APP ANTI-HACKER PARA PROTEÇÃO E BLINDAGEM DE SMARTPHONES

JULHO/2021

GOLDLOCK
Gold Line Group Ltd

- A GOLD LOCK FOI FUNDADA EM 2003 EM ISRAEL E CHEGOU AO BRASIL EM 2005
- FOI A PIONEIRA NA TECNOLOGIA DE CRIPTOGRAFIA PARA TELEFONES CELULARES
- PRESENTE EM MAIS DE 20 PAÍSES E EM TODOS OS CONTINENTES
- LÍDER DE MERCADO GLOBAL NESSE SEGMENTO
- REFERÊNCIA MUNDIAL NA PROTEÇÃO DE DISPOSITIVOS MÓVEIS
- LICENCIADA PELO MINISTÉRIO DE DEFESA DE ISRAEL
- REPRESENTA NO BRASIL EMPRESAS DE EUA, ISRAEL E SUÍÇA
- CRIOU O VAULT OS, O SISTEMA OPERACIONAL BLINDADO DA GOLD LOCK
- CLIENTES ALTAMENTE SATISFEITOS: GRANDES EMPRESAS PRIVADAS E PÚBLICAS, ÓRGÃOS GOVERNAMENTAIS E MILITARES

ALGUNS PRÊMIOS E RECONHECIMENTOS DA SOLUÇÃO

CYBERSECURITY EXCELLENCE AWARDS 2020: GOLD WINNER IN MOBILE THREAT DEFENSE – ZPLATFORM

CYBERSECURITY EXCELLENCE AWARDS 2020: SILVER WINNER IN BEST CYBERSECURITY COMPANY

Most Innovative Enterprise Mobile Threat Defense - 2020
Next Gen Application Security – 2020
Best Product Mobile Endpoint Security - 2020
Best Product Artificial Intelligence and Machine Learning - 2020

Best Application Security in 2019

Cybersecurity Excellence Awards 2019: Best Mobile Application Security - zIAP

z9™: MECANISMO DE DETECÇÃO PATENTEADO PROJETADO PARA CELULARES

O mecanismo de detecção z9™ usa aprendizado de máquina para fornecer proteção em tempo real no dispositivo contra ameaças conhecidas e desconhecidas

zIPS™

Identificação dos riscos

Riscos do dispositivo
- Vulnerabilidades
- Sem criptografia no dispositivo
- Jailbreaks
- Perfis não gerenciados

Riscos dos Apps
- Apps não seguros
- Sideloaded Apps

Riscos das Redes
- Scans de reconheciment.
- Wifi não seguro

Detecção de Ameaças

Dispositivo comprometido
- Rooted Device
- Privilégios elevados
- System Tampering

