STERNUM

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

Computer Science Student (age 14)

Reverse Engineer, Unit 8200 (Israel NSA)

Exploit Designer

Cellebrite

Sternum Co-founder

Forbes 30 Under 30

Forbes 30 30

Talking to You Today!

Working with Leaders

Medtronic · TX · NXP · VIBRANT · Zephyr™ · arm

Backed by Top Investors

SPARK · Square Peg · hinrich foundation · b to v

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

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

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

Ripple20

AMNESIA:33

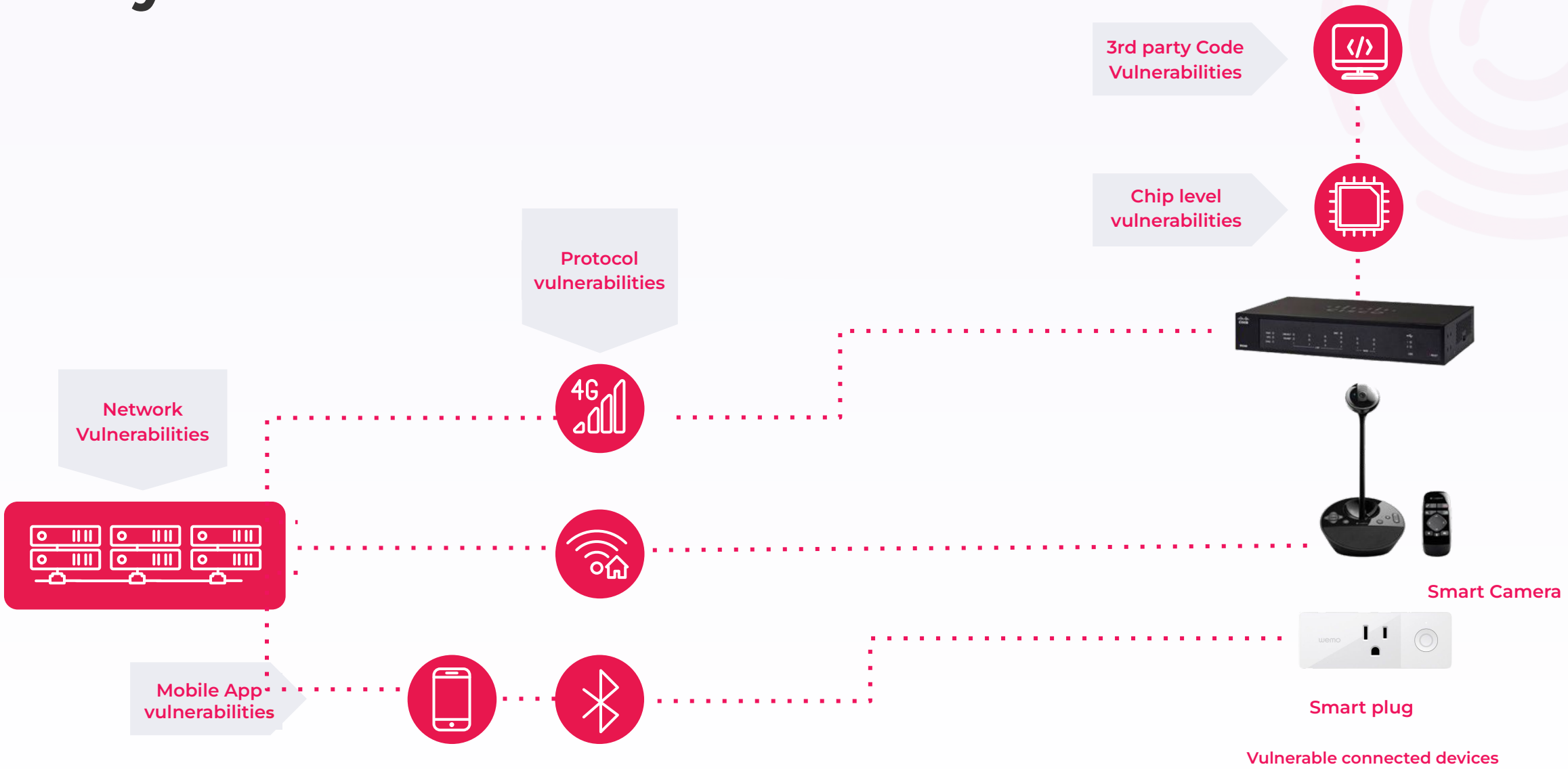
BlueBorne

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.

