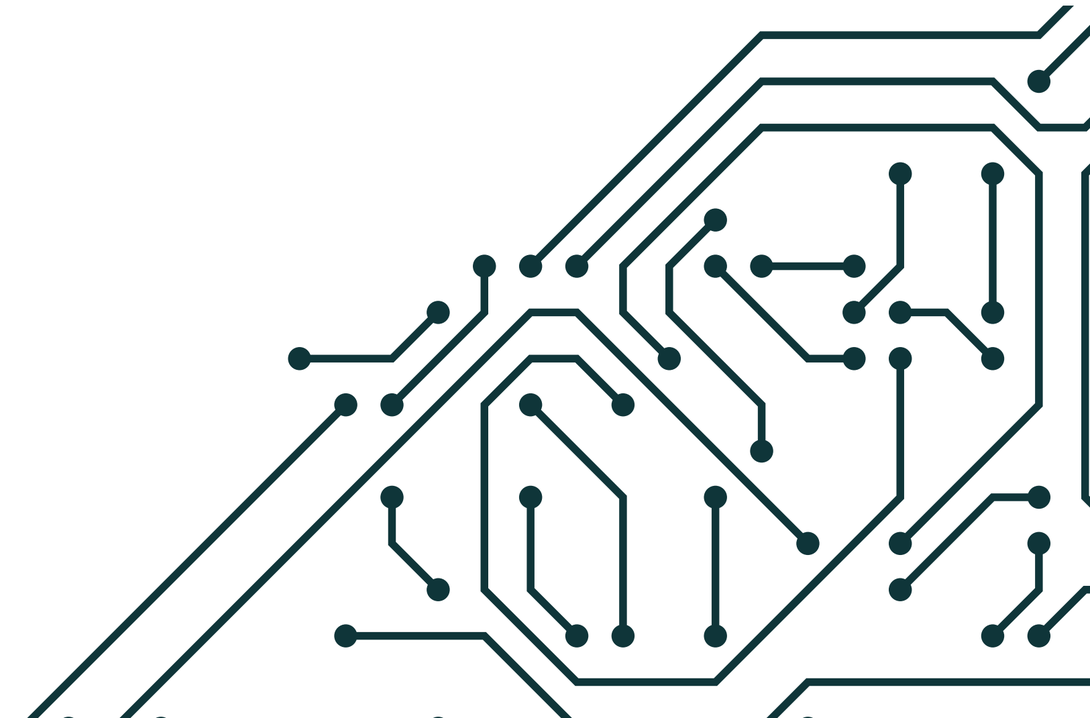
GIORGIO PERTICONE

# THE PITFALLS OF POOR REMEDIATION

How Companies Sabotage
Incident Response Efforts



# Giorgio Perticone

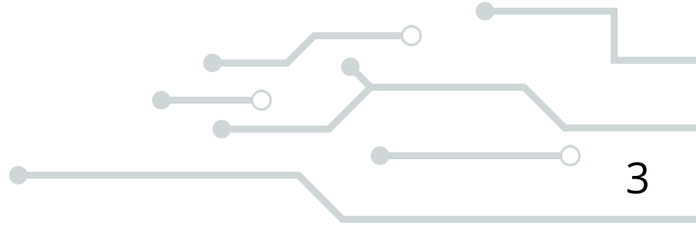
Just a guy obsessed with the idea of playing detective in front of a PC, catching bad (cyber) guys and saving (business) damsels in distress.

