



The Hacker's Perspective:  
**Zephyr OS and On-device  
Runtime Protection**

Zephyr Developer Summit 2023 | Natali Tshuva



”

The challenge for connected device manufacturers is to strike a delicate balance between security, reliability, scalability, and meeting the increasing demand for smart solutions. It requires unwavering dedication, innovation, and a customer-centric mindset to shape the future of connected devices and transform the way we live, work, and thrive in the digital age.

— Rachel Patel, Technology Strategist



# About Me



**Natali Tshuva**  
CEO & Co-founder  
Sternum



Reverse Engineer,  
Unit 8200 (Israel NSA)

Computer Science  
Student (age 14)



Sternum Co-founder



Talking to  
You Today!

Exploit Designer



Forbes 30 Under 30



## Working with Leaders

Medtronic



## Backed by Top Investors



SPARK

Square Peg



## Best IoT Product Award



# Application Security Layers Overview

In Dev:

Stack Canaries

Dynamic Analysis

Best Practices: Encryption /  
Data Protection / User mgmt

Static Analysis

Software composition  
Analysis

Post-Production:

Endpoint Protection

Zero-Day attack  
prevention and detection

Application Performance  
Monitoring

Real-Time Alerts

## Application Security

Endpoint Protection

Permissions & Policies

Continuous Monitoring

Stack Canaries

## User Space Security

Memory Isolation /  
Segmentation / Canaries

Secure API with userspace

Secure Boot + OTA

Hardware Security

## Secure OS and Infrastructure



# Security Layers - The “Embedded” Status



In Dev:

Stack Canaries

Dynamic Analysis

Best Practices: Encryption /  
Data Protection / User mgmt

Static Analysis

Software composition  
Analysis

Post-Production:

Endpoint Protection

Zero-Day attack  
prevention and detection

Application Performance  
Monitoring

Real-Time Alerts

## Application Security

Endpoint Protection

Permissions & Policies

Continuous Monitoring

Stack Canaries

## User Space Security

Memory Isolation /  
Segmentation / Canaries

Secure API with userspace

Secure Boot + OTA

Hardware Security

## Secure OS and Infrastructure



# What Happened to **Real-time** Monitoring and Protection?



# IoT/Embedded Security is **Different**.

Software Vulnerabilities Are The Main Threat

## Uniquely Deterministic Nature

- No user interface
- Predictable operation
- Minimal input channels etc.

## Different Threat Landscape

Phishing, malicious websites, viruses, file manipulations, poisoning, etc. are not a major threat for IoT.

## Limited Available Resources

- Compute
- Memory
- Battery
- Bandwidth etc.

## Uniquely Diversified

- 100+ different operating systems
- Communication stacks
- Applications & Industries

*New security solutions are required.*



# Status Today

OS Security features covers the first layers.

- Secure/trusted boot
- Over the air (OTA) updates
- Memory separation
- Stack protection
- Thread separation
- Support for crypto and TEE



Zephyr™

## Best Practices:

- Static analysis
- SBOM
- Encryption
- Vulnerability management

## The GAPS

- Static analysis misses 50% of vulnerabilities
- SBOM and vulnerability mgmt only takes care of public, well known vulnerabilities
- Patches takes time and money
- Encryption does not prevent software vulnerability exploitation
- No zero-day prevention
- No real-time application security and monitoring
- OS memory protections does not prevent memory vulnerabilities in user-space and application
- No real-time alerts and monitoring
- Result: Embedded Endpoints are **far behind**, and **blind**



# No monitoring and protection leads to...

## Software issues and vulnerabilities

### BotenaGo Malware Targets Millions of IoT Devices

AT&T Alien Labs identified the malware that has left millions of IoT devices exposed.

### Critical Vulnerabilities Patched in ThingWorx, Kepware IIoT Products

Several ThingWorx and Kepware products are affected by two vulnerabilities that can be exploited for DoS attacks and unauthenticated remote code execution.

### BlackBerry QNX flaw left cars and medical devices vulnerable to attack

The company reportedly didn't want to make the issue public at first.



Mariella Moon · Contributing Reporter

August 18, 2021 · 2 min read



### Serious Unpatched Vulnerability Uncovered in Popular Belkin Wemo Smart Plugs

May 17, 2023

Ravie Lakshmanan

## Device issues recalls

### Wearable Smart Thermometer Recalled Due to Reports of Injury



Brian Park, PharmD | May 19, 2023



Siemens Recalls 57,000 Temperature Sensors After Reports Of Fires In Hospitals And Schools





NORTH

ATLANTIC

OCEAN

Azores

PORtUGAL

SPAIN

MONTEVIDEO

Montevideo

Barcelona

Rome

Istanbul

Sofia

Ankara

Bucharest

Tashke

Tashke

Urumqi

Beijing

CHINA

Shan

georgetown  
Paramaribo  
French Guiana  
(FRANCE)

BRAZIL

Brasilia

Sao  
Paulo

ASUNCIÓN

MONTEVIDEO

Montevideo

ATLANTIC

OCEAN

Tristan da Cunha

NAMIBIA

MADAGASCAR

Reunion  
(FRANCE)

INDIAN

OCEAN



# Vulnerabilities are Inevitable and Endless

Software vulnerabilities are the main threat for IoT

**~2000**

New CVE's  
Each Month

**70%**

Patch Tuesdays  
Due To Memory  
Vulnerabilities

**58%**

Companies Have  
A Publicly  
Available Exploit.

**15**

Vulnerabilities  
Per 1000 Lines  
Of Code

Many third-party code vulnerabilities  
**left undiscovered by static analysis tools**



