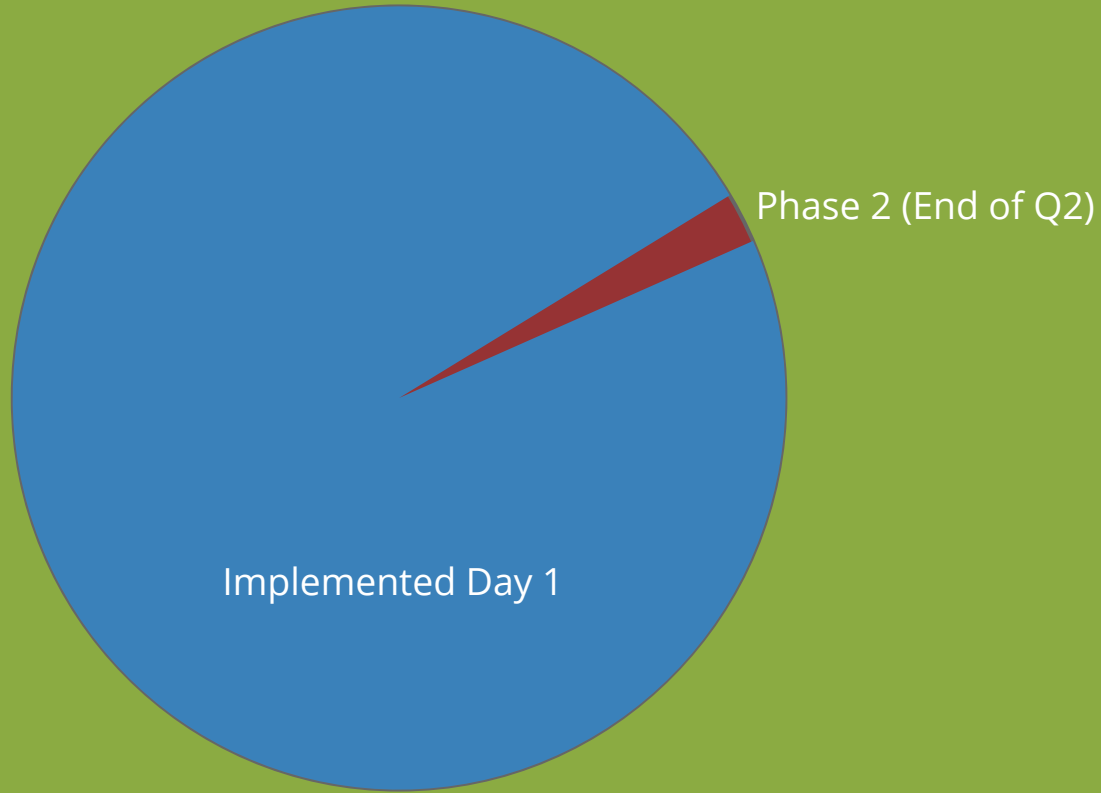
Ten years with CBTS as security consultant to shops small (5 person) and large (Fortune 5)

GIAC Certified Incident Handler, Forensic Analyst, Penetration Tester

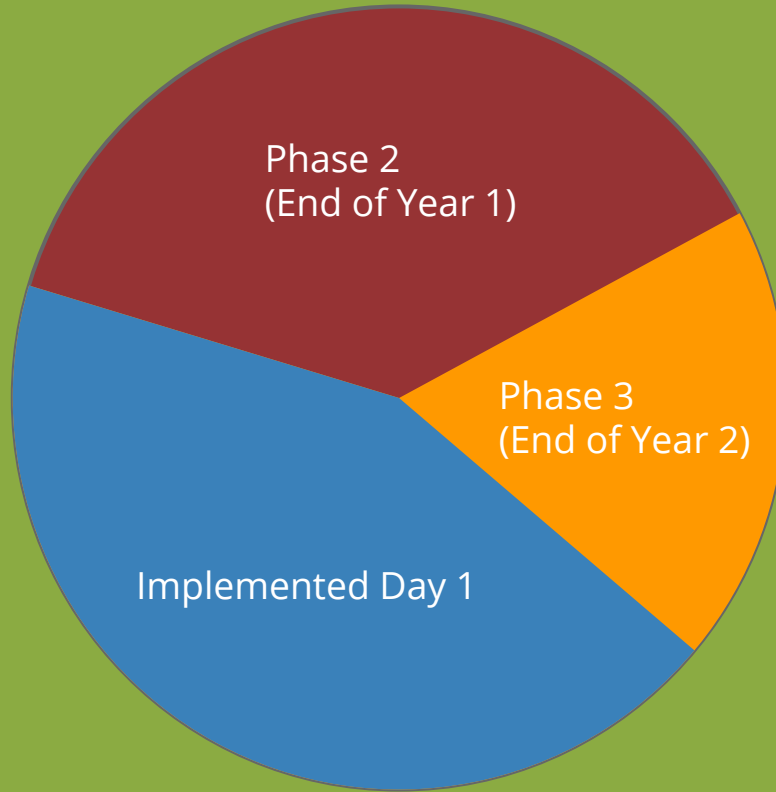
A large construction crane stands tall against a dark, twilight sky. Below it, a multi-story building is under construction, with its skeletal frame and some interior lights visible. The scene is dimly lit, with the primary light source being the ambient light of dusk.