- Threat Detection & Response @ Vectra AI
- Cyber Security Podcast @ SECURITYbreak
- Co-Founder @ SecurityCert
- Previously contributor to: Bsides Milan, r00tMI
- Digital Nomad

# OBJECTIVES

**What’s the point of this talk**

1. Companies identify incidents faster
2. They are not able to respond effectively
3. Why and what can be done



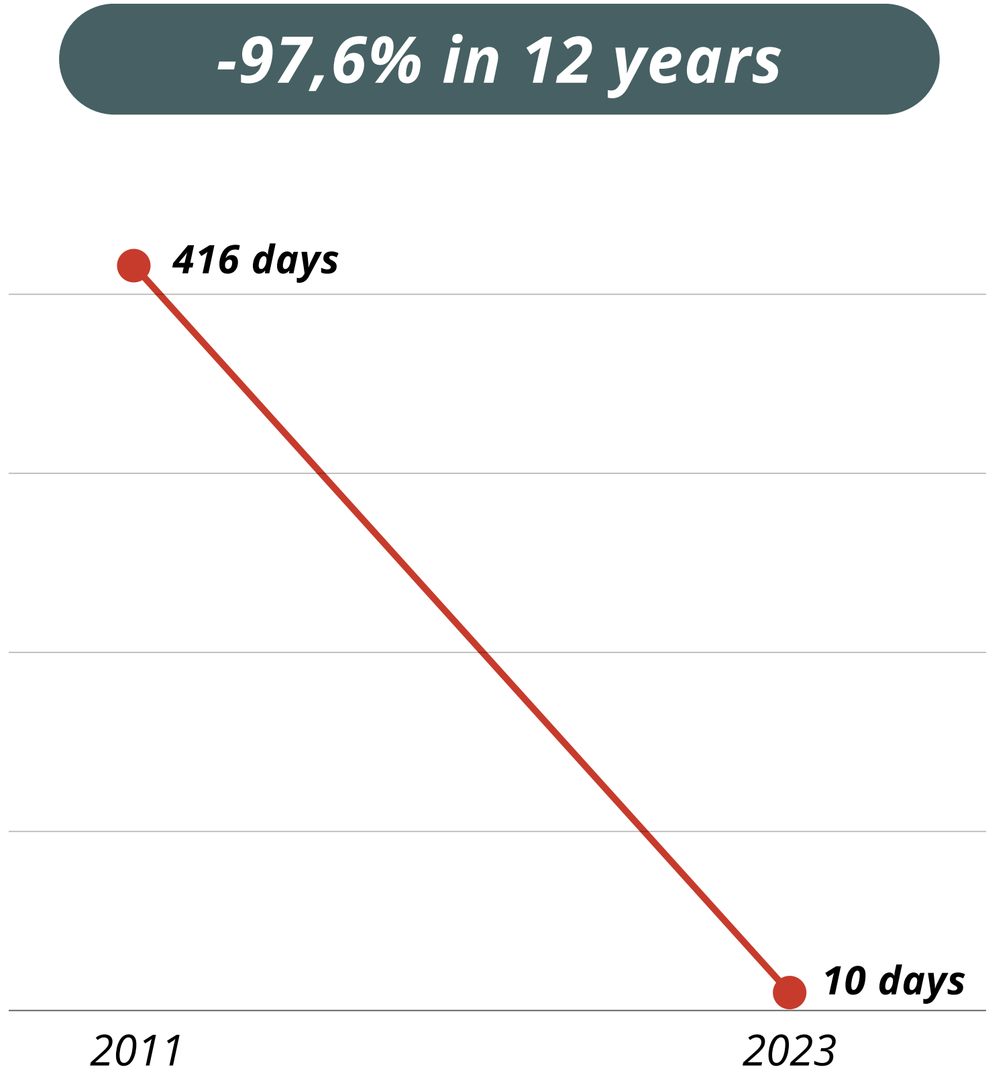
# WHAT'S THE PROBLEM?