**AMNESIA:33**



**URGENT/11**

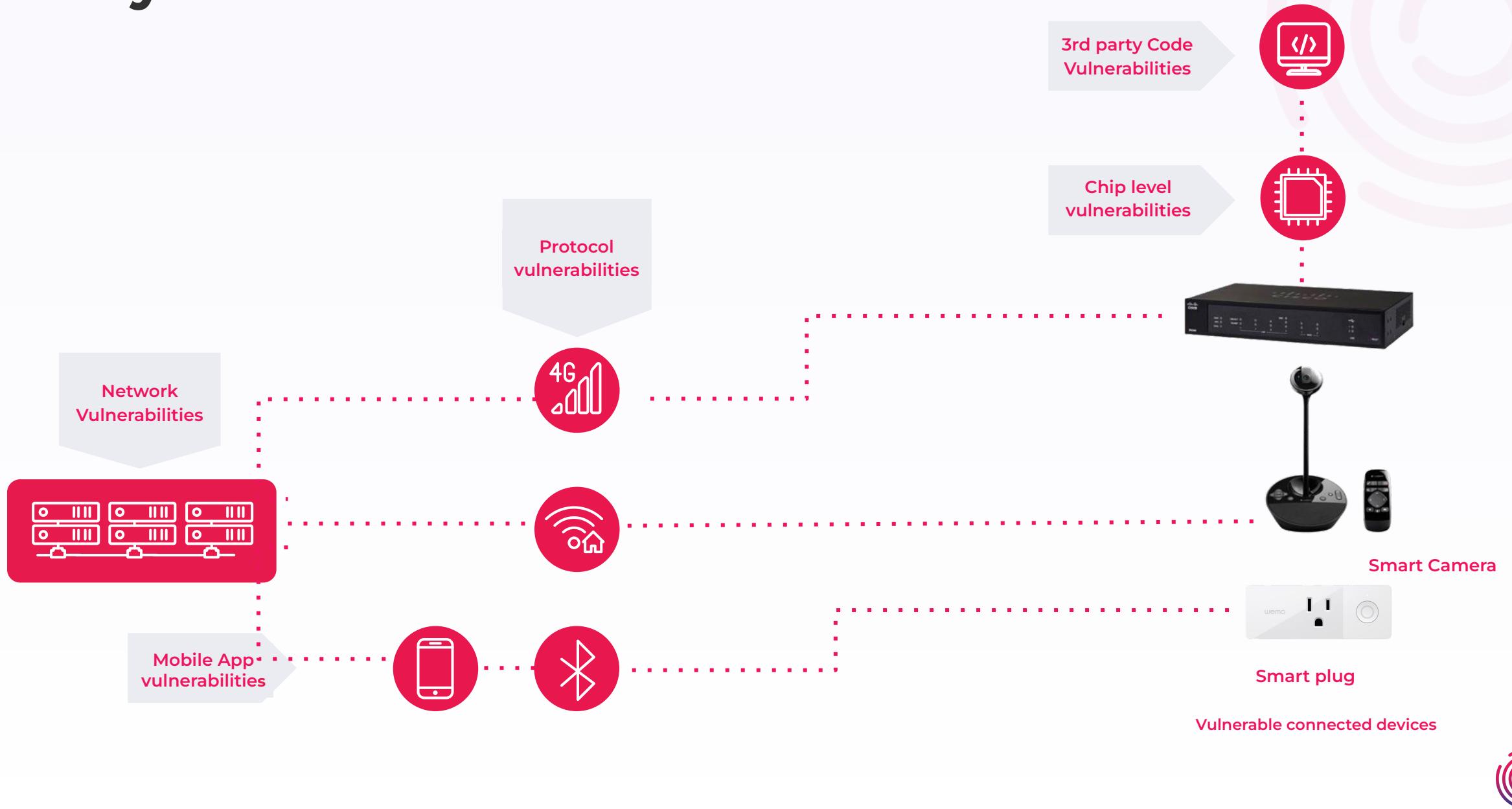


”

I know a vulnerability  
**exists**



# Many Attack Vectors



# Hacker

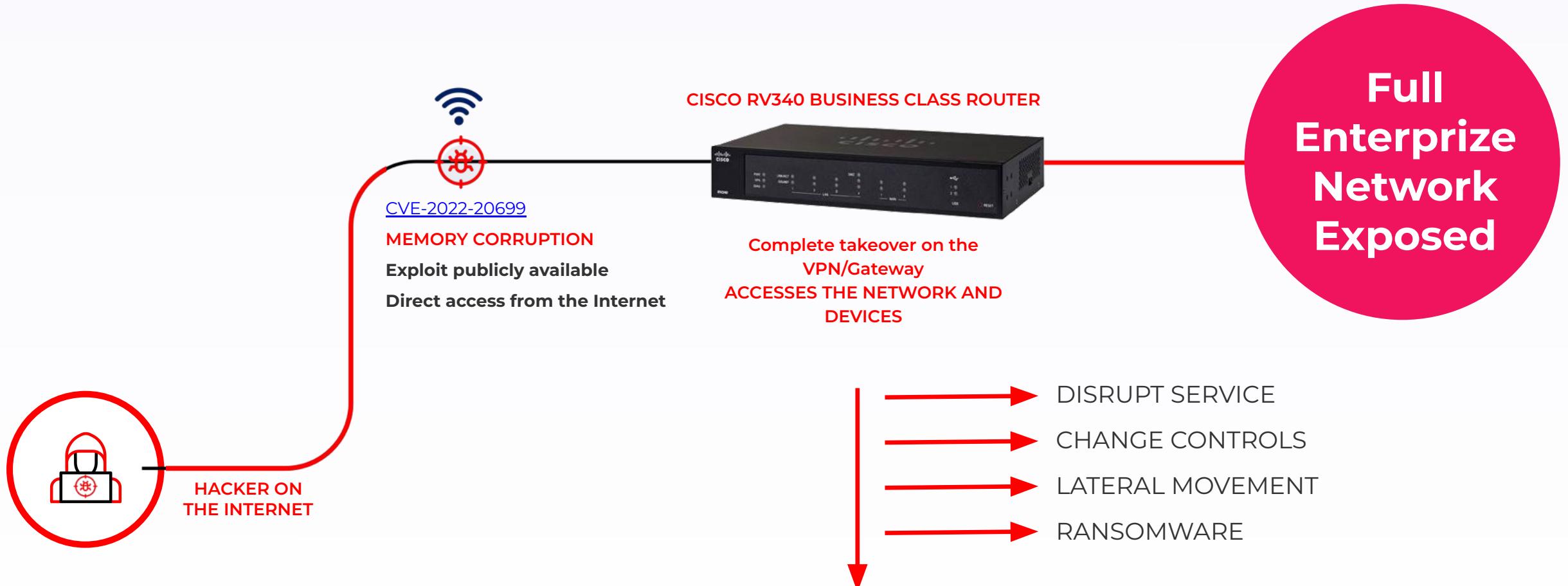


# Defender



# Hacker View: Cisco Router

No prevention on-device. No search for indicators of attack.

