BUSINESS CONTINUITY OUTSIDE THE PERIMETER

EYAL ESHEL | VP LATAM

eyal.eshel@cybereason.com

BUSINESS CONTINUITY IN THE NEW NORMAL

The world has changed

- Economies are under stress, some sectors are suffering more than others
- The entire workforce is disrupted, many businesses switched to 100% work from home
- The “perimeter” as we know it does not exist, home Wi-Fi is more risk, VPNs don’t scale up
- Security teams are overwhelmed, budgets are frozen
- Do you have a Business Continuity Plan (BCP) ?

In this presentation we will cover

- What can you do immediately, with the resources you have
- What are the latest attack trends and risks that we should be aware of
- What solutions and technologies can improve business continuity in the “new normal”

THINGS THAT YOU CAN DO.. NOW

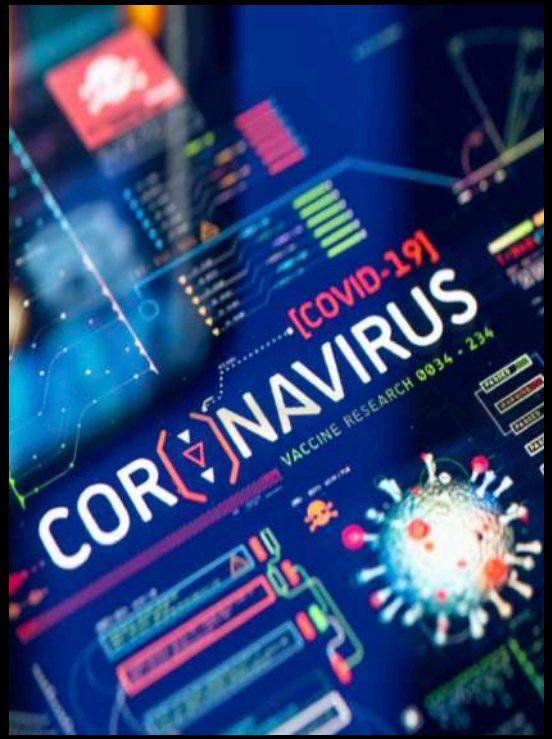
“securing the enterprise when no-one works from the office”

Identity: Do you use strong authentication in all cases and, if you suddenly switch it on, will people be able to do the things they are supposed to do?

Remote Access: Consider by department what data types are accessed and what the data exposure might mean from a risk perspective.

Endpoint Security: The endpoint is about to become the newest, most distributed place where your corporate data exists.

Mobile: The post-crisis day is coming where mobile is likely to be the hottest new risk area for many businesses.



Laptops and Desktops: In a very real way, every employee will be working on data that is outside the perimeter

Security Operations: Can your employees discuss ideas, talk, chat, meet *ad-hoc*, and exchange data securely?

Physical Security : Remember, not all employees have a home office and personal workspace outside the office like yours.

Business Continuity: If tomorrow you are attacked by ransomware, Do you know what to do, what not to do, who to call?

Business continuity: Think also Internal communication, team engagement, emotional support

PRACTICE GOOD CYBER HYGIENE

- Having secure passwords (12-16 characters, digits, letters, caps, special characters)
- Storing your secure password
- Two factor authentication
- Not use work devices for personal activities
- Only using secure routers
- Never use public Wi-Fi
- Beware of smart phishing campaigns (e-mail + text)
- Beware of free Mobile APPs and free PDF Converters, etc.

RISKS THAT YOU SHOULD BE AWARE OF

Phishing, Ransomware, Brute-force Attacks

COVIDLock Ransomware

In Costa Rica, a ransomware app called COVIDLock spread across the country in the second half of March, targeting individuals and companies. COVIDLock relied on the people's fear of the pandemic, claiming to prevent contagion by providing interactive maps of the virus' spread. Instead, the application hijacked victims' devices and demanded a ransom in the cryptocurrency bitcoin. The ransomware even tripped the alarms of

SLOCKER, ANDROID LOCKING TROJAN

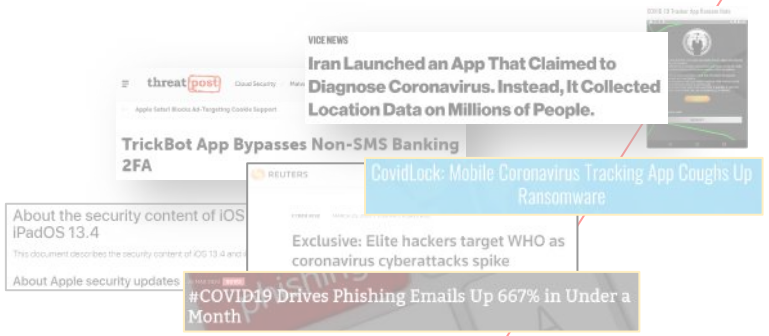
Congratulations!Your phone is blocked! You have 20 minutes to enter the code, otherwise the phone will not turn on again ...Don't see this as an arbitrary message, it will be difficult for you 🙂Unlock passwordExact timeTo unlock the code, call +998 998 910 312 Make 8000 paynet and get the code. (Don't ask for the code without Paynet, I won't tell you anyway)