CISCO RV340 BUSINESS CLASS ROUTER

CVE-2022-20699

MEMORY CORRUPTION

Exploit publicly available

Direct access from the Internet

Complete takeover on the VPN/Gateway
ACCESSES THE NETWORK AND DEVICES

Full Enterprize Network Exposed

HACKER ON THE INTERNET

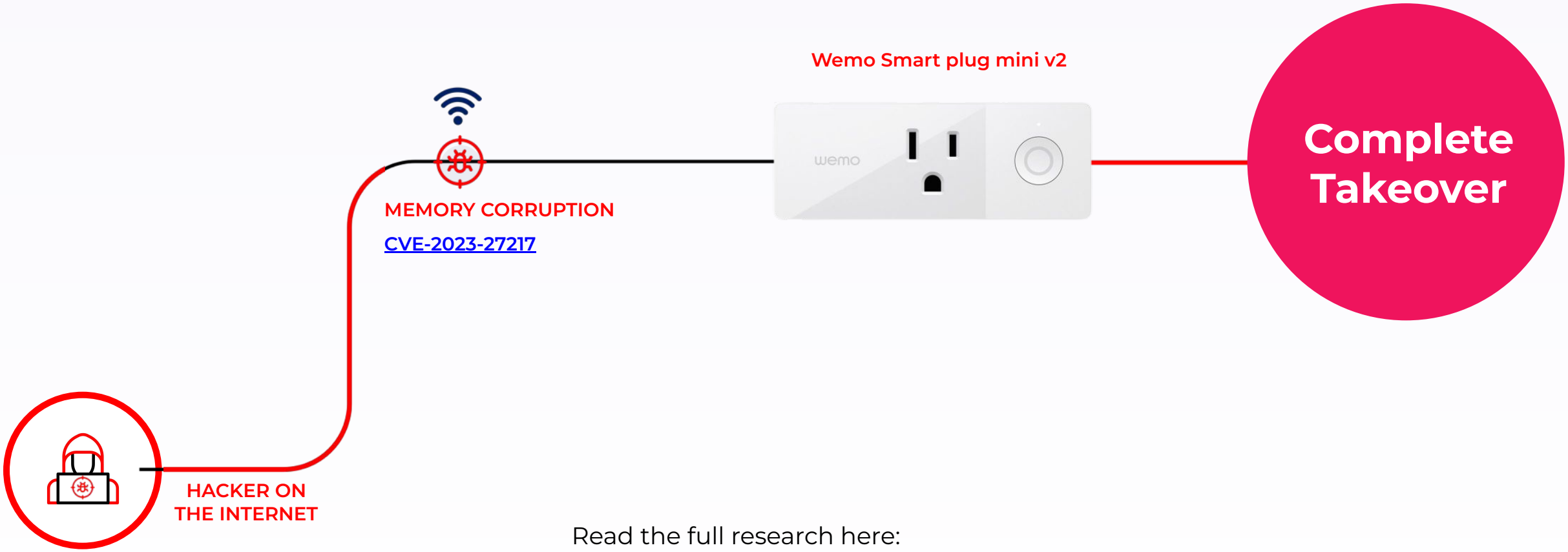
- DISRUPT SERVICE
- CHANGE CONTROLS
- LATERAL MOVEMENT
- RANSOMWARE

LIMITED OPTIONS:
REACT. PATCH.

