

How To CISO

VOLUME 1

THE FIRST 91
DAYS



Sink or Swim

A CISO's First 91 Days

Andy Ellis
Principal, Duha

How To
CISO

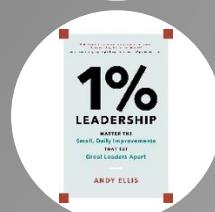
Andy Ellis



Andy Ellis

www.csoandy.com
@csoandy

How To
CISO



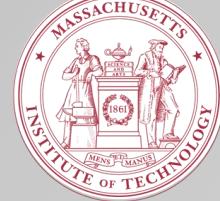
Principal
Duha

Author
1% Leadership

2021 inductee
CSO Hall of Fame

Podcast Co-host
CISO Series

Editor
How To CISO



Quick CV

Partner
YL Ventures

Advisory CISO
Orca Security

CSO
Akamai

Officer
US Air Force

6-3, minor in 18
MIT

Success Criteria

Gain Political Capital

- People will take your calls, listen to your ideas

Removed Negativity

- Solved problems that destroyed value

Clear Identity

- Predictable interactions and goals

Referenceable Wins

- Achieved visible successes

Approaching Your Role

Understand the Organization

Gain Situational Awareness

The State of Security

Make Changes

Understand the Organization

Every organization is *unique*, but there are patterns



Understand the Organization

Every organization is *unique*, but there are patterns



Understand the Organization

Every organization is *unique*, but there are patterns



Understand the Organization

Every organization is *unique*, but there are patterns



Understand the Organization

Every organization is *unique*, but there are patterns



Carbon
Silicon

Vampire
Zombie

Big Fish
Small Fry

Understand the Organization

Every organization is *unique*, but there are patterns



Understand the Organization

Every organization is *unique*, but there are patterns

Jane Doe

Kardashian

Executive



Operator

How To
CISO

Carbon
Silicon

Vampire
Zombie

Big Fish
Small Fry

(Re)build
Maintain

Understand the Organization

Every organization is *unique*, but there are patterns

Jane Doe

Kardashian

Outcome



Executive

Operator

Effort

How To
CISO

Carbon
Silicon

Vampire
Zombie

Big Fish
Small Fry

(Re)build
Maintain

Understand the Organization

Jane Doe
Kardashian

Outcome
Effort

Executive
Operator

Carbon
Silicon

Vampire
Zombie

Big Fish
Small Fry

(Re)build
Maintain

Approaching Your Role

Understand the Organization

Gain Situational Awareness

The State of Security

Make Changes

Gain Situational Awareness

What exactly is the situation you walked into?

People

Product

Environment

Three Questions

What do you do?

What should we stop doing?

What should we start doing?

People

Four Personas

Excited

Nervous

Old-timers

Newbies

People

Four Personas

You Should

Excited

Channel Excitement

Nervous

Calm Concerns

Old-timers

Learn History

Newbies

Listen to Ideas

How To
CISO

People

Four Personas

You Should

But Don't

Excited

Channel Excitement

Inflate expectations

Nervous

Calm Concerns

Ignore worries

Old-timers

Learn History

Accept ruts

Newbies

Listen to Ideas

Ignore side effects

Three Questions

Five Groups

Your Group

Your Partners

Your Peers

Your Executives

Your Board

Gain Situational Awareness

What exactly is the situation you walked into?