Phishing Sites

Apps maliciosos

Ataques às redes
- MITM Attacks
- Rogue Access Points

Remediação

Ações do MDM
- Limpar dados
- Terminar o acesso

Bloquear Sites de Phishing

Redes
- Disconectar WiFi
- Disconectar Bluetooth
- Network Sinkhole

Samsung KNOX
- Prevenir instalação App
- Desinstalar Apps

Reporte

Dados Forenses

Integrações com SOC
- SIEMs
- EDRs

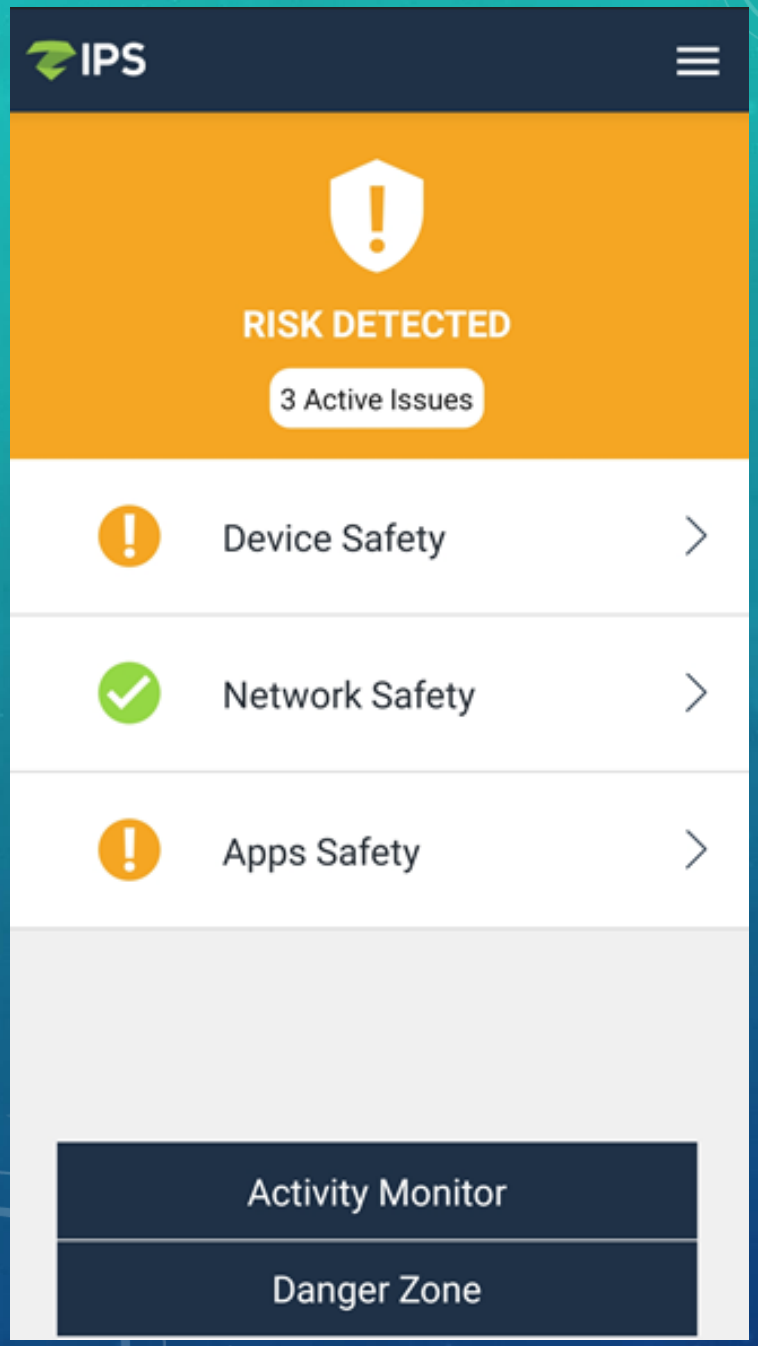
Threat Hunting

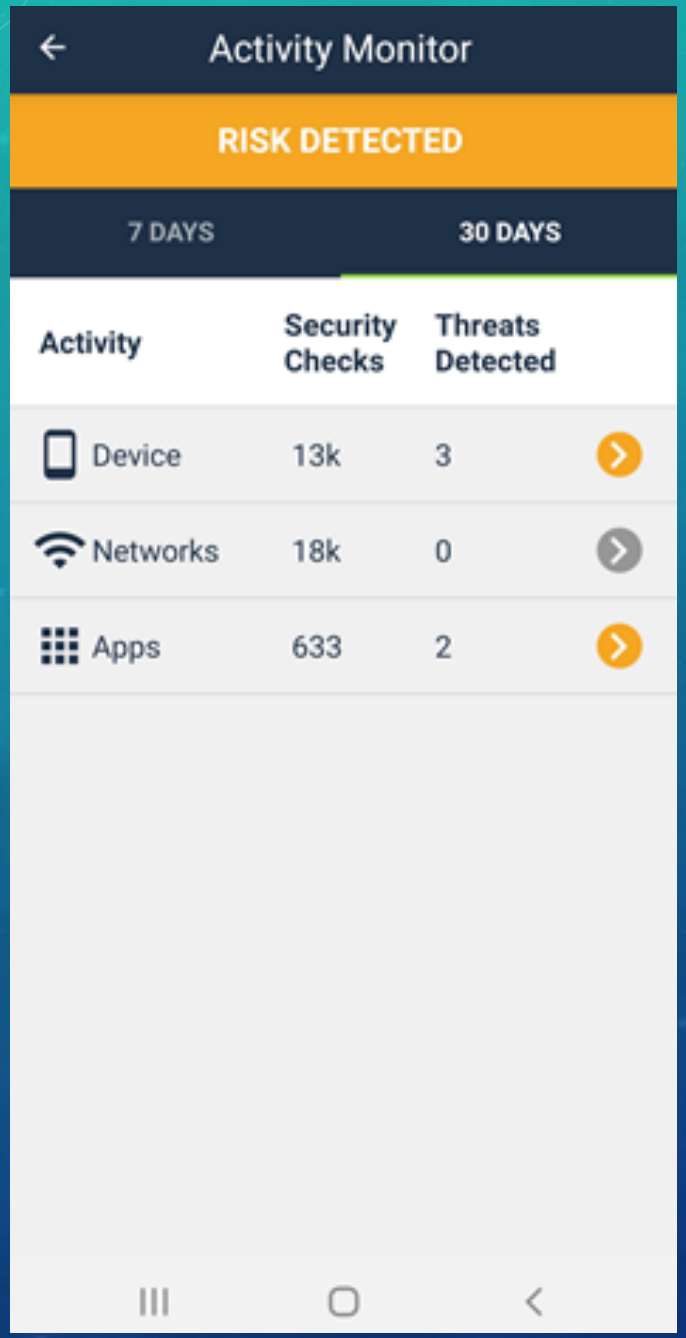
Princípios fundamentais de design

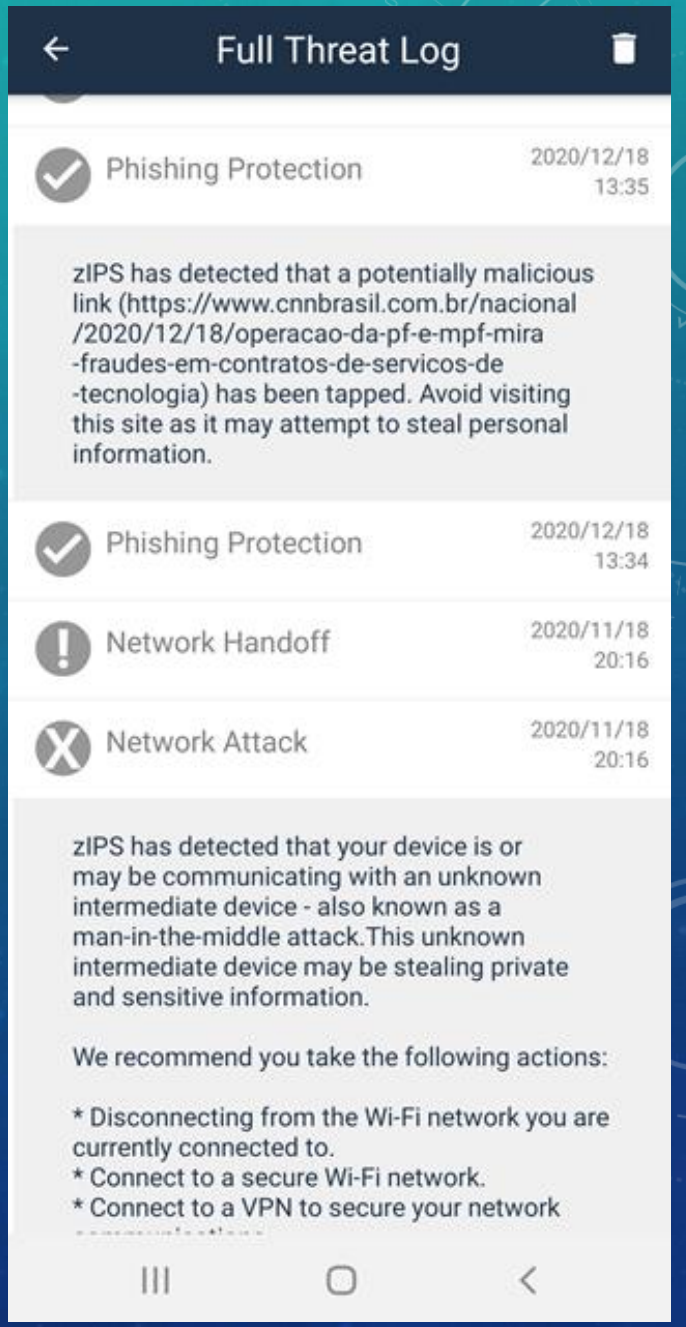
- Capabilidades e escalabilidade
- Detecção de ameaças conhecidas e desconhecidas
- Privacidade e transparência
- Fornece console de gerenciamento em qualquer nuvem ou local
- Opera com vários UEMs simultaneamente