Exploitation Video: 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

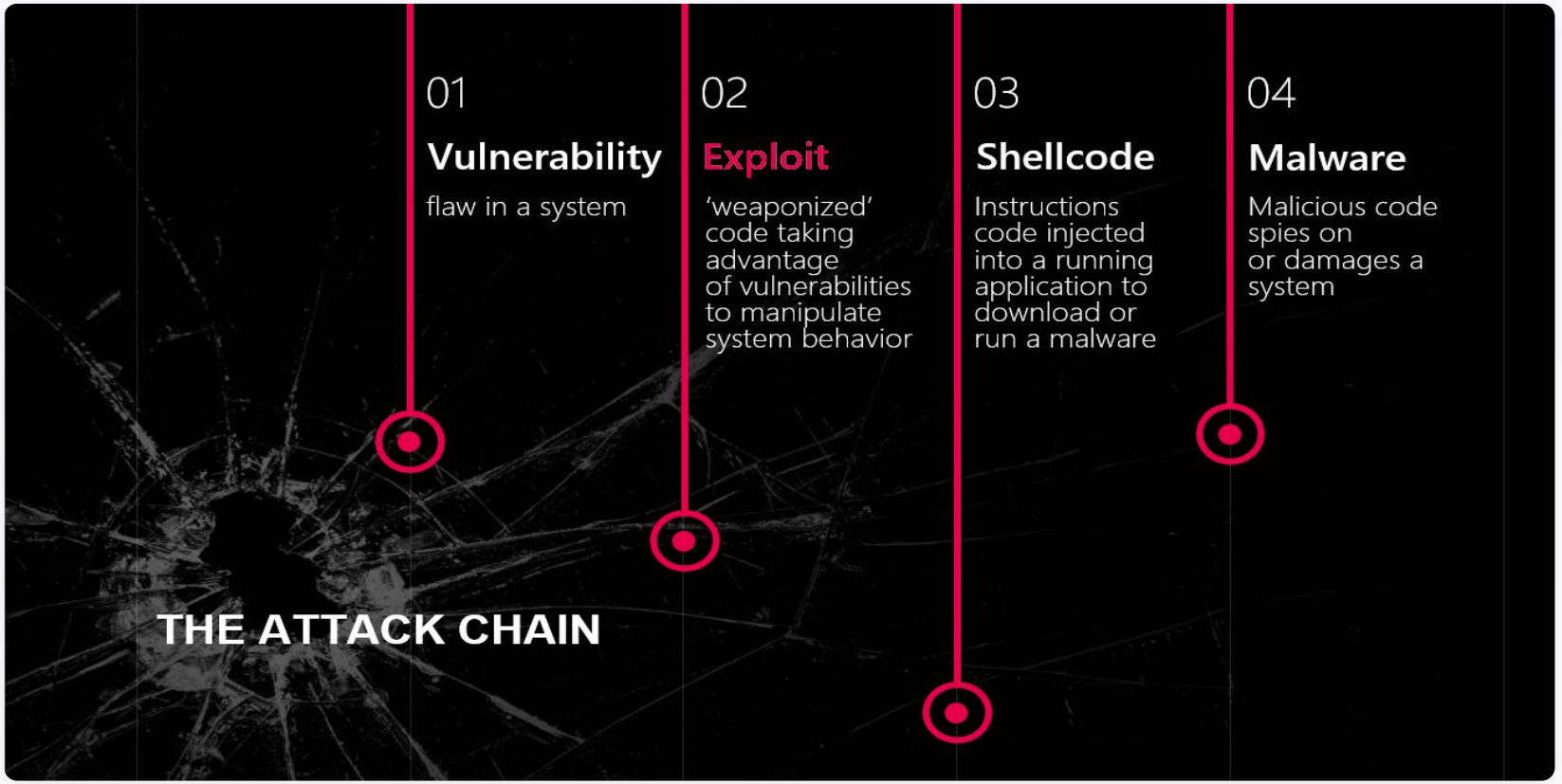
Static Analysis Finds Only 50% of Vulnerabilities

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)."