**2013:** Build a secure network

- ☒ ISO 27K
- ☒ NIST 800-53
- ☒ SANS CSC



# My Expectations



# What Happened



**Assume you will be breached**



Cyber-Safe

# <Your Company's Name Here> hit by massive data breach



By Charles Riley @CRrileyCNN



## Most Popular



Walmart ups pay well above minimum wage



Delta CEO apologizes for 9/11 comment



America's most successful stock



**62%** of organizations do not believe they  
are prepared to respond to a breach

Ponemon Institute 2014 Study on Data Breach Preparedness

**81%** of organizations are not fully  
monitoring their environment

SANS 2014 Critical Security Controls Adoption Survey

**IEC 61508/61511**

“Safety Instrumented  
Systems”

# Response Ready Infrastructure

“A computing environment designed and instrumented to facilitate detection of, and response to, an intrusion”

ALERT: CONDITION RED

LCARS 40257

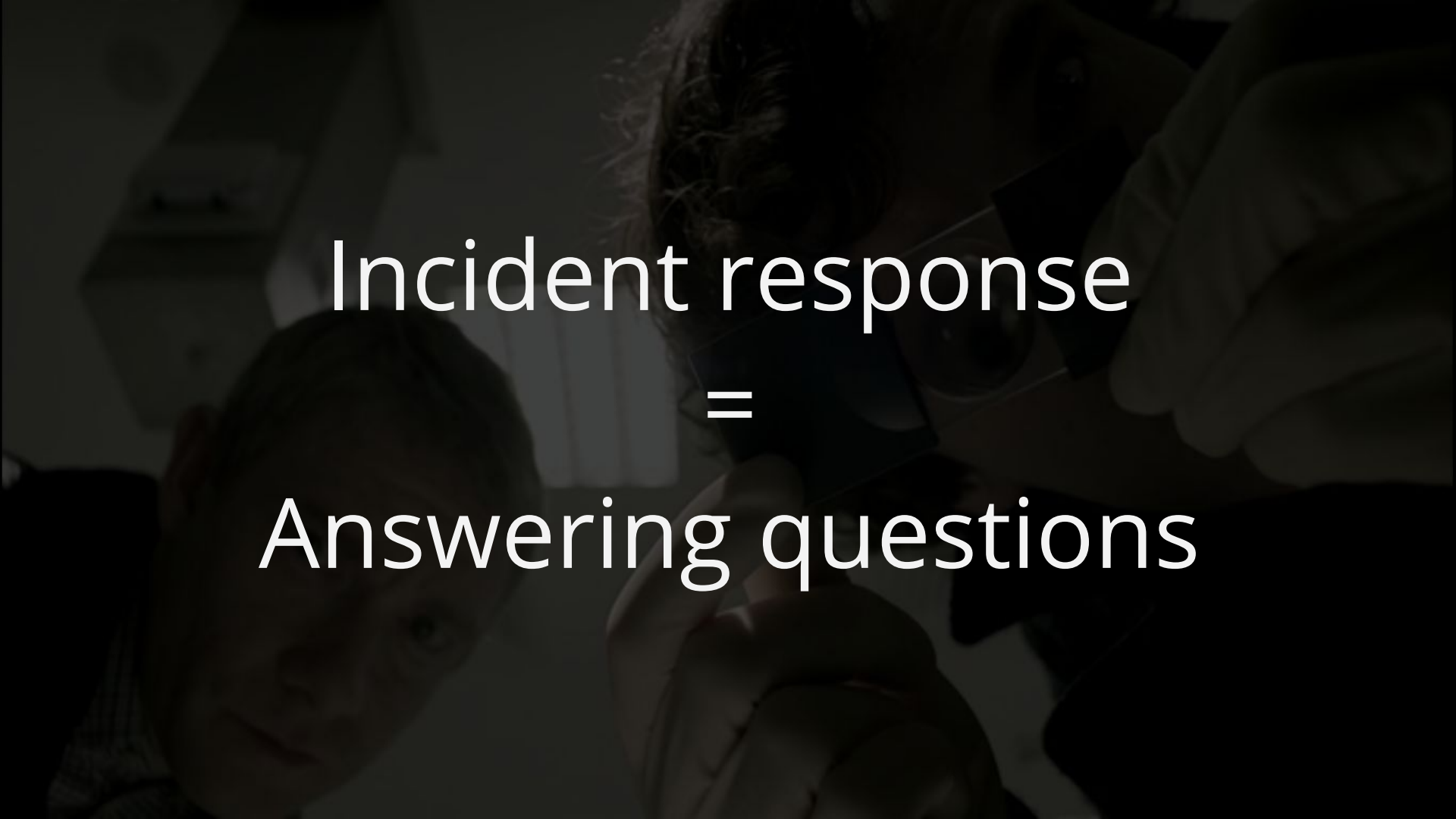
```
[**] [1:2016922:6] ET TROJAN Backdoor family PCrat/Gh0st CnC traffic  
[**][Classification: Potentially Bad Traffic] [Priority: 2]  
03/01-15:50:29.236253 82.165.50.118:80 -> 172.20.129.181:39929
```