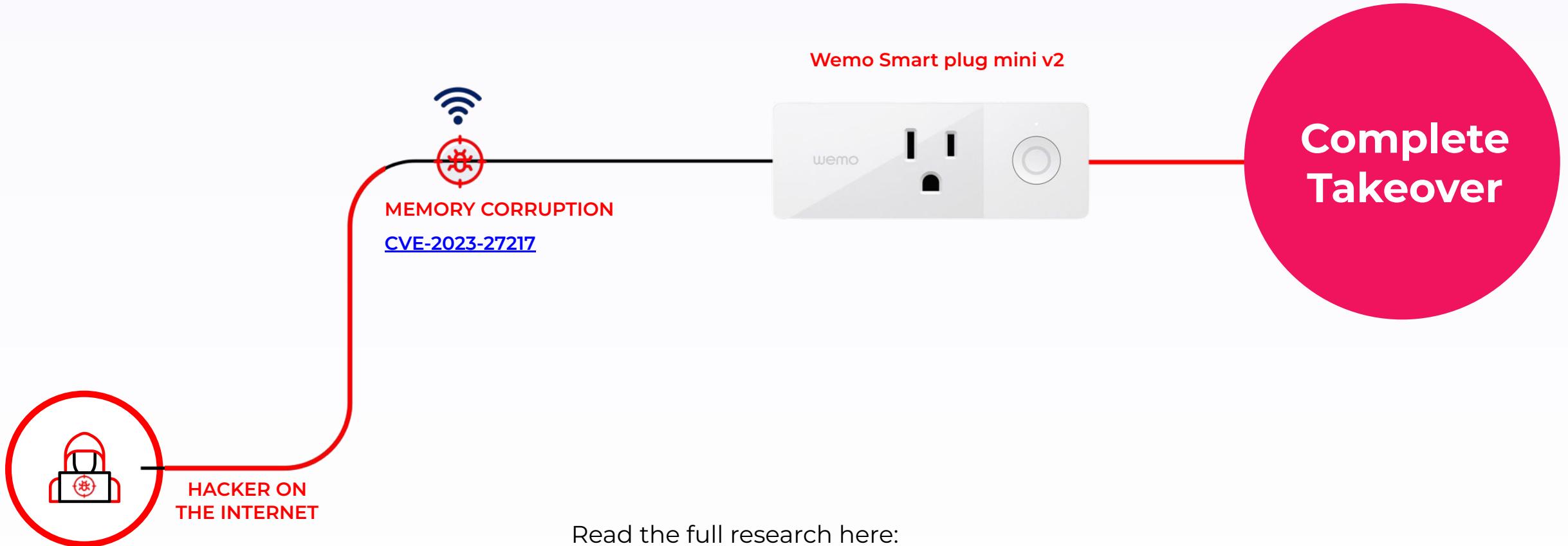


Exploitation Video: [https://youtu.be/O1uK\\_b1Tmts](https://youtu.be/O1uK_b1Tmts)



# Hacker View: Wemo Smart Plug

Sternum Disclosed a Critical Vulnerability in Wemo Devices



Read the full research here:

<https://sternumiot.com/iot-blog/mini-smart-plug-v2-vulnerability-buffer-overflow/>



# Current Approaches

## Reactive. Imposing. Not Holistic.

Patching is Reactive  
& Costly but Can't  
Safeguard

“ Usually there are  
much simpler ways  
of penetrating the  
security system [...]  
than cracking the crypto”

Adi Shamir

Static Analysis Finds  
Only 50% of  
Vulnerabilities





What can we do to **protect**  
against **zero-days and**  
**unpatched**  
**vulnerabilities?**



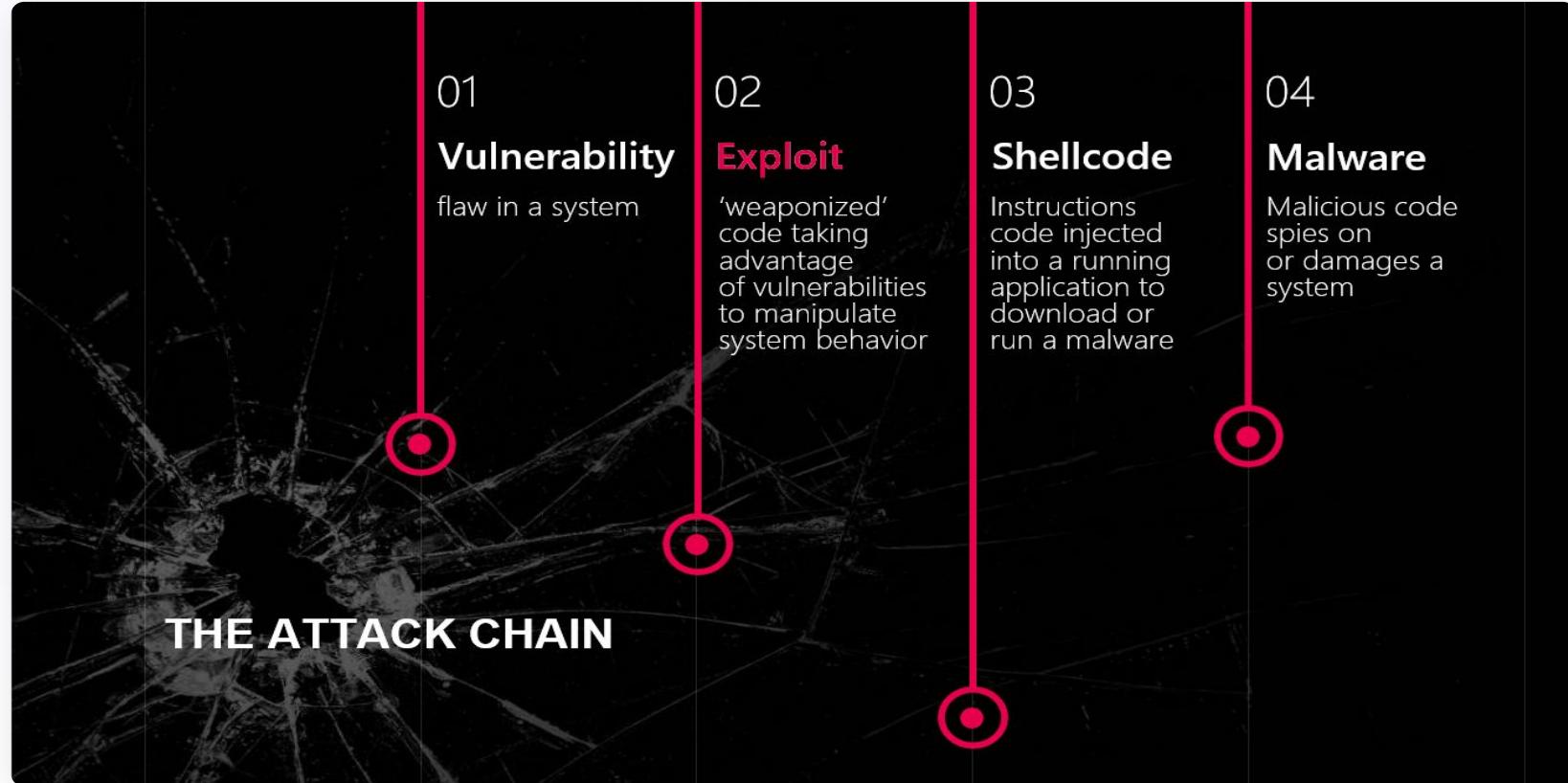
While Every  
Vulnerability is Different,  
Exploitations Share a  
**Unique Fingerprint**