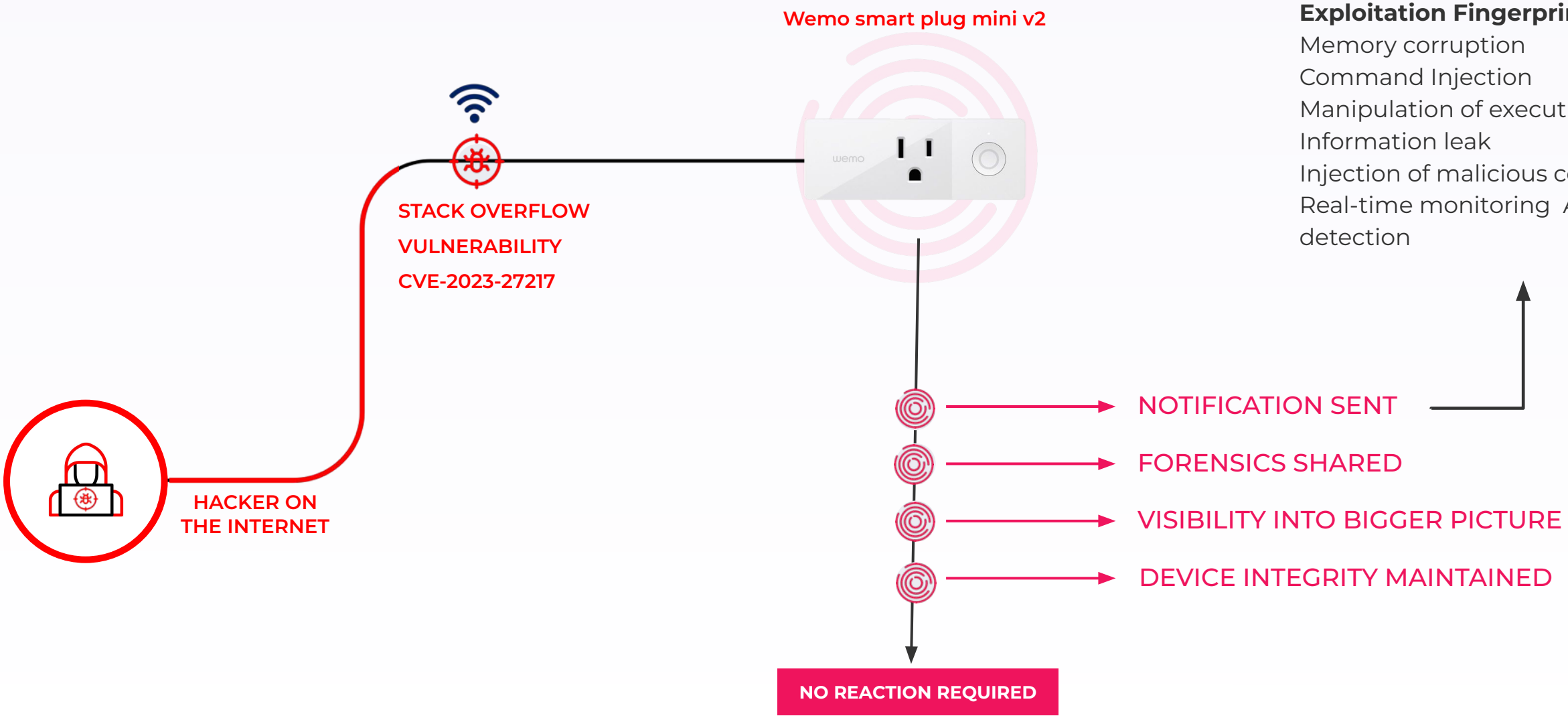
Exploitation Fingerprint™

Patented Technology

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


HACKER
DEFENDER
POWER FLIP
MESSI
10
unicef

Defender View - Wemo Smart Plug
Power Flips.



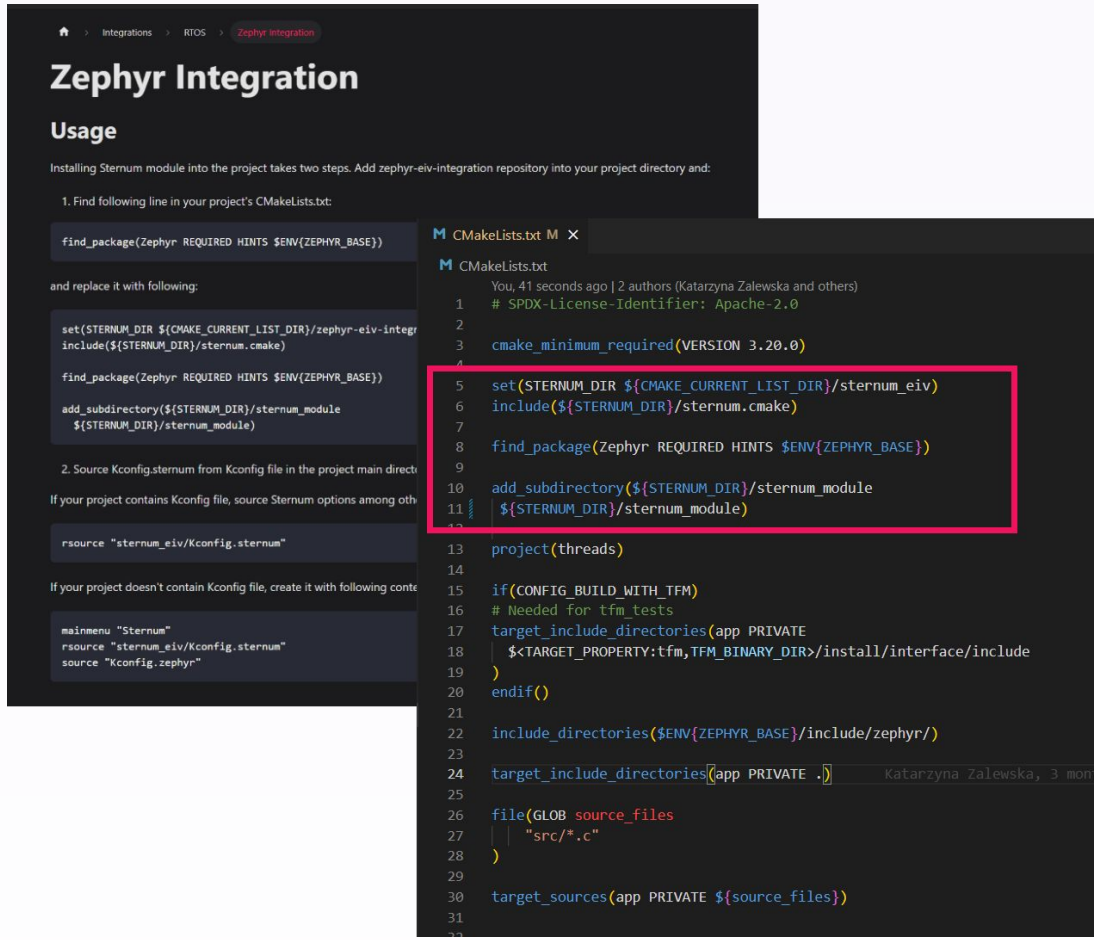
Exploitation Fingerprint:
Memory corruption
Command Injection
Manipulation of execution flow
Information leak
Injection of malicious code
Real-time monitoring Anomaly detection

