

APRESENTAÇÃO SOLUÇÃO IOT INTERNET DAS COISAS

JULHO DE 2021



50B

Connected
Devices

NOT SO
INNOCENT

Unprotected
storage

Hardcoded
backdoors

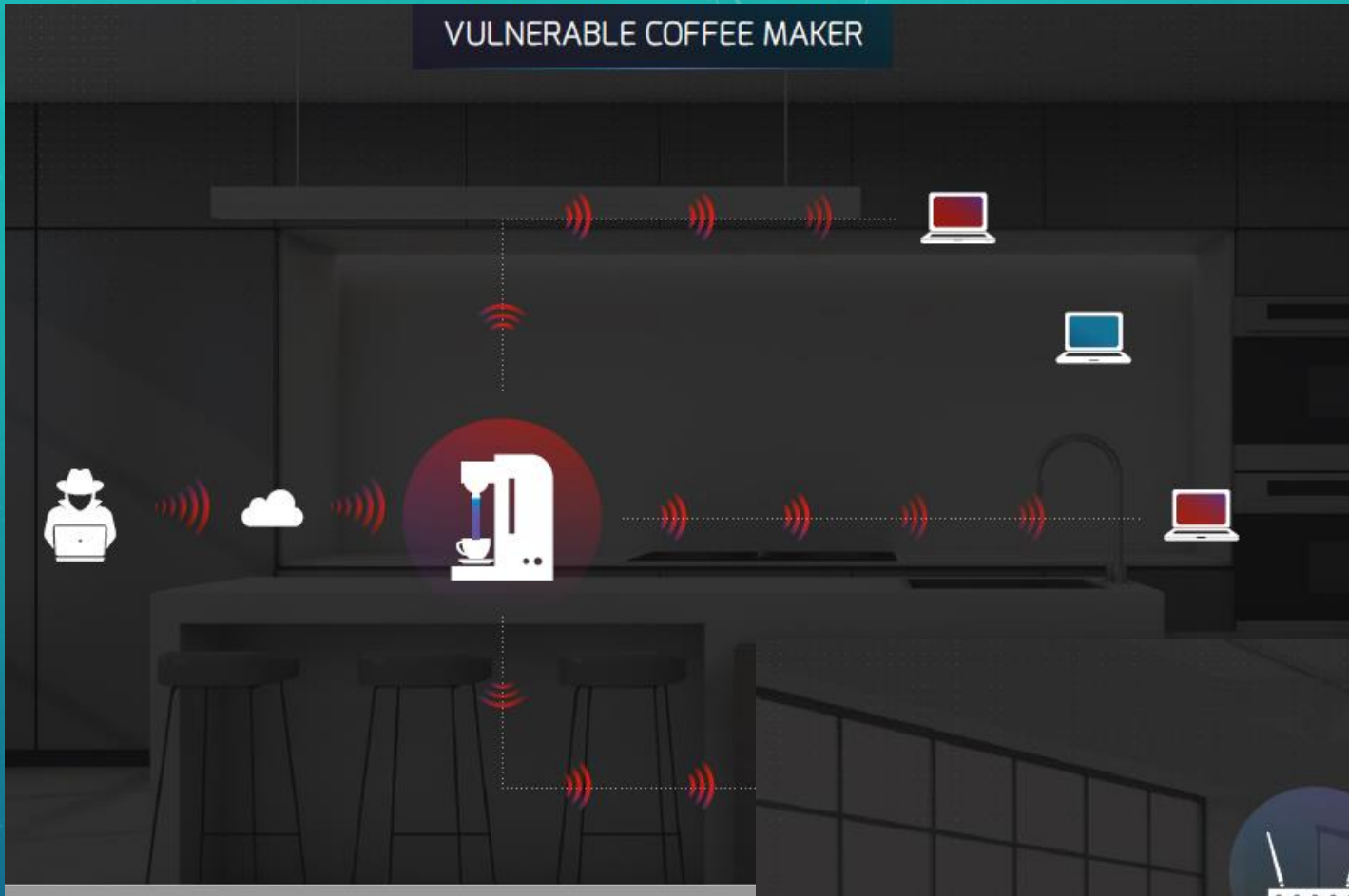
Unencrypted
communication

Vulnerable web/
mobile/cloud interface

Insecure pairing
procedures

No security
patches

VULNERABLE COFFEE MAKER



ROGUE AP



SOLUÇÃO IOT – O QUE FAZ?