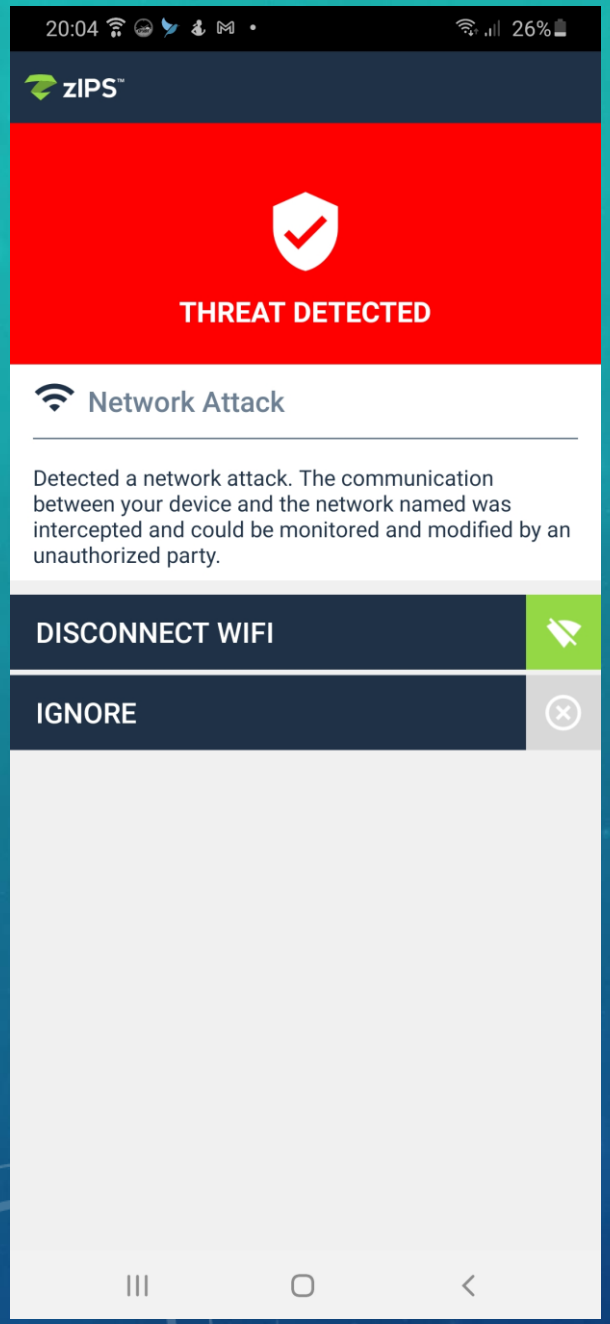
App anti-hacker para proteção de smartphones