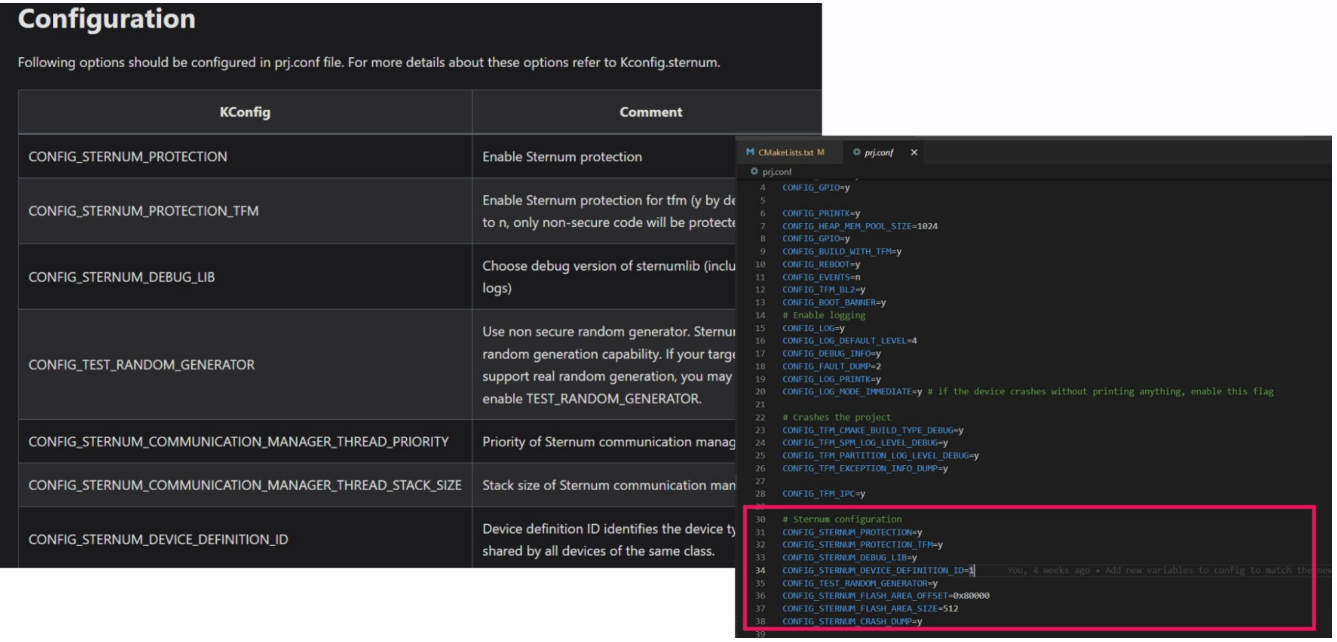
”Integrating runtime protection and monitoring to an embedded device?