# DWELL TIME HAS BEEN DECREASING

**WHY?**

- Detection technology advancement and adoption
- In-house SOC and MDR services development
- Ransomware Operators eventually notify orgs

***Dwell time***
*The number of days an attacker is present in a compromised environment before they are detected*




***Source:*** *Mandiant M-Trends 2024 report*

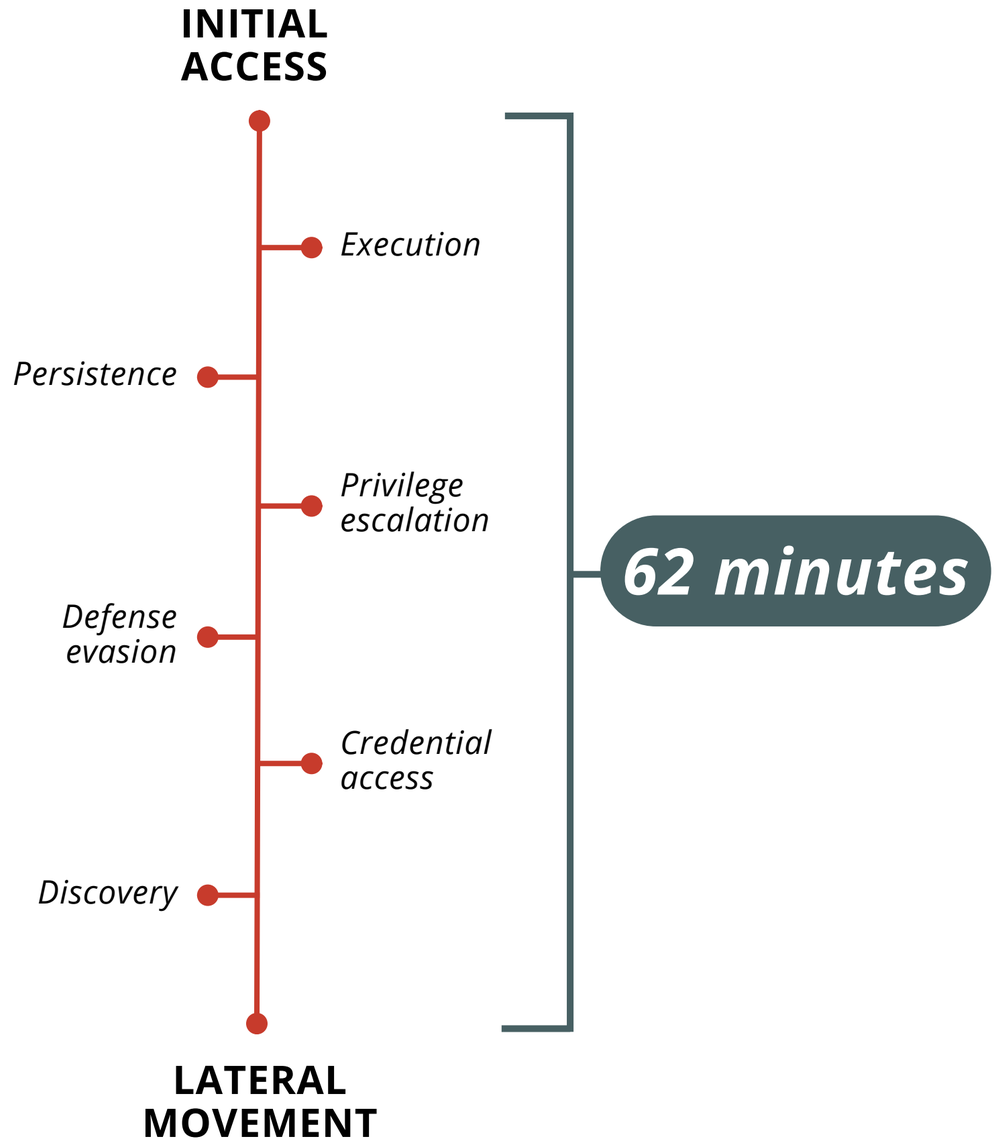
# BREAKOUT TIME IS ~1 HOUR

## MAIN THREAT CHANGED

***From:*** Stealth, Espionage-driven attacks aiming to spread their control over the network

***To:*** CyberCrime, Monetization-driven attacks aiming to ask for a Ransom

***Breakout time***
*The time it takes for an intruder to begin moving laterally outside of the initial foothold into the network*




***Source:*** *Crowdstrike Global Threat Report 2024*

# TIME TO CONTAIN & ERADICATE

**There is no value in Detection without Containment and Eradication.**

While complete Eradication can be postponed until the scope of the incident is clear, Containment should be immediate so to slow down the adversary and prevent worst case scenario.