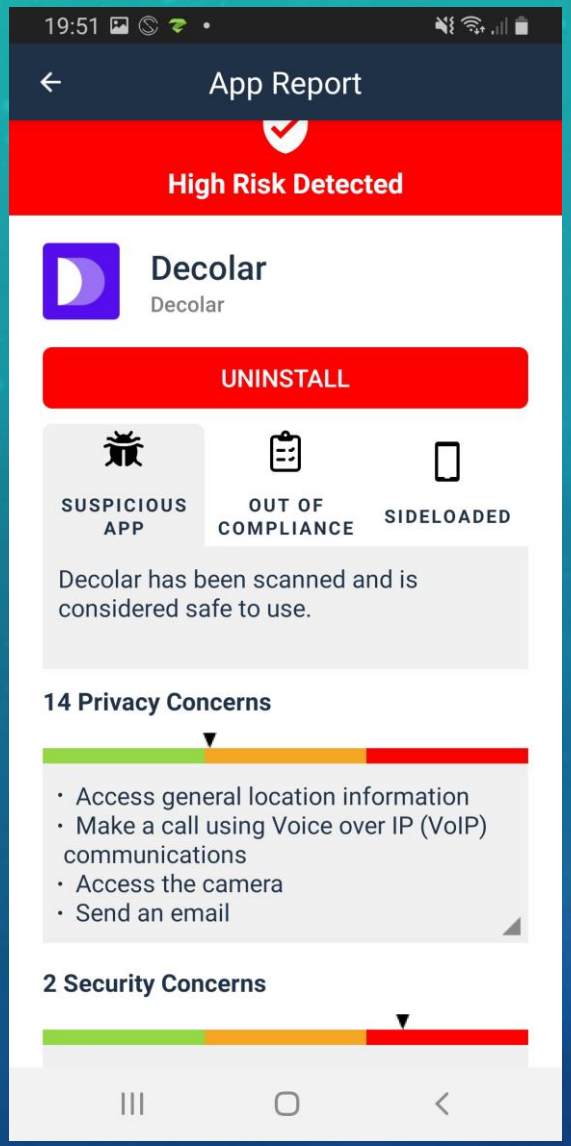
- Varredura do dispositivo, redes Wifi e apps
- Detecta comportamentos maliciosos e ameaças conhecidas e desconhecidas em tempo real
- Analisa desvios no comportamento do dispositivo e identifica os tipos de ataque
- Remedia através de rápidas recomendações e decisões quando uma atividade maliciosa é descoberta
- Utiliza inteligência artificial e aprendizado de máquina para evitar ataques como MITM, Phishing Malware e zero-day, entre outros
- Painel Web com dados forenses