People

Product

Environment

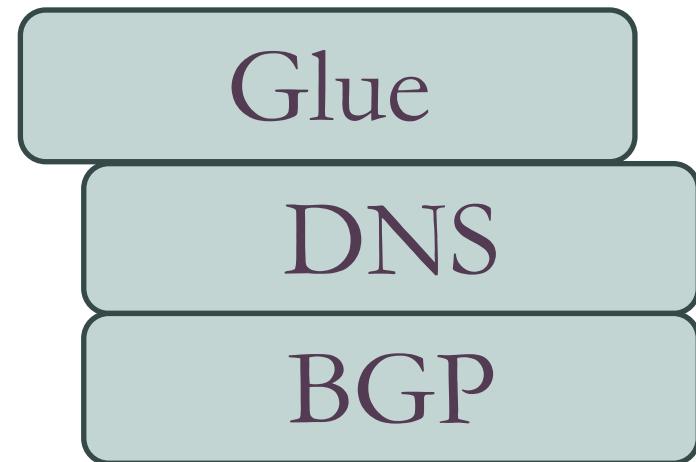
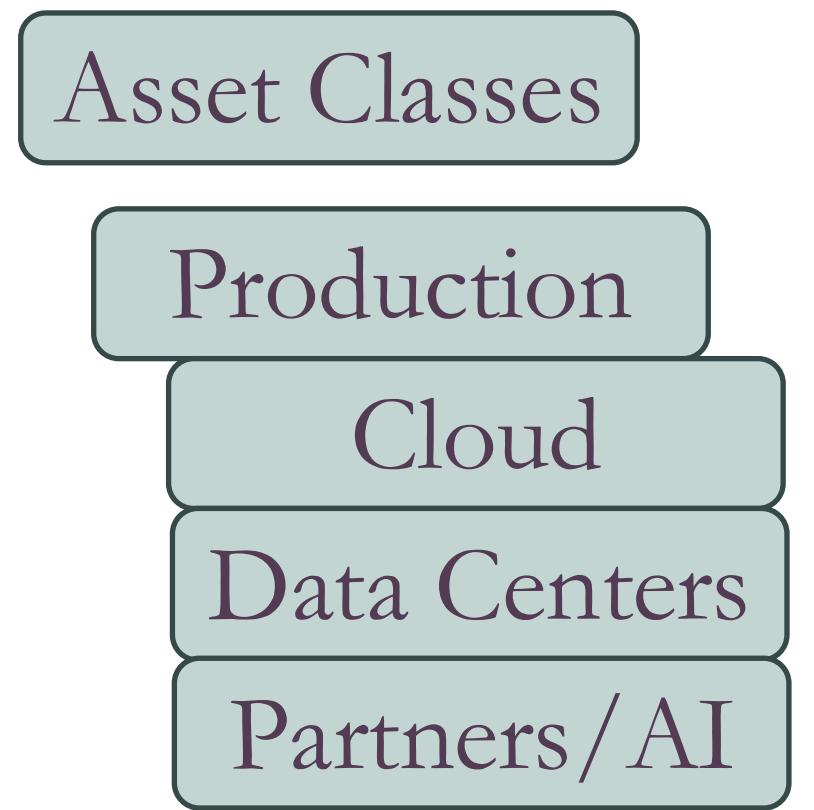
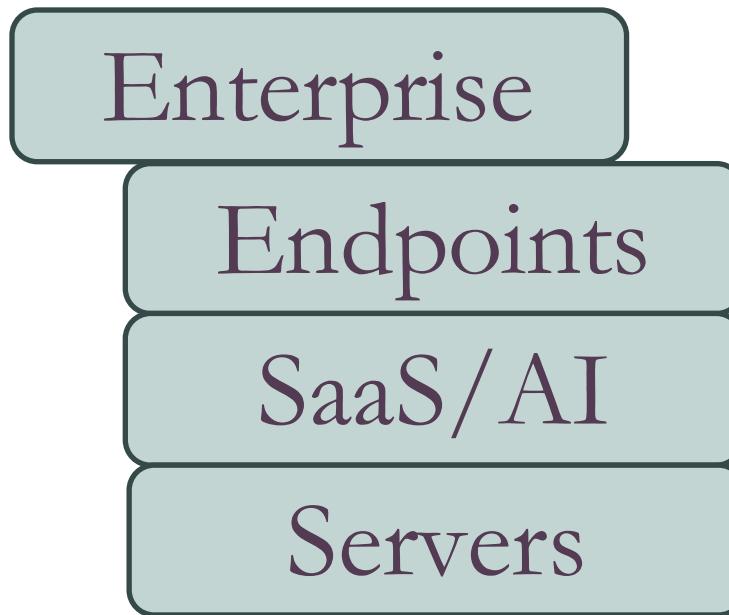
Environment

Identify *unacceptable* losses before you get lost in assets

Asset Classes

Environment

Identify *unacceptable* losses before you get lost in assets



Gain Situational Awareness

What exactly is the situation you walked into?

People

Product

Environment

Product

How does your employer make the money it uses to pay you?

Who are your customers?

What is your language?

What do you sell?

How do you sell?

Product

How does your employer make the money it uses to pay you?

Physical Goods

Retail

User Services

Professional Services

Software

Content

Gain Situational Awareness

What exactly is the situation you walked into?

People

Product

Environment

Approaching Your Role

Understand the Organization

Gain Situational Awareness

The State of Security

Make Changes

The State of Security

How do adversaries and your environment interact?

Attacks

Vendors

Program

Attacks

Common

- BEC
- Phishing
- Ransomware
- ATO
- DDoS

Industry-Specific

- Who are your industry's common vendors?
- Are you a consolidated vendor?

Company-Specific

- Your Insiders
- Your software and configurations

The State of Security

How do adversaries and your environment interact?

Attacks

Vendors

Program

Three Questions

What do you do?

What should we stop doing?

What should we start doing?

The State of Security

How do adversaries and your environment interact?

Attacks

Vendors

Program

Organization

- What does each organization do?
- Are they organized by asset classes, or *operational tasks*?
- Is their tempo measured in minutes, hours, days, or months?
- How do they add work?
- How do they park work?
- What don't they do?

Capability

- What activities need doing across all systems?
- Are they performed by system owners or specialists?
- Are metrics useful, universal, unambiguous?
- How do you know if the capability exists?

The State of Security

How do adversaries and your environment interact?

Attacks

Vendors

Program

Approaching Your Role

Understand the Organization

Gain Situational Awareness

The State of Security

Make Changes

Make Changes

Move fast on small changes and deliberately on large ones

Reorganization

Vision & Mission

Pillars

Make Changes

Move fast on small changes and deliberately on large ones

Initiatives

Buy-In

Sharing

Approaching Your Role

Understand the Organization

Gain Situational Awareness

The State of Security

Make Changes

How To CISO

VOLUME 1

THE FIRST 91
DAYS



Sink or Swim

A CISO's First 91 Days

Andy Ellis
Principal, Duha

How To
CISO