# WHAT OPTIONS DO WE HAVE?

# USE CASES:
# DETECTION


## 1 USER ESCALATION

A user suspect something is off with their device or they’re being targeted, therefore reachout to the Security Team

## 2 SYSTEM ALERT

XDR, SIEM, AV or similar solutions trigger an alert because a certain item or activity matched a malicious signature (IoC) or behavior

# USE CASES:
# DETECTION

## INTERNAL

### 1 USER ESCALATION

A user suspect something is off with their device or they’re being targeted, therefore reachout to the Security Team

### 2 SYSTEM ALERT

XDR, SIEM, AV or similar solutions trigger an alert because a certain item or activity matched a malicious signature (IoC) or behavior

## EXTERNAL

### 3 THIRD PARTY NOTIFICATION

A Partner or Law Enforcement notify about some indicator identified on their side which suggest a potential compromise

### 4 ATTACKER RANSOM

Ransomware or Extorsion gangs reach out after encrypting and/or exfiltrating company data in order to obtain a Ransom

# USE CASES:
# CONTAINMENT


## 1 AUTOMATIC ACTION

Up-to-date XDR and SOAR products permit programmatic blocking of artifacts and devices based on triggers and thresholds

## 2 MANUAL INTERVENTION

Could require physical access to remote sites, and it implies verifications which slow down response

# USE CASES: CONTAINMENT

## VELOCITY

### 1 AUTOMATIC ACTION

Up-to-date XDR and SOAR products permit programmatic blocking of artifacts and devices based on triggers and thresholds

### 2 MANUAL INTERVENTION

Could require physical access to remote sites, and it implies verifications which slow down response

## PRECISION

### 3 ENDPOINT ISOLATION

Individual client device and user accounts containment affects a single employee productivity

### 4 NETWORK LOCKDOWN

Shutting down a Server or isolating an entire network will affect entire departments and may directly influence business lines

# WHAT CAN WE DO ABOUT IT?

# SECURITY vs BUSINESS CONTINUITY

### AUTOMATION IS RISKY

Automatic actions lack accountability, especially when containment is triggered by a False Positive alert

### BUSINESS CONTINUITY IS CRITICAL

Even if they are often considered antitheses, Business Continuity and Cyber Security aim to the same long-term goal

# SECURITY vs BUSINESS CONTINUITY

### AUTOMATION IS RISKY

Automatic actions lack accountability, especially when containment is triggered by a False Positive alert

### BUSINESS CONTINUITY IS CRITICAL

Even if they are often considered antitheses, Business Continuity and Cyber Security aim to the same long-term goal

### BUSINESS CRITICALITY RATING

Maintaning an accurate score of the business impact for every system downtime

- Leverage it to apply automation for lower scored assets
- Helps drive containment velocity over lesser priority incidents
- Leave to Security Team the responsibility over more critical assets

# LACK OF AUTHORITY

### MANUAL INTERVENTION TAKES TIME

Security analysts have a natural tendency to delay decision making to prevent repercussions when False Positives occur

### ANALYSTS LACK AUTHORITY

Security Teams are not empowered to autonomously apply containment on a network scale and to Servers.

This usually require time-consuming escalation processes.

# LACK OF AUTHORITY

### MANUAL INTERVENTION TAKES TIME

Security analysts have a natural tendency to delay decision making to prevent repercussions when False Positives occur

### ANALYSTS LACK AUTHORITY

Security Teams are not empowered to autonomously apply containment on a network scale and to Servers.

This usually require time-consuming escalation processes.

## INCIDENT COMMANDER ROLE

Guides an incident to its remediation, managing the resources, plan, and communication involved.

- Supervise Incident Response operations
- Act as a relay between the Security Team and Business Executives
- Is appointed with the authority to contain Critical Assets

# ANY QUESTIONS?

THANK YOU