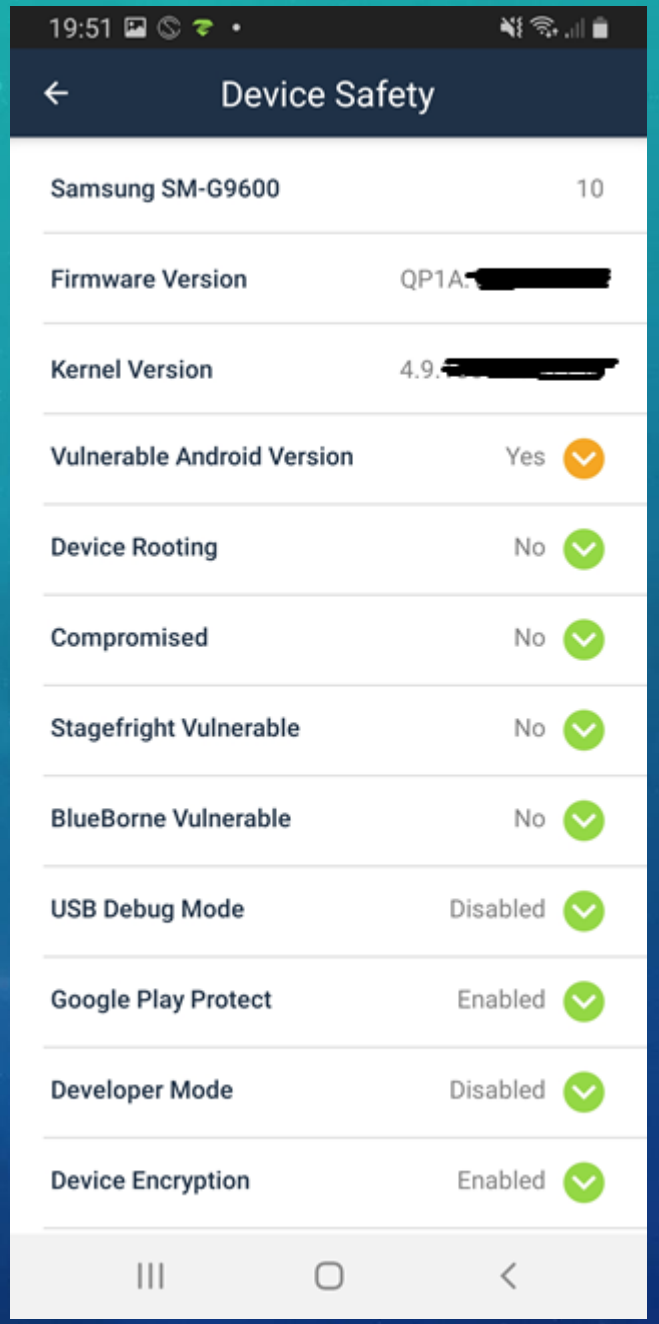

IPS
RISK DETECTED
3 Active Issues
Device Safety
Network Safety
Apps Safety
Activity Monitor
Danger Zone

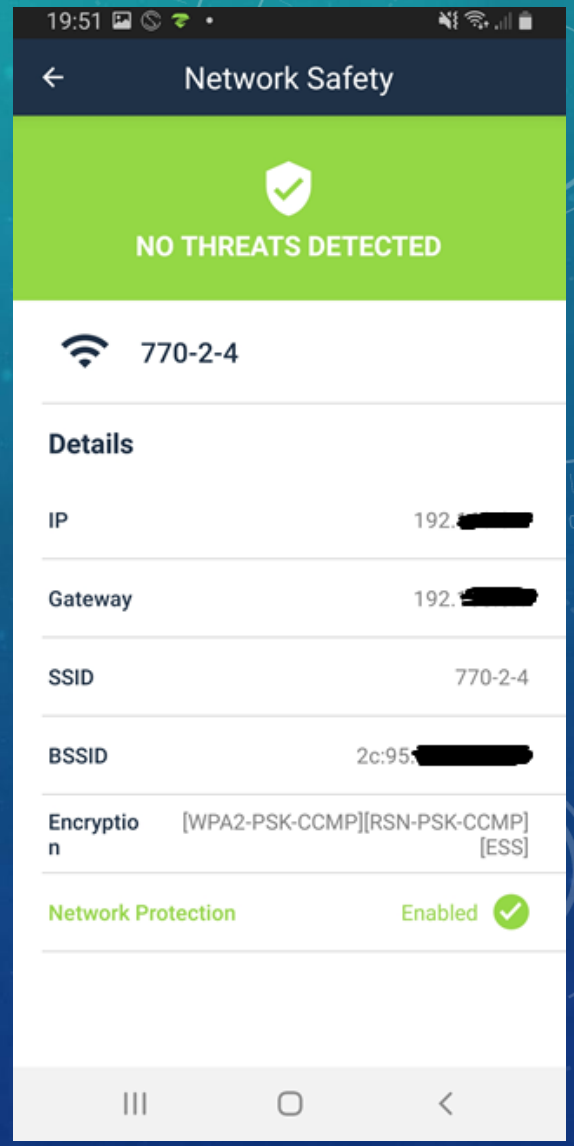

Activity Monitor
RISK DETECTED
7 DAYS
30 DAYS
Activity
Security Checks
Threats Detected
Device 13k 3
Networks 18k 0
Apps 633 2


Full Threat Log
Phishing Protection
2020/12/18 13:35
zIPS has detected that a potentially malicious link (https://www.cnnbrasil.com.br/nacional/2020/12/18/operacao-da-pf-e-mpf-mira-fraudes-em-contratos-de-servicos-de-tecnologia) has been tapped. Avoid visiting this site as it may attempt to steal personal information.
Phishing Protection
2020/12/18 13:34
Network Handoff
2020/11/18 20:16
Network Attack
2020/11/18 20:16
zIPS has detected that your device is or may be communicating with an unknown intermediate device - also known as a man-in-the-middle attack.This unknown intermediate device may be stealing private and sensitive information.
We recommend you take the following actions:
* Disconnecting from the Wi-Fi network you are currently connected to.
* Connect to a secure Wi-Fi network.
* Connect to a VPN to secure your network