# What is exploitation?

”

*“To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness.”*



”

*“An exploit... is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized).”*



# Exploitation Fingerprint™

## Patented Technology

Sternum Is Uniquely Able to Deliver The Benefits of EPP/XDR & RASP



HACKER

POWER FLIP

DEFENDER

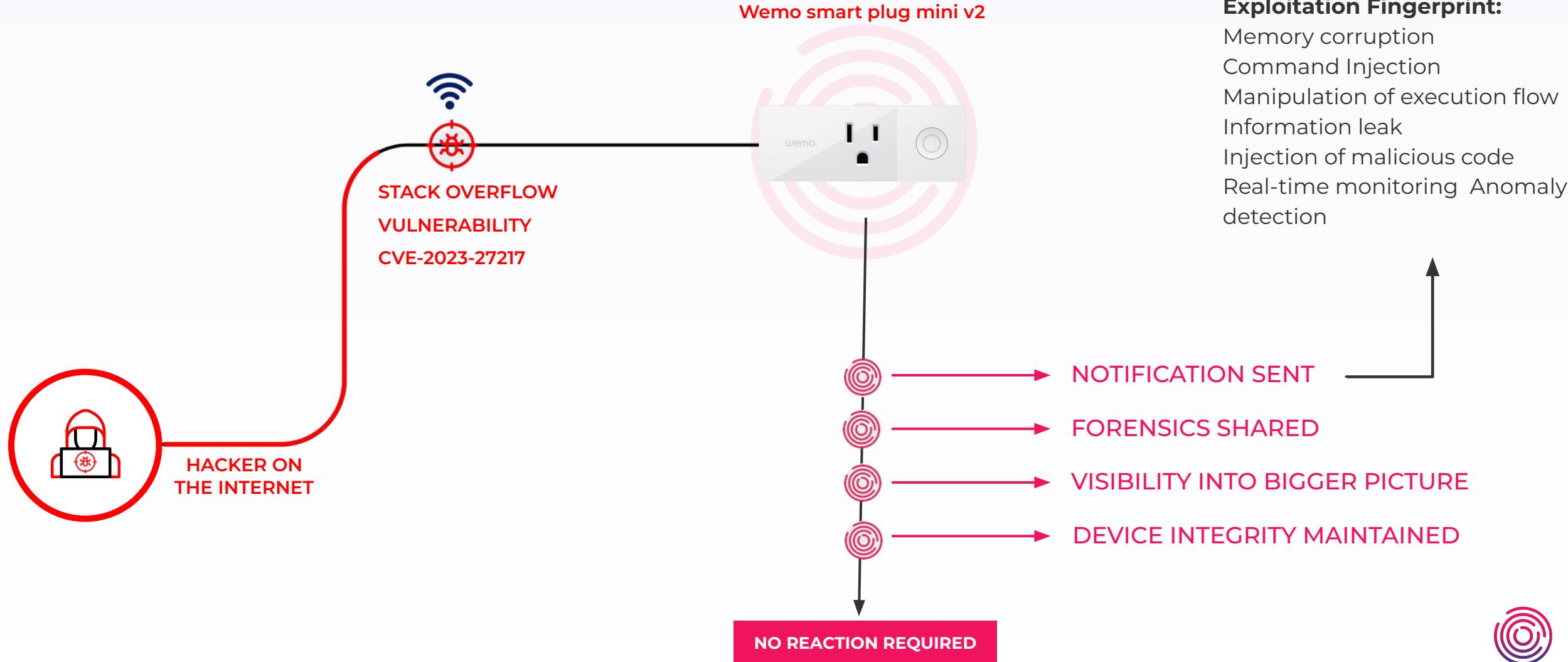


# Defender View - Wemo Smart Plug Power Flips.



## Exploitation Fingerprint:

Memory corruption  
Command Injection  
Manipulation of execution flow  
Information leak  
Injection of malicious code  
Real-time monitoring Anomaly detection



Integrating runtime protection and monitoring to an embedded device?

**This must be a  
nightmare...**



# Zephyr Integration With Sternum: Easy as 123

1. Just add our directory and a few lines to the CMakeLists. No code changes necessary.

## Configuration

Following options should be configured in prj.conf file. For more details about these options refer to Kconfig.sternum.

KConfig	Comment
CONFIG_STERNUM_PROTECTION	Enable Sternum protection
CONFIG_STERNUM_PROTECTION_TFM	Enable Sternum protection for tfm (y by default n, only non-secure code will be protected)
CONFIG_STERNUM_DEBUG_LIB	Choose debug version of sternumlib (includes logs)
CONFIG_TEST_RANDOM_GENERATOR	Use non secure random generator. Sternum random generation capability. If your target support real random generation, you may enable TEST_RANDOM_GENERATOR.
CONFIG_STERNUM_COMMUNICATION_MANAGER_THREAD_PRIORITY	Priority of Sternum communication manager
CONFIG_STERNUM_COMMUNICATION_MANAGER_THREAD_STACK_SIZE	Stack size of Sternum communication manager
CONFIG_STERNUM_DEVICE_DEFINITION_ID	Device definition ID identifies the device type shared by all devices of the same class.