- 1) FORNECE VISIBILIDADE COMPLETA DE TODOS OS DISPOSITIVOS CONECTADOS ATRAVÉS DE WIFI E BLUETOOTH
- 2) ALAVANCA CIÊNCIA DE DADOS PARA CRIAÇÃO DE PERFIL DE DISPOSITIVOS E COMPORTAMENTOS
- 3) DETECÇÃO DE VULNERABILIDADES E AMEAÇAS, E MITIGAÇÃO DE ATAQUES EM TEMPO REAL

SENSORES IOT



Tela inicial do painel de controle

SECURITY

VISIBILITY

OPERATIONS

REPORTS



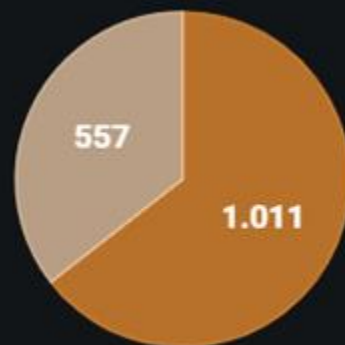
Incidents Breakdown

TODAY THIS WEEK

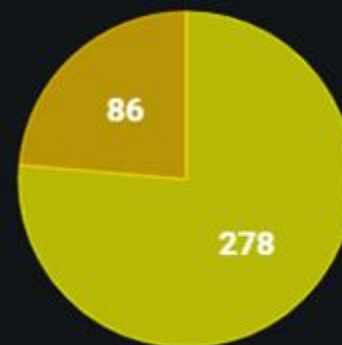
Attacks (0) ⓘ



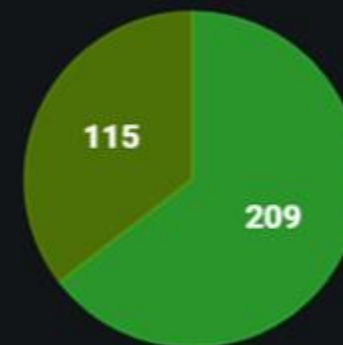
High (1568) ⓘ



Medium (364) ⓘ



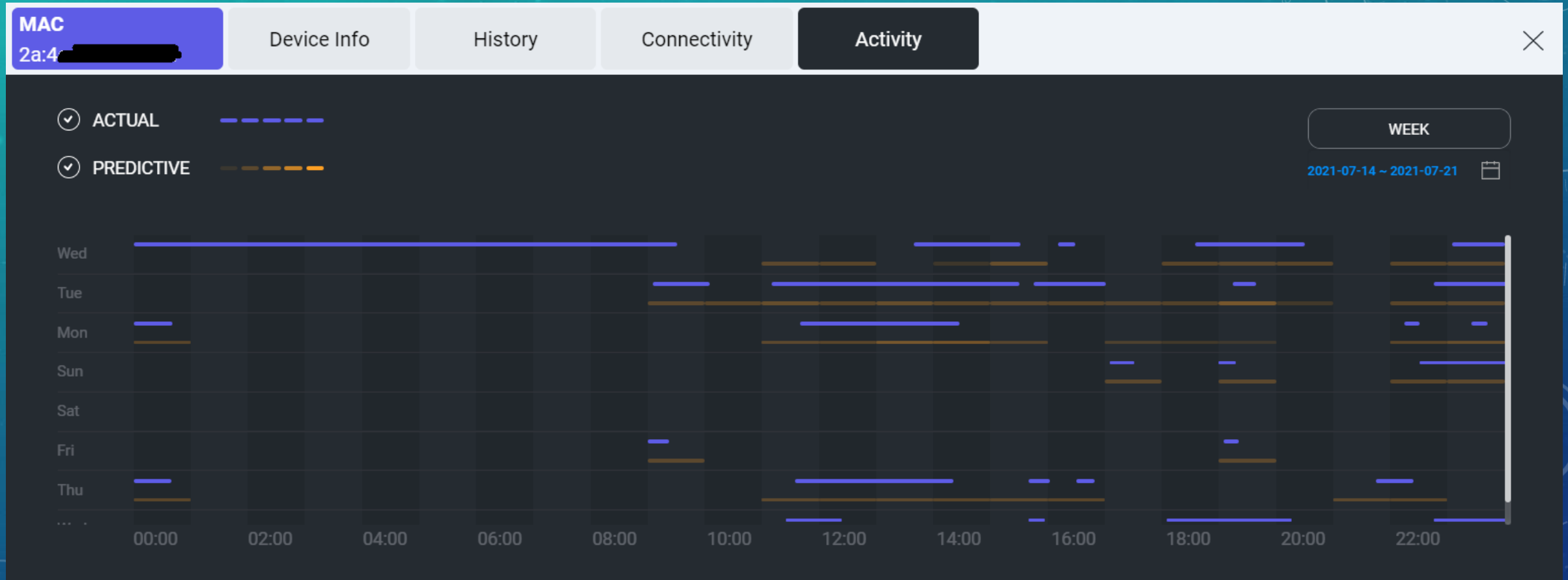
Low (324) ⓘ



Aba de Dispositivos

Goldlock									
SECURITY									
VISIBILITY									
OPERATIONS									
RECENT PAST HOUR TODAY THIS WEEK									
Visible Networks 226 Corporate Networks 2 Devices 1960									
Enter search phrase									
PROTOCOL	TYPE	VENDOR	NETWORK	LOCATION	ON-PREMISE	FIRST SEEN	LAST SEEN	MAC	
	Guest	N/A	#NET-CLARO-WIFI_EXT	Floor 1	Out	03/10/2020 22:59:25	03/10/2020 23:05:05	98:da:c4:00:00:00	
	Guest	N/A	camillo1	Floor 1	Out	02/26/2020 08:30:08	03/10/2020 23:04:41	f0:72:ea:00:00:00	
	Guest	SamsungE	#NET-CLARO-WIFI	Floor 1	Out	03/09/2020 12:45:38	03/10/2020 23:04:40	50:92:b9:00:00:00	
	Guest	BelkinIn	belkin.b86.media	Floor 1	In	02/26/2020 08:51:39	03/10/2020 23:04:21	ec:1a:59:00:00:00	
	Guest	Tecnomen	Marcelo	Floor 1	Out	02/26/2020 08:28:29	03/10/2020 23:04:12	00:e0:20:00:00:00	
	Guest	N/A	Covidados	Floor 1	Out	02/26/2020 08:28:19	03/10/2020 23:04:06	78:8b:ca:00:00:00	
	Guest	Tp-LinkT	Camillonet3	Floor 1	Out	02/26/2020 08:28:19	03/10/2020 23:04:06	7c:8b:ca:00:00:00	
	Guest	N/A	Not connected	Floor 1	In	03/09/2020 13:35:35	03/10/2020 23:04:04	10:3D:0A:00:00:00	
	Guest	Sagemcom	LFTF1	Floor 1	Out	02/26/2020 08:28:29	03/10/2020 23:04:03	00:37:b7:00:00:00	
	Guest	ArrisGro	#NET-CLARO-WIFI	Floor 1	Out	02/26/2020 10:48:40	03/10/2020 23:03:34	fa:2d:c0:00:00:00	
	Corporate	Apple	belkin.b86	Floor 1	Out	02/26/2020 08:42:47	03/10/2020 23:03:13	00:56:cd:00:00:00	

Aba de Informações de um dispositivo específico



Aba de Redes

Goldlock

SECURITY

VISIBILITY

OPERATIONS

Visible Networks

226

Corporate Networks

2

Devices

1959

RECENT

PAST HOUR

TODAY

THIS WEEK

Q Enter search phrase

ESSID	# APs	FIRST SEEN	LAST SEEN		SIGNAL
%23NET-CLARO-WIFI	41	02/26/2020 08:28:19	03/10/2020 22:59:27		
%23NET-CLARO-WIFI_EXT	1	03/10/2020 22:59:25	03/10/2020 22:59:24		
Marcelo	3	02/26/2020 08:28:19	03/10/2020 22:59:02		
770-2-4	1	02/26/2020 08:28:19	03/10/2020 22:58:53		
FucsHome 2.4G	1	02/26/2020 09:05:53	03/10/2020 22:58:52		
belkin.b86	1	02/26/2020 08:28:19	03/10/2020 22:58:52		
Cafofo	1	02/26/2020 08:28:38	03/10/2020 22:58:37		
CASA1	1	02/26/2020 08:29:24	03/10/2020 22:58:33		
Covidados	1	02/26/2020 08:28:19	03/10/2020 22:58:28		
Barbalho	1	02/26/2020 08:28:19	03/10/2020 22:58:28		
Mp_veiga 2g	1	02/26/2020 08:28:30	03/10/2020 22:58:21		
Marcelo-5G	1	02/26/2020 08:28:30	03/10/2020 22:58:10		

Aba de Operações

Mostra os detalhes e status de cada sensor

SECURITY VISIBILITY OPERATIONS REPORTS						
All 5 Active 3 Inactive 2						
Enter Protect ID						
PROTECT ID	LOCATION	PROTECT STATUS	IP	LAST COMMAND	ACTIONS	
p_IL_TelAviv_20200114_111501	N/A	Protect Mode	201.13.47.47			
p_IL_TelAviv_20200114_111456	Fix	Protect Mode	201.13.47.47			
p_IL_TelAviv_20200114_111453	N/A	Protect Mode	201.13.47.47			
p_IL_TelAviv_20200114_111508	Fix	Not Connected	177.139.154.54			
p_IL_TelAviv_20200114_111454	N/A	Not Connected	201.13.47.47			

Aba de Notificações

Mostra os tipos de ataques e vulnerabilidades que o sistema detecta e mitiga, além de poder enviar alertas por email

The screenshot displays the 'Notifications' settings interface. On the left, a sidebar contains the following menu items: 'User Settings', 'Profile information', and 'Notifications preferences' (which is currently selected). The main content area is titled 'Notifications' and features a 'Disabled' toggle switch. Below the title is a list of notification types, each with three checkboxes for enabling notifications via email, SMS, and push. The list includes:

Notification Type	Email	SMS	Push
1 Malicious Wi-Fi AP	☐	☐	☐
2 WPS Vulnerability Detected	☐	☐	☐
3 WPS Brute Force Attack	☐	☐	☐
6 Deauthentication Flood	☐	☐	☐
7 Customer network unknown ap	☐	☐	☐
8 New Corporate Station Detected	☐	☐	☐
9 Illegal Frame Type/Subtype	☐	☐	☐
10 Device changed his behavior and network signature	☐	☐	☐

At the bottom of the settings panel are two buttons: 'Cancel' and 'Save'.

Notifications

Disabled ☐

13	Corporate Device Degraded Security	☐	☐	☐
15	Wi-Fi Covert Channel	☐	☐	☐
16	Host Scan Detected	☐	☐	☐
17	Authentication Flood	☐	☐	☐
18	Denial-of-Service Attack	☐	☐	☐
19	Deassociation attack	☐	☐	☐
50	Man-in-the-Middle	☐	☐	☐

Notifications

Disabled ☐

310	New Corporate Device Detected	☐	☐	☐
311	Rogue Device	☐	☐	☐
312	(Insecure) (hidden) Rogue AP	☐	☐	☐
313	Suspicious Device (in the area / on-premise)	☐	☐	☐
314	Corporate Device Hotspot External Connection	☐	☐	☐
317	Corporate Device Insecure Behavior	☐	☐	☐
320	Corporate AP Disappeared	☐	☐	☐

Cancel

Save

Goldlock

SECURITY

VISIBILITY

OPERATIONS

Suspicious AP Detected

An access point broadcasting a suspiciously similar ESSID to your corporate network was detected

Risk: **CRITICAL**

Location: N/A

Seen by: N/A

Start Time: 03/10/2020 15:26:47

End Time: 03/10/2020 15:26:47

Goldlock

SECURITY

VISIBILITY

OPERATIONS

WPS Vulnerability Detected

A corporate access point is vulnerable to a WPS brute force attack

Risk: **HIGH**

Location: N/A

Seen by: N/A

Start Time: 03/10/2020 06:58:10

End Time: 03/10/2020 23:12:13

Similar MAC - OPN vs. WPA2

A new AP detected as another interface on a corp device with different enc

Risk: **LOW**
Location: N/A
Seen by: N/A
Start Time: 03/08/2020 16:22:40
End Time: 03/08/2020 18:44:07

Watchlist Device Appeared

A device previously added to the watchlist has appeared

Risk: **HIGH**
Location: N/A
Seen by: N/A
Start Time: 02/27/2020 10:18:42
End Time: On going

LOCATION	STATION MAC	STATION VENDOR
N/A	ec:9b:f3:0a:66:94	SamsungE

Aba de Criação de Regras para ações de segurança

Create rule

Please select the desired properties for each section to create a new rule

Corporate device cannot connect to select network

Actions:

Alert **Yes** No

Mitigate Yes **No**

Severity:

Low Medium High

Rule name:

☐ non

any

corporate

SPECIFIC

mac

ssid

VULNERABLE

wps

Cancel

Create

Aba de Mitigações

RECENTPAST HOURTODAY1 WEEKPAST MONTH

Ongoing Mitigations0

Devices Mitigated2

Networks Mitigated1

APs Mitigated2

Export

Search

Target Vendor	Network	Start Time	End Time	Target Mac	Network Mac
IntelCor	belkin.b86	05/24/2021 14:51:49	05/24/2021 14:56:58	64:32	ec:1a:
SamsungE	belkin.b86	05/24/2021 14:52:27	05/24/2021 14:57:50	68:7d	ec:1a:

Aba de Políticas e Regras Criadas

POLICIES

2

Search

NAME	DESCRIPTION	Status
CY-POL-001	Corporate Device Cannot Connect To Non Corporate Access Point	
CY-POL-002	Any Device Cannot Connect To Suspicious Network	