This must be a nightmare...

Zephyr Integration With Sternum: Easy as 123

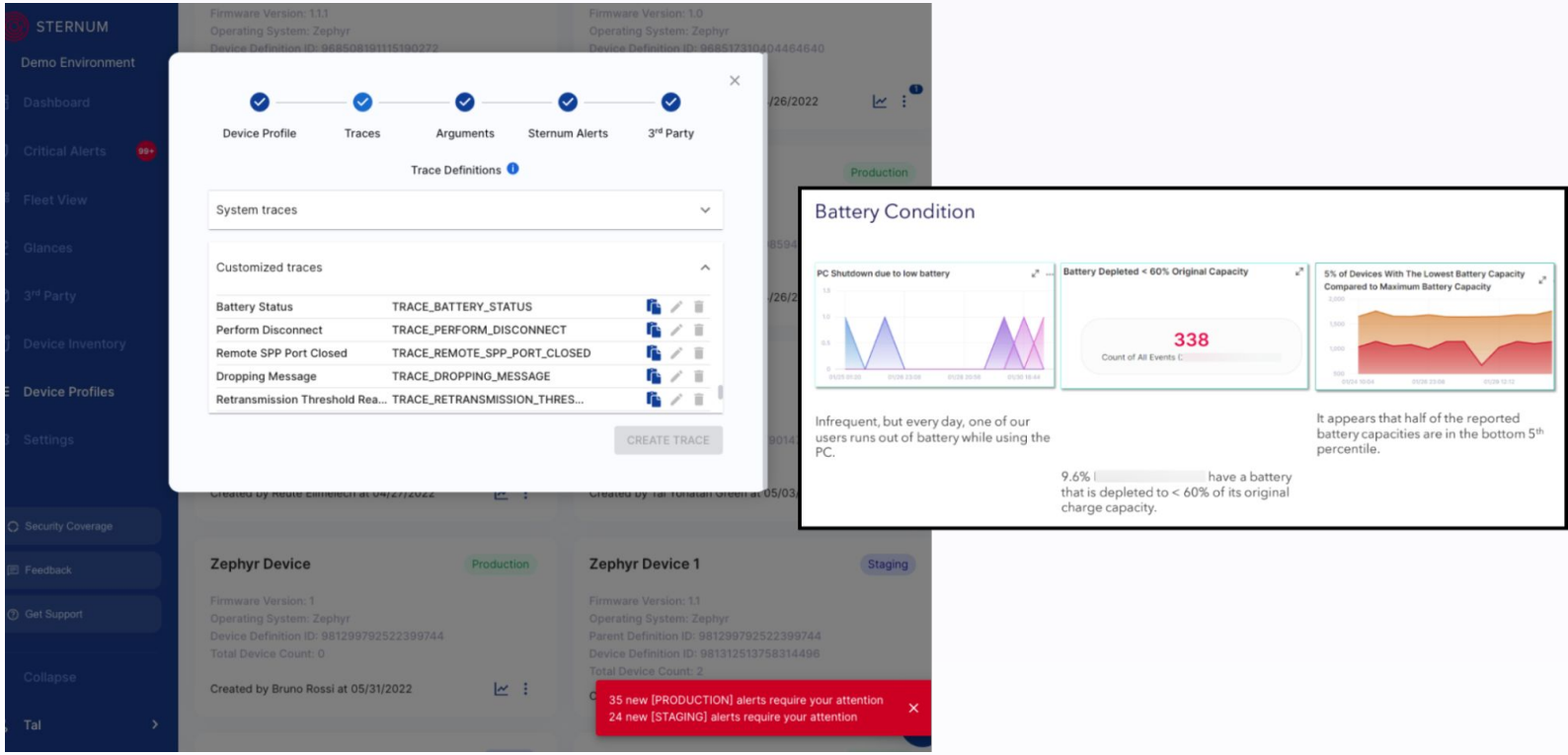
1. Just add our directory and a few lines to the CMakeLists. No code changes necessary.





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.