Ransomware targets: Hospitals, school districts, state and local governments, law enforcement agencies, small businesses, large businesses, Coronavirus vaccine university research

MOBILE-GEDDON

(ALREADY HERE?)

2020



2019

60% MOBILE > 40% LAPTOPS

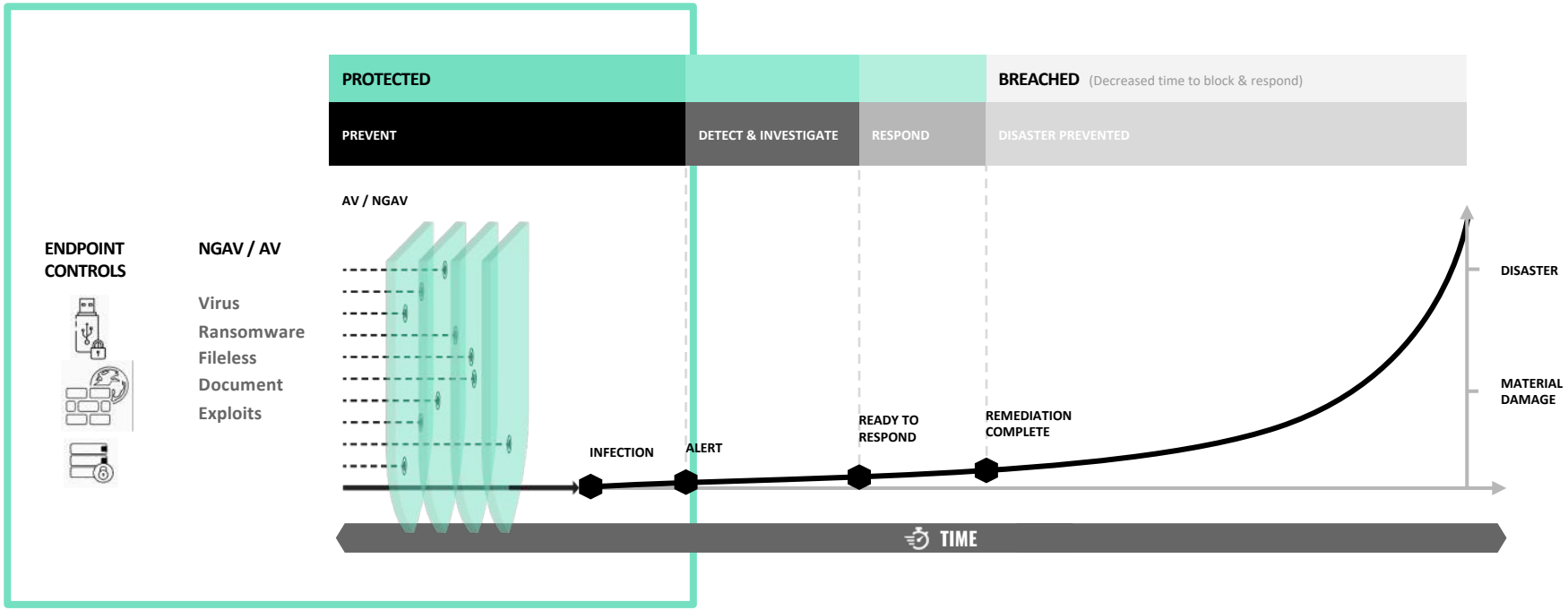
¼ COMPAMNY OWNED
¾ BYOD

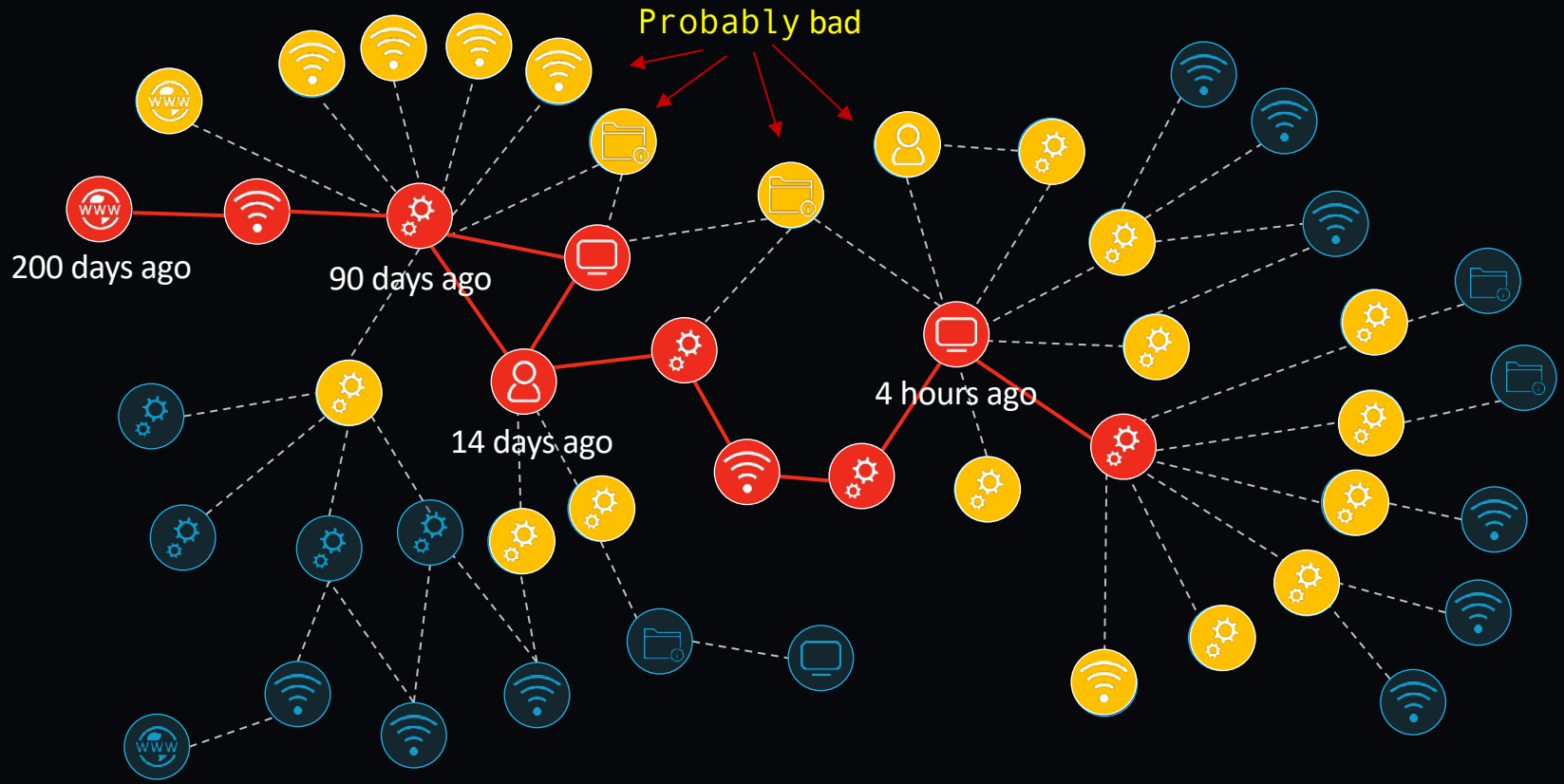
MOBILE MALWARE IS
30% OF ALL MALWARE

2 OUT OF 3
EMAILS ARE OPENED ON
A MOBILE DEVICE

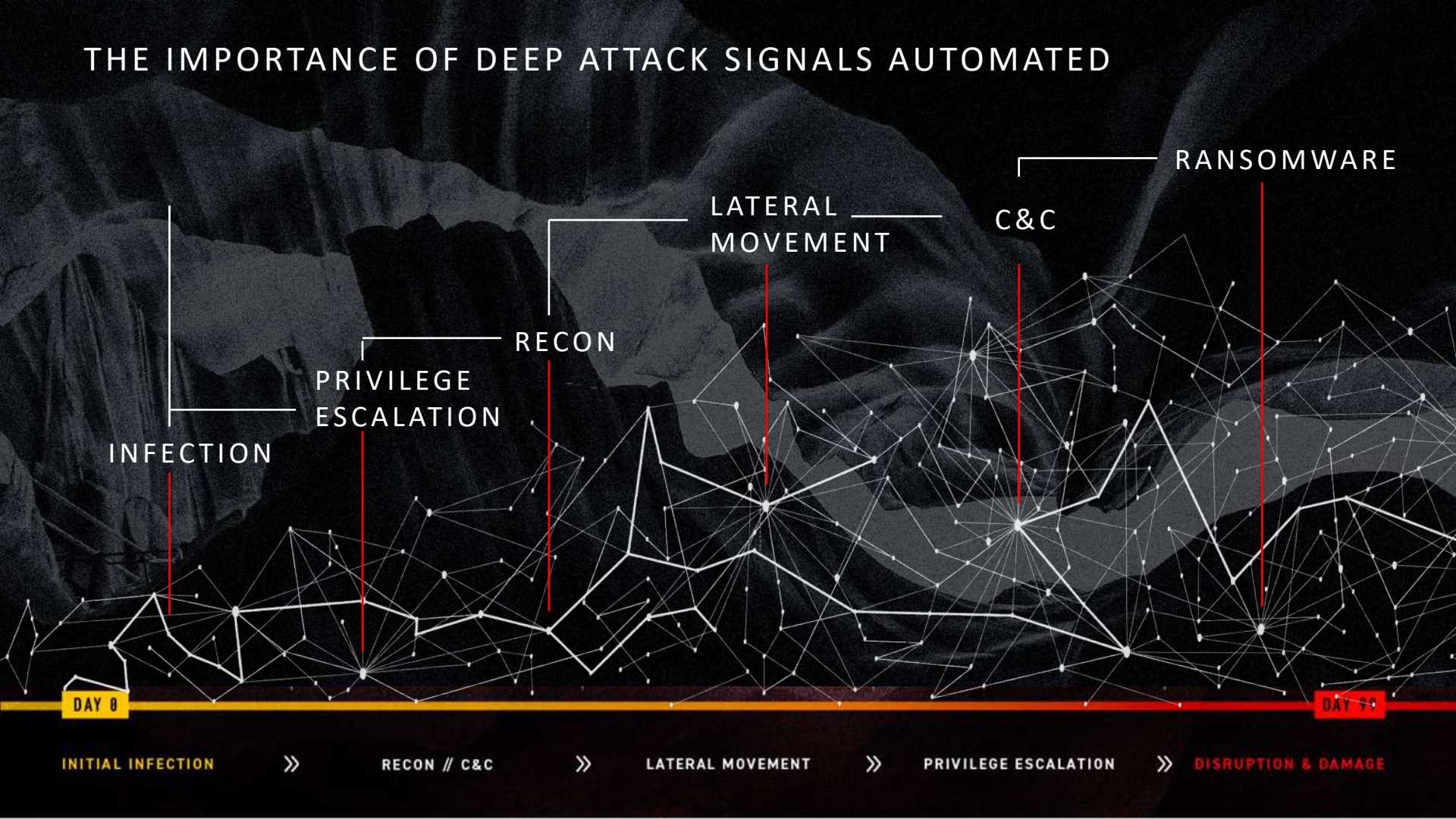
STEPS THAT YOU CAN TAKE TO PROTECT

GAIN THE UPPER HAND: *MULTI-LAYERED PREVENTION*




Probably bad
200 days ago
90 days ago
14 days ago
4 hours ago

THE IMPORTANCE OF DEEP ATTACK SIGNALS AUTOMATED