The screenshot shows a terminal window with two tabs: 'CMakeLists.txt' and 'CMakeLists.txt M'. The 'CMakeLists.txt' tab displays the original Zephyr CMakeLists.txt file, which includes a 'find\_package(Zephyr REQUIRED HINTS \${ENV{ZEPHYR\_BASE}})' command. The 'CMakeLists.txt M' tab shows the modified file where the 'find\_package' command has been replaced with Sternum-specific logic. A red box highlights the modified section of the CMakeLists.txt file.

```
find_package(Zephyr REQUIRED HINTS ${ENV{ZEPHYR_BASE}})

set(STERNUM_DIR ${CMAKE_CURRENT_LIST_DIR}/zephyr-eiv-integration
    include(${STERNUM_DIR}/sternum.cmake)

find_package(Zephyr REQUIRED HINTS ${ENV{ZEPHYR_BASE}})
add_subdirectory(${STERNUM_DIR}/sternum_module
    ${STERNUM_DIR}/sternum_module)

2. Source Kconfig.sternum from Kconfig file in the project main directory
If your project contains Kconfig file, source Sternum options among others

resource "sternum_eiv/Kconfig.sternum"

If your project doesn't contain Kconfig file, create it with following content

mainmenu "Stendum"
resource "sternum_eiv/Kconfig.sternum"
source "Kconfig.zephyr"
```

```
set(STERNUM_DIR ${CMAKE_CURRENT_LIST_DIR}/sternum_eiv)
include(${STERNUM_DIR}/sternum.cmake)

find_package(Zephyr REQUIRED HINTS ${ENV{ZEPHYR_BASE}})
add_subdirectory(${STERNUM_DIR}/sternum_module
    ${STERNUM_DIR}/sternum_module)

project(threads)

if(CONFIG_BUILD_WITH_TFM)
# Needed for tfm tests
target_include_directories(app PRIVATE
    ${TARGET_PROPERTY:tfm,TFM_BINARY_DIR}/install/interface/include
)
endif()

include_directories(${ENV{ZEPHYR_BASE}}/include/zephyr/)

target_include_directories(app PRIVATE .)
file(GLOB source_files
    "src/*.c"
)
target_sources(app PRIVATE ${source_files})
```

2. Sternum runtime security will immediately auto-activate and can be controlled directly from Kconfig.



### 3. You can deploy custom traces to set up your monitoring strategy and start collecting device-level data.

The screenshot displays the STERNUM platform's monitoring and configuration interface. At the top, two device cards are shown: 'STERNUM' (Firmware Version: 1.1.1, Operating System: Zephyr, Device Definition ID: 988508101115190272) and 'Zephyr Device 1' (Firmware Version: 1.0, Operating System: Zephyr, Device Definition ID: 988512310404464640). Below these are tabs for 'Device Profile', 'Traces', 'Arguments', 'Sternum Alerts', and '3rd Party'. The 'Traces' tab is active, showing sections for 'System traces' and 'Customized traces'. Under 'Customized traces', several entries are listed with icons for edit and delete:

Battery Status	TRACE_BATTERY_STATUS
Perform Disconnect	TRACE_PERFORM_DISCONNECT
Remote SPP Port Closed	TRACE_REMOTE_SPP_PORT_CLOSED
Dropping Message	TRACE_DROPPING_MESSAGE
Retransmission Threshold Re...	TRACE_RETRANSMISSION_THRES...

A 'CREATE TRACE' button is located at the bottom right of this section. In the center, there is a 'Zephyr Device' card with details: Firmware Version: 1.1, Operating System: Zephyr, Device Definition ID: 981299792522399744, Total Device Count: 0, and a note that it was created by Bruno Rossi at 05/31/2022. To the right of this is a 'Zephyr Device 1' card with similar details. A red alert box at the bottom right of the Zephyr Device card states: '35 new [PRODUCTION] alerts require your attention' and '24 new [STAGING] alerts require your attention'. On the right side of the interface, a 'Battery Condition' dashboard is displayed with various charts and metrics. One chart shows 'PC Shutdown due to low battery' over time, another shows 'Battery Depleted < 60% Original Capacity' with a count of 338, and a third shows the '5% of Devices With The Lowest Battery Capacity Compared to Maximum Battery Capacity'. A note below the charts states: 'Infrequent, but every day, one of our users runs out of battery while using the PC.' Another note indicates: '9.6% [redacted] have a battery that is depleted to < 60% of its original charge capacity.'

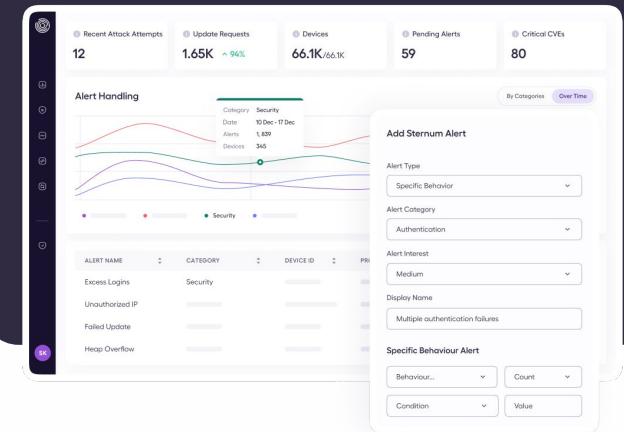
With sternum on your Zephyr devices, you get an additional layer of runtime protection, as well as access to live and historical data, AI-powered anomaly detection, advanced investigation capabilities, and more



# The Sternum Platform

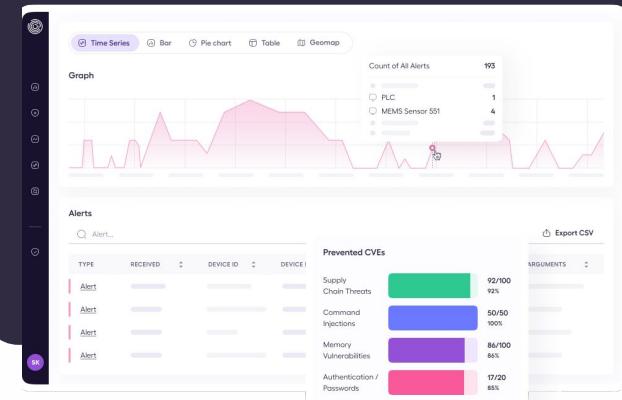
## Embedded Security

Agentless runtime protection,  
AI-powered threat detection



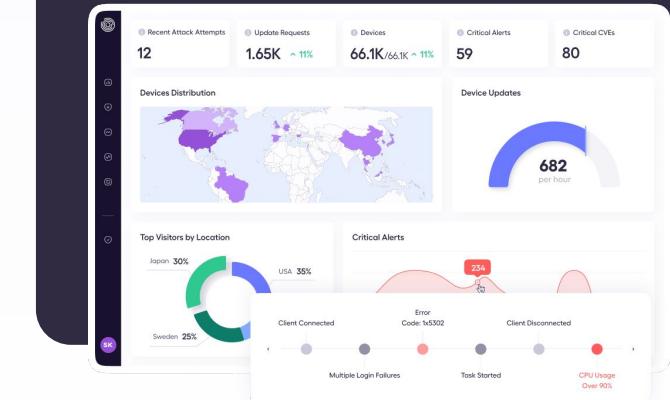
## Continuous Monitoring

Live remote monitoring & analysis,  
AI-powered anomaly detection



## Business & Operational Insights

Operational insights,  
fleet management,  
business analytics

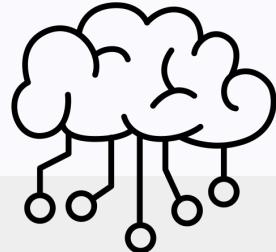


# The Sternum Platform Overview

## Cloud

Business & operational insights   Policies Management   Fleet Management   Cybersecurity Monitoring