20:04
26%
zIPS
THREAT DETECTED
Network Attack
Detected a network attack. The communication between your device and the network named was intercepted and could be monitored and modified by an unauthorized party.
DISCONNECT WIFI
IGNORE

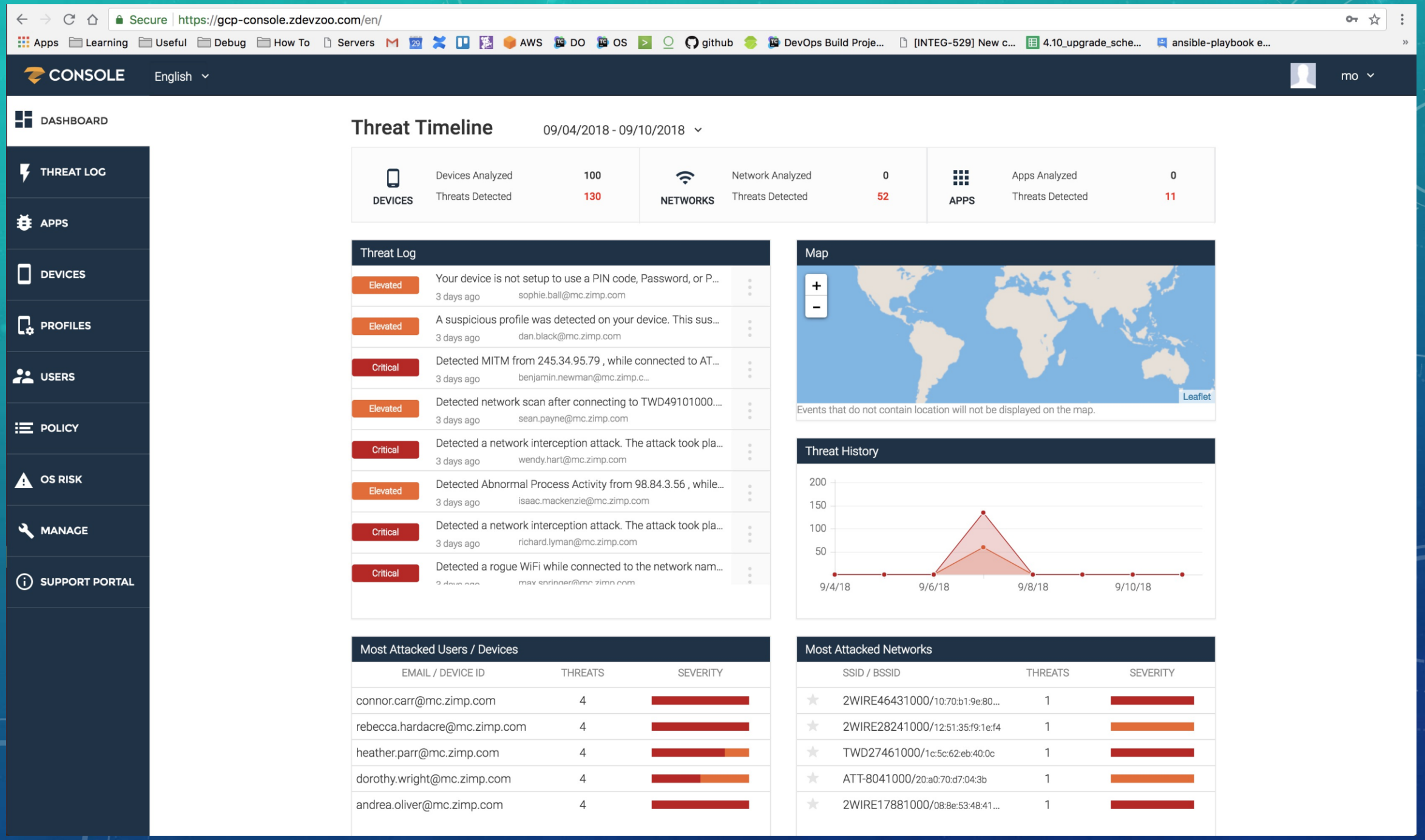

19:51
App Report
High Risk Detected
Decolar
Decolar
UNINSTALL
SUSPICIOUS APP
OUT OF COMPLIANCE
SIDELOADED
Decolar has been scanned and is considered safe to use.
14 Privacy Concerns
· Access general location information
· Make a call using Voice over IP (VoIP) communications
· Access the camera
· Send an email
2 Security Concerns