Manufacturing Under Attack → Resolved in 36H

Ransomware stands no chance vs. Cybereason

INDUSTRY
Manufacturing

CURRENT SOLUTIONS
EDR, AMS

Time to Resolution
36 hours

SIZE OF SECURITY TEAM
4 full-time staff

NUMBER OF ENDPOINTS
18,000

Situation

7pm Sunday | Hit by Ransomware

- **"My entire server infrastructure is down we need help"**
- 700+ Servers encrypted
- Breach originated in part of network not covered by Cybereason
- Attempt to contain by internal SOC failed
- AMS alerted customer and IR team

Result

- **Breach 2 Board Room with Remediation Complete in 36 hours**
- **Expanded Cybereason deployment to protect entire infrastructure**

Action

7am Monday

- We knew what data was exfiltrated
- Who the actors were
- Contained + TI Report

7am Tuesday

- Full Remediation Complete
- Attack Story & Timeline Sent
- Critical Infrastructure Secured
- Report shared with customer on details of the breach & necessary actions to take to protect this from happening again

REMOTE WORKFORCE PROTECTION BUSINESS CONTINUITY

NEXT GENERATION ANTIVIRUS

ENDPOINT DETECTION & RESPONSE

MANAGED DETECTION & RESPONSE

MOBILE DEFENSE

REMOTE INCIDENT RESPONSE

Q&A + FREE RESOURCES

[Webinars](#) [Blog](#) [Malicious Life Podcast](#)

Eyal Eshel: eyal.eshel@cybereason.com

E-mail me for a Business Continuity Emergency Checklist