LCARS 40257

LCARS 40257

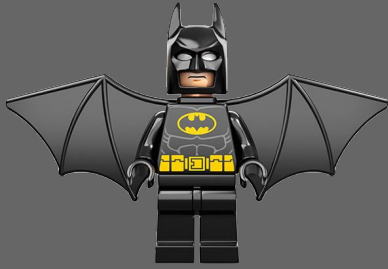
LCARS 40257

LCARS 40257



Incident response  
=  
Answering questions

Real Quick: People



Incident Handler



Incident Analyst



Decision Maker



Real Quick: Process

**Eight key items** to have in place



Preparation

Detection  
&  
Analysis

# Item 1: **Logs**

Anything with a **host**

Anything with a **user**

Anything involving a critical **process**

Anything involving sensitive **data**

**Centralize** the data

Make it **searchable**

Make it **accessible**

## Item 2: **Indicators**

# Network-based Indicators



# Host-based Indicators

# Item 3: **Asset Inventory**

Authorized **Asset** Database

Authorized **Software** Database

# Item 4: **Analysis Tools**

Complete **tool set**

**Ideal network placement**

Sufficient **privileges**





Detection  
&  
Analysis

Containment  
Eradication  
Recovery

# Item 5: **Access Controls**

# **Network** Access Controls

# **Endpoint** Access Controls

# Item 6: **Gold Image**

# Item 7: **Communication**

# Item 8: Incident Tracking

# Whitepaper: Incident Tracking in the Enterprise



[sans.org/reading-room](https://sans.org/reading-room)



**Test** Your Controls

ALERT: CONDITION RED

LCARS 40257

```
[**] [1:2016922:6] ET TROJAN Backdoor family PCrat/Gh0st CnC traffic  
[**][Classification: Potentially Bad Traffic] [Priority: 2]  
03/01-15:50:29.236253 82.165.50.118:80 -> 172.20.129.181:39929
```

LCARS 40257

LCARS 40257

LCARS 40257

LCARS 40257

**SANS CSC**



**NIST 800-53**



**NIST 800-61**



# Thanks for listening!

@justinhall

justin.hall@cbts.net

# The Response Ready Infrastructure

Logs

Indicators

Asset Inventory

Analysis Tools

Access Controls

Gold Image

Communications

Incident Tracking