Customizable views, dashboards, queries, alerts



### AI-powered Security & Monitoring

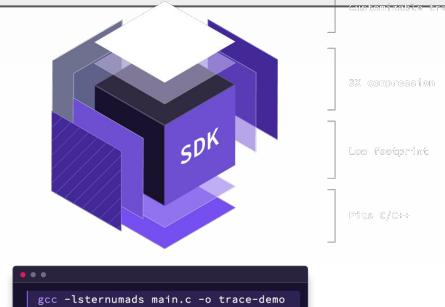
- Anomaly detection
- Threat intelligence

## Device

### Agentless Runtime Protection

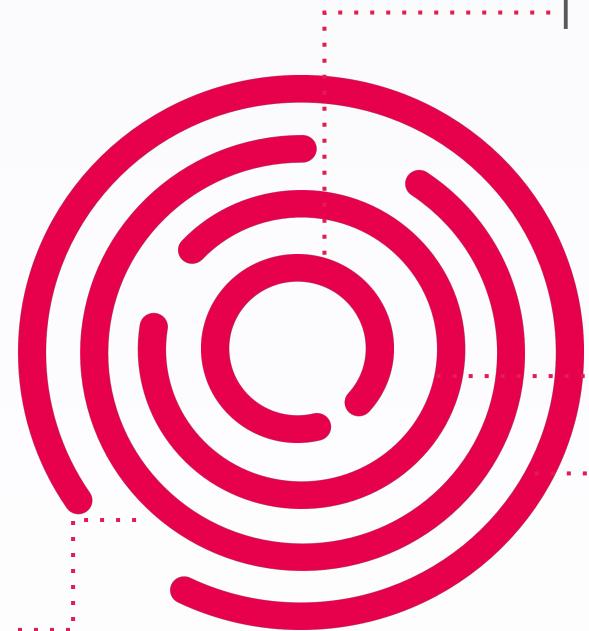


### Universal Telemetry & Monitoring SDK



# End-to-End Device Security

Embedded Prevention, AI Detection, Cloud Management and Response

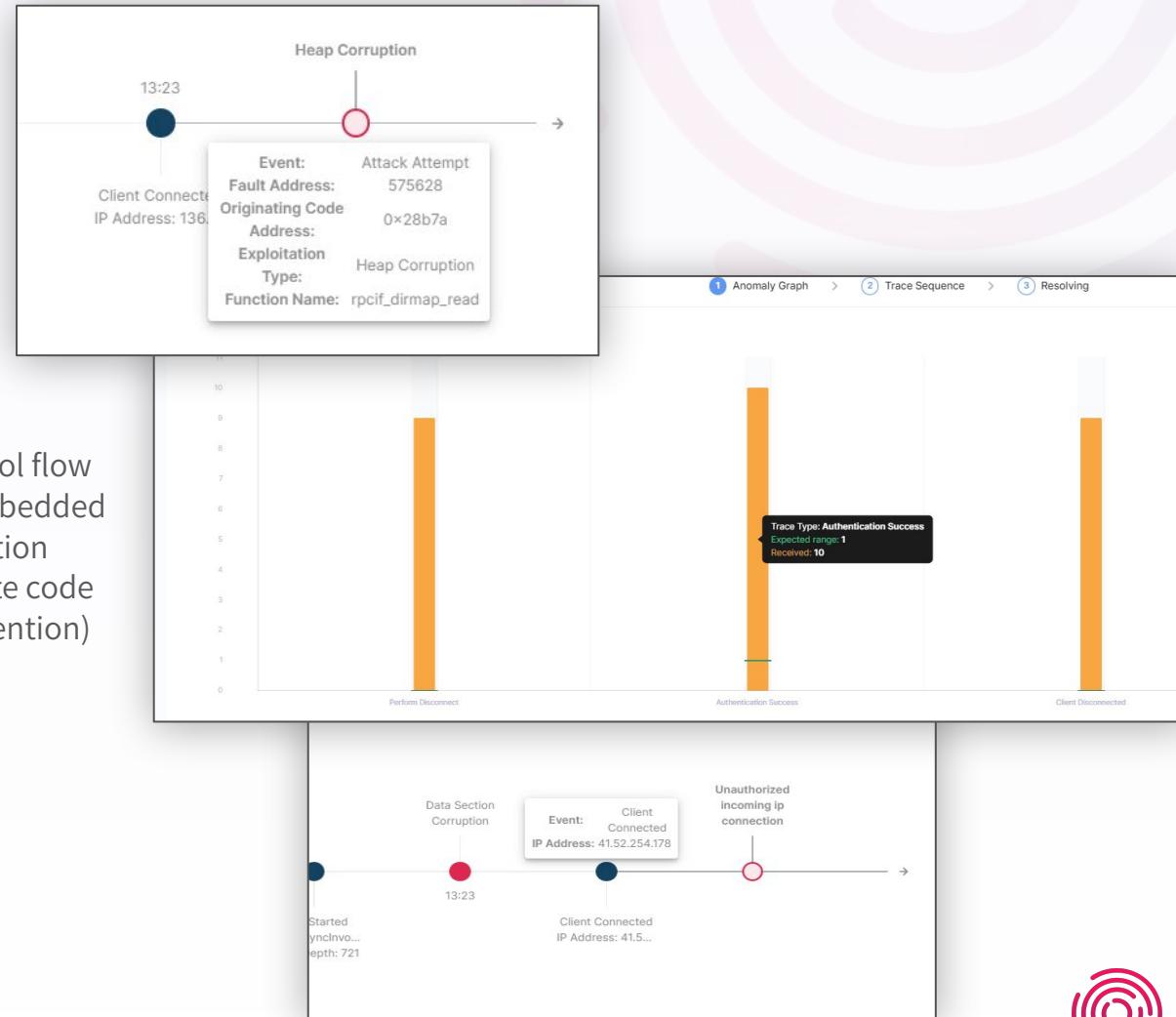


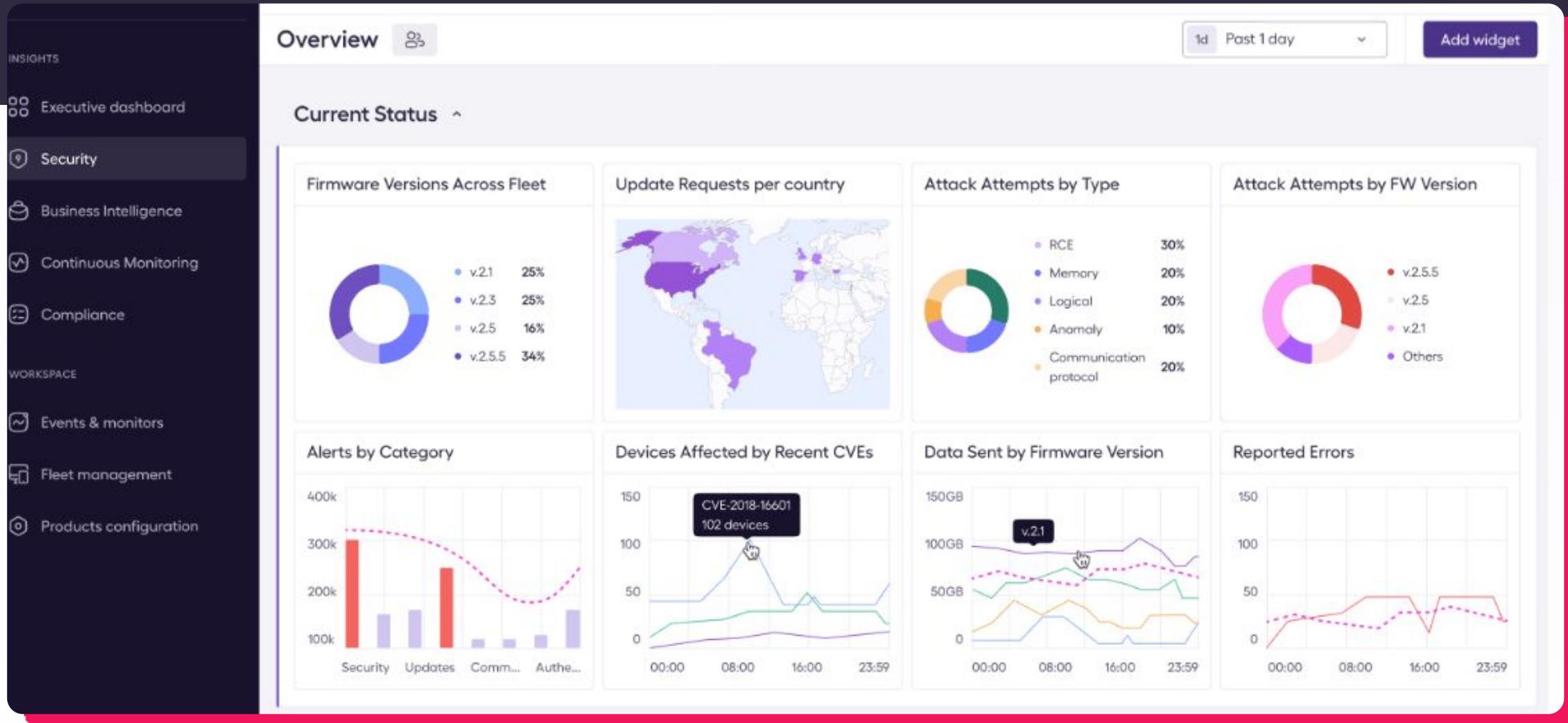
3  
Operating System  
Anti-Exploitations:  
**Command injections**,  
unallowed operations

1 **Patented:** Memory Integrity Protection, fileless attacks, in-memory attacks (top threat – 70% of vulnerabilities)

2 **Patented** control flow integrity for embedded systems, execution integrity (remote code execution prevention)

4





This is simulated data

\*Screenshot from the next version of our platform, currently in development



## Detailed View ^

### Attack Attempts

TYPE	LOCATION	DETAILS	IP ADDRESS	DEVICE	STATUS	RESPOND
Heap overflow	Germany	zero-day	104.66.223.32		Protected	Notify customer
RCE	Germany	zero-day	108.179.120.99		Protected	View Fleet
Use after free	Germany	one-day	109.125.67.15		Protected	Investigate the attack

### Anomalies

#### Latest Security Anomalies

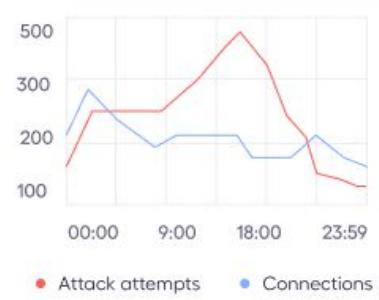
ANOMALY	DEVI...
Update Anomaly	12
Authentication Issue	3
Failed Connections	2
Update Anomaly	4