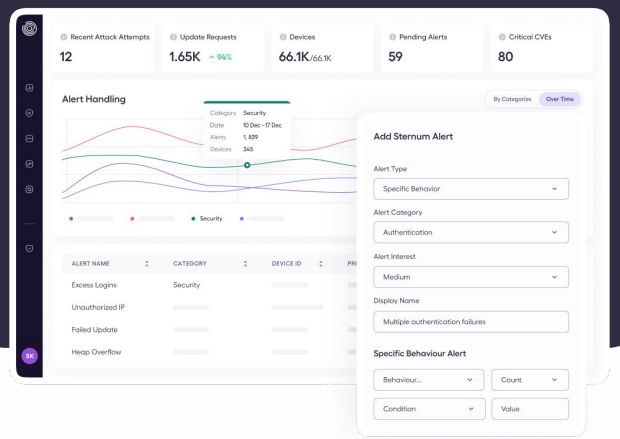


With sternum on your Zephyr devices, you get an additional layer of runtime protection, as well as access to live and historical data, AI-powered anomaly detection, advanced investigation capabilities, and more

The Sternum Platform

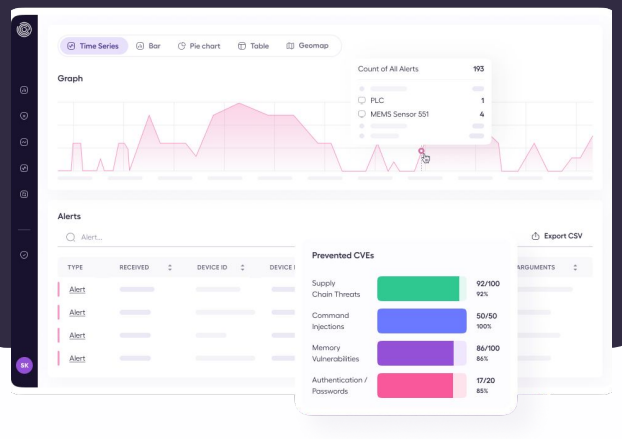
Embedded Security

Agentless runtime protection,
AI-powered threat detection



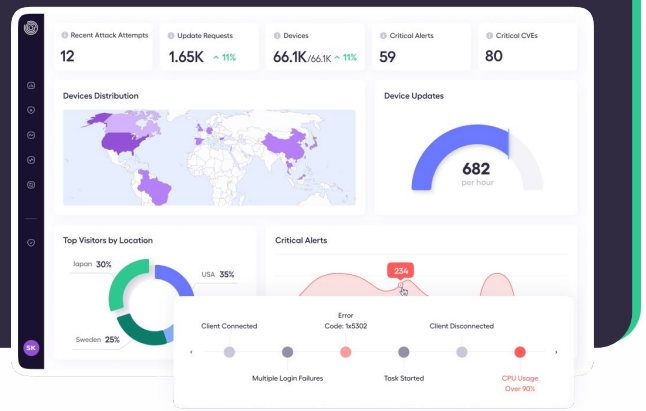
Continuous Monitoring

Live remote monitoring
& analysis,
AI-powered anomaly detection



Business & Operational Insights

Operational insights,
fleet management,
business analytics



The Sternum Platform Overview

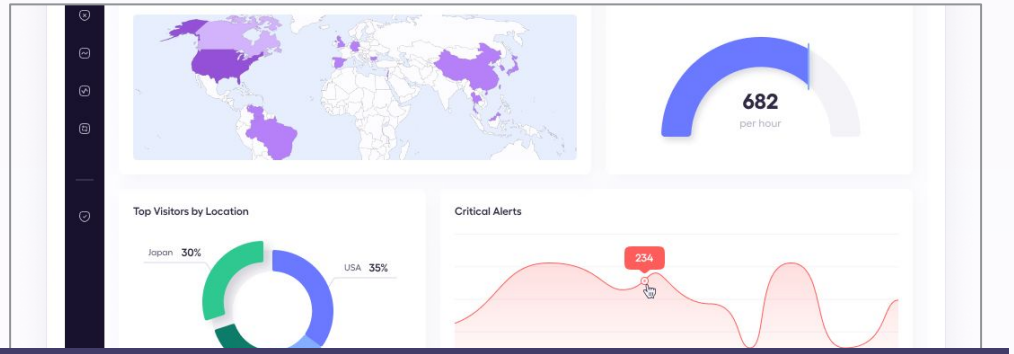
Cloud

Business & operational insights

Policies Management

Fleet Management

Cybersecurity Monitoring



