RSAC Studio

Connect to Protect

The First 12

An Hour-by-Hour Breakdown of a Threat Actor Inside Your Environment

ARMOR

Dr. Chase Cunningham
ECSA, LPT

HEAD OF THREAT RESEARCH & DEVELOPMENT, ARMOR

@CynjaChaseC

#RSAC

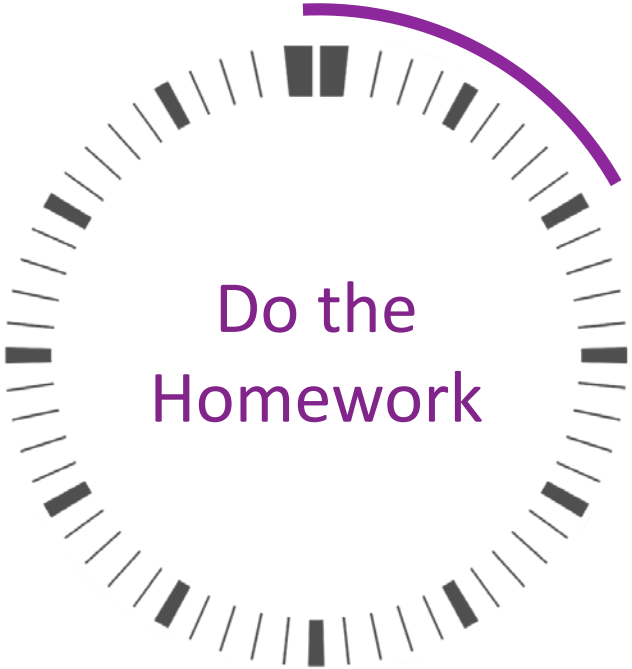
Hour 1

0100 HOURS

Finding the
Slow Gazelle

Hour 2

0200 HOURS



Map & Detail the Network, Users & Data Points

Hour 3

0300 HOURS

Dropping the Crosshairs

Hour 4

0400 HOURS

Poking Away at Easy Access Points

Hour 5

0500 HOURS

Unlocking
the Door

Hour 6

0600 HOURS

Let the
Data Flow

Hour 7

0700 HOURS

Hiding
Inside the
Network
Shadows

Hour 8

0800 HOURS

Planning the Escape with Your Data

Hour 9

0900 HOURS

It's Not Bolted Down?

Take it.

Hour 10

1000 HOURS

The Lucrative Link to Unfettered Entry

Hour 11

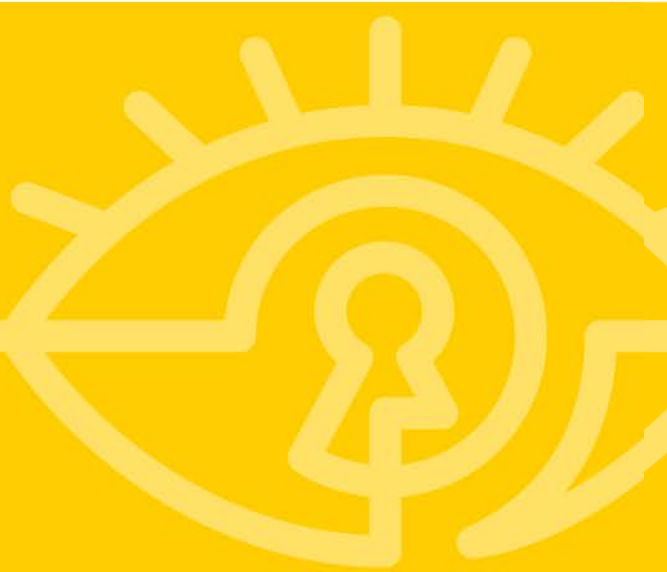
1100 HOURS

The Silent Exit

Hour 12

1200 HOURS

Cashing In on the Breach



Steps You Can Take So This Doesn't Happen To You

ARMOR

Changes to Apply Immediately

Find a Leader

Place someone in charge of cybersecurity who has the backing of the CEO.

Changes to Apply Immediately

Patch Everything

Update all patches across the board; out-of-date systems represent the most common security vulnerabilities.

Five Long-Term Objectives

Know Your Data

Design and implement a data classification program.
You can't defend what you don't understand.

Five Long-Term Objectives

Build a VTM Plan

Build a thorough vulnerability and threat management (VTM) program that will keep patches constantly updated and identify points of risk.

Five Long-Term Objectives

Create the Culture

Make security a culture change. Educating employees is more than sending one email a year with a simple multiple-choice test.

Five Long-Term Objectives

Layer Up

Implement a multilayered security environment that not only identifies and defeats inbound threats, but also watches and mitigates outbound traffic.

Five Long-Term Objectives

Be Honest

Decide if this is a war you can win with in-house resources. If there is even a little doubt, outsource to proven and trusted cybersecurity experts.

RSAC Studio

Connect to Protect

The First 12

An Hour-by-Hour Breakdown of a Threat Actor Inside Your Environment

ARMOR™

Dr. Chase Cunningham
ECSA, LPT

HEAD OF THREAT RESEARCH
& DEVELOPMENT, ARMOR

@CynjaChaseC

#RSAC