#### Detection Alerts / Policy Violati...



### Customer Impact

#### Attack Attempts vs Connections



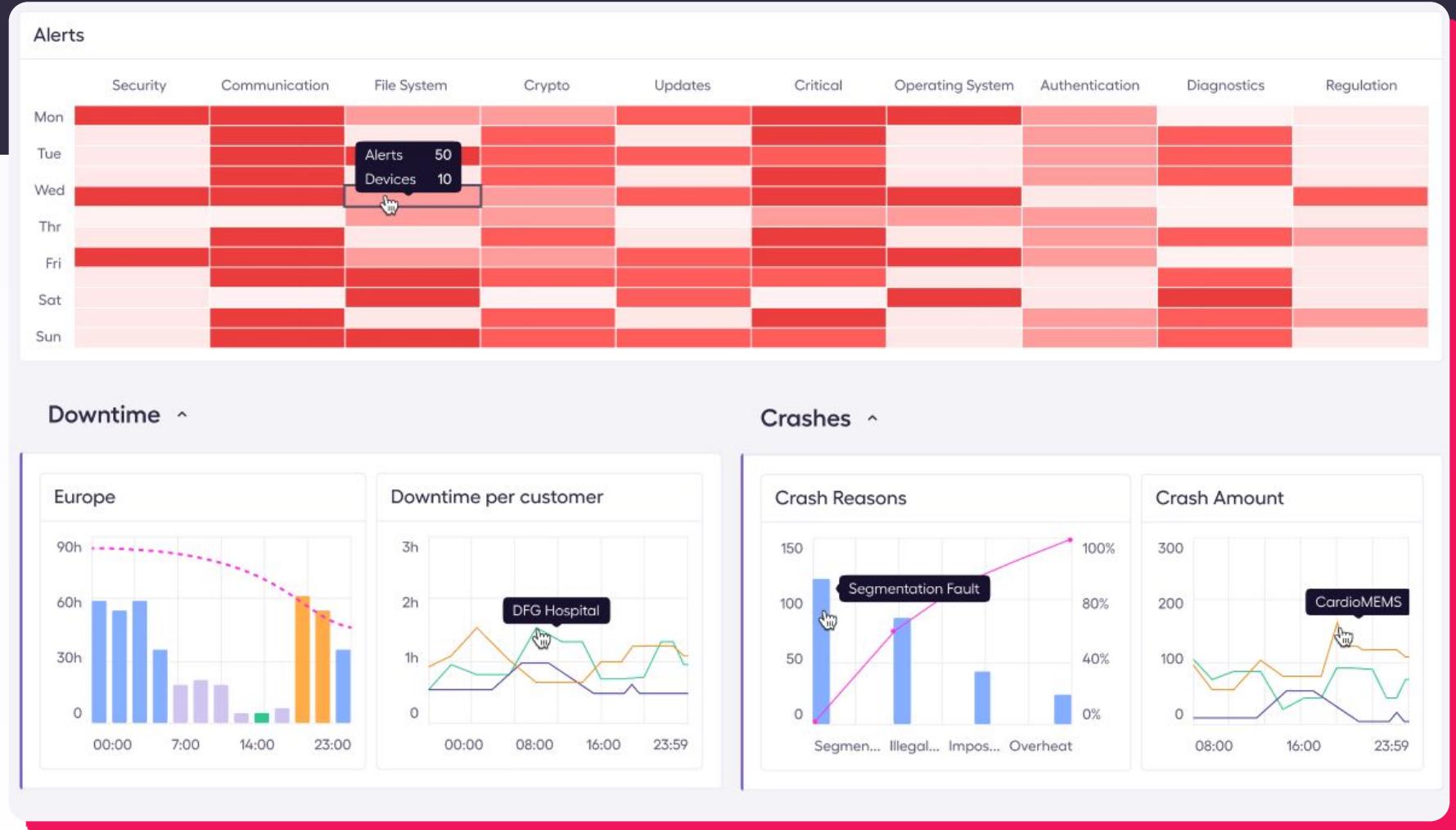
#### User Operations vs Errors



This is simulated data

\*Screenshot from the next version of our platform, currently in development





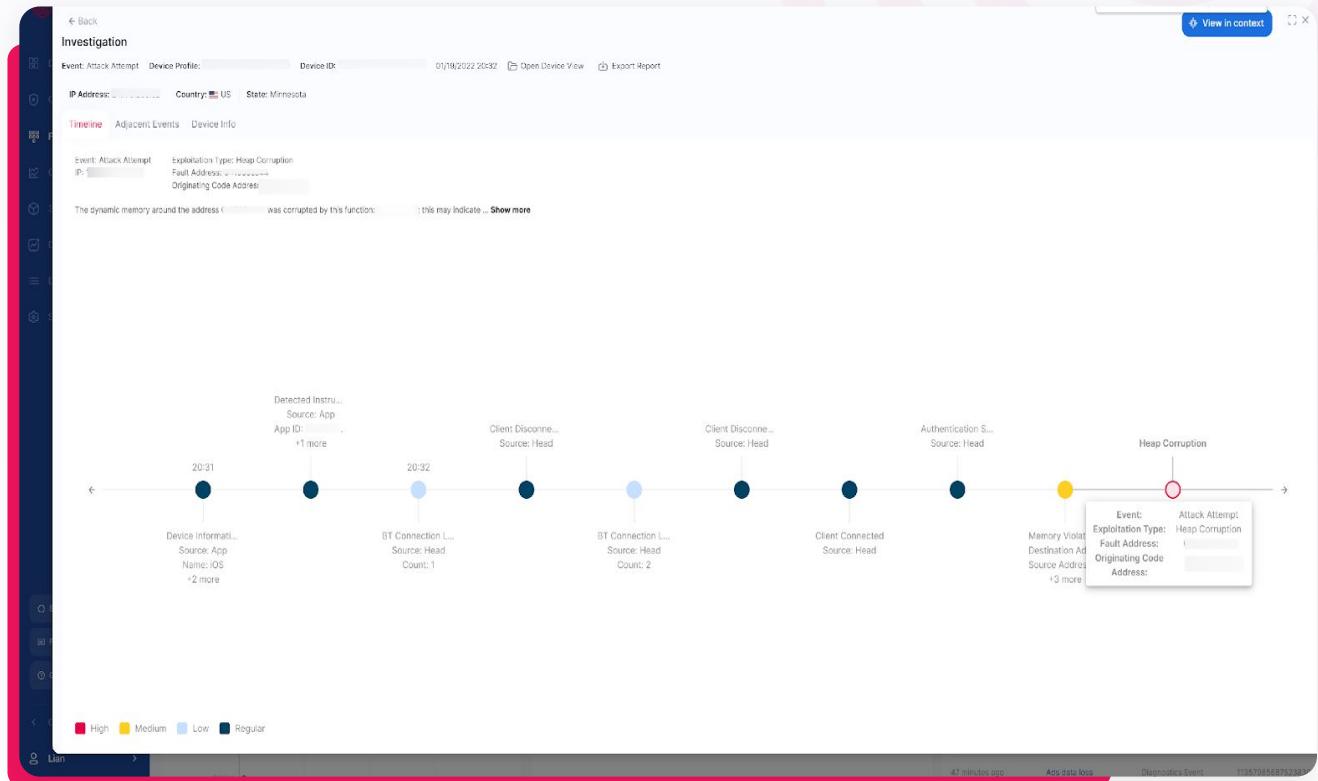
**This is simulated data**

\*Screenshot from the next version of our platform, currently in development



# Security and Monitoring are Tied Together

- ✓ Embedded Endpoint Protection
- ✓ Alerts
- ✓ Anomaly detection
- ✓ Root-cause analysis
- ✓ Policy management
- ✓ Post production monitoring
- ✓ Real time debugging,  
performance monitoring and  
operational insights



Operational Cost-saving



Device Security



# The device-centric security & data platform



Runtime Protection

Continuous Monitoring

Operational & Business Insights

Multiple Patents

Raised \$40M, 10x  
in sales this year

Awards: Best  
IoT Product

Unit 8200  
heritage

Trusted by Leaders

Medtronic

Undisclosed Fortune 50 Company

Working With Largest Device Manufacturers

**“Sternum saves us time, manpower, and money.”**

Kyle Ericson, Product Security Director

**“Sternum gives us the opportunity to do advanced planning, triage the issue, and manage the situation.”**

Chas Meyer, Sr. Principal Product Security Engineer

**Medtronic**



**Thank You ZDS 2023**  
[natali@sternumiot.com](mailto:natali@sternumiot.com)