19:51
Device Safety
Samsung SM-G9600 10
Firmware Version QP1A.[redacted]
Kernel Version 4.9.[redacted]
Vulnerable Android Version Yes
Device Rooting No
Compromised No
Stagefright Vulnerable No
BlueBorne Vulnerable No
USB Debug Mode Disabled
Google Play Protect Enabled
Developer Mode Disabled
Device Encryption Enabled


19:51
Network Safety
NO THREATS DETECTED
770-2-4
Details
IP 192.[redacted]
Gateway 192.[redacted]
SSID 770-2-4
BSSID 2c:95[redacted]
Encryption [WPA2-PSK-CCMP][RSN-PSK-CCMP][ESS]
Network Protection Enabled

ALGUMAS VULNERABILIDADES, AMEAÇAS E ATAQUES QUE A SOLUÇÃO DETECTA

DEVICE	NETWORK	APPLICATION	PHISHING
OS/Kernel exploitation	Man-in-the-Middle (MITM)	Malicious apps	Malicious URL
Profile/configuration modification	SSL stripping	Risky Apps	Phishing emails
System tampering	SSL traffic intercept	Known and unknown malware	Phishing text messages
Device vulnerability assessment	Rogue access points	Dynamic threats abusing download and execute techniques	Application embedded URLs
Physical USB exploitation	Reconnaissance scams	Potentially unwanted applications from untrusted sources	Obscured URLs


Secure https://gcp-console.zdevzoo.com/en/
Apps Learning Useful Debug How To Servers AWS DO OS github DevOps Build Proje... [INTEG-529] New c... 4.10_upgrade_sche... ansible-playbook e...
CONSOLE English mo
DASHBOARD
THREAT LOG
APPS
DEVICES
PROFILES
USERS
POLICY
OS RISK
MANAGE
SUPPORT PORTAL
Threat Timeline 09/04/2018 - 09/10/2018
DEVICES Devices Analyzed 100 Threats Detected 130
NETWORKS Network Analyzed 0 Threats Detected 52
APPS Apps Analyzed 0 Threats Detected 11
Threat Log
Elevated Your device is not setup to use a PIN code, Password, or P... 3 days ago sophie.ball@mc.zimp.com
Elevated A suspicious profile was detected on your device. This sus... 3 days ago dan.black@mc.zimp.com
Critical Detected MITM from 245.34.95.79 , while connected to AT... 3 days ago benjamin.newman@mc.zimp.c...
Elevated Detected network scan after connecting to TWD49101000.... 3 days ago sean.payne@mc.zimp.com
Critical Detected a network interception attack. The attack took pla... 3 days ago wendy.hart@mc.zimp.com
Elevated Detected Abnormal Process Activity from 98.84.3.56 , while... 3 days ago isaac.mackenzie@mc.zimp.com
Critical Detected a network interception attack. The attack took pla... 3 days ago richard.lyman@mc.zimp.com
Critical Detected a rogue WiFi while connected to the network nam...
Map
Leaflet
Events that do not contain location will not be displayed on the map.
Threat History
200
150
100
50
9/4/18
9/6/18
9/8/18
9/10/18
Most Attacked Users / Devices
EMAIL / DEVICE ID THREATS SEVERITY
connor.carr@mc.zimp.com 4
rebecca.hardacre@mc.zimp.com 4
heather.parr@mc.zimp.com 4
dorothy.wright@mc.zimp.com 4
andrea.oliver@mc.zimp.com 4
Most Attacked Networks
SSID / BSSID THREATS SEVERITY
2WIRE46431000/10:70:b1:9e:80... 1
2WIRE28241000/12:51:35:f9:1e:f4 1
TWD27461000/1c:5c:62:eb:40:0c 1
ATT-8041000/20:a0:70:d7:04:3b 1
2WIRE17881000/08:8e:53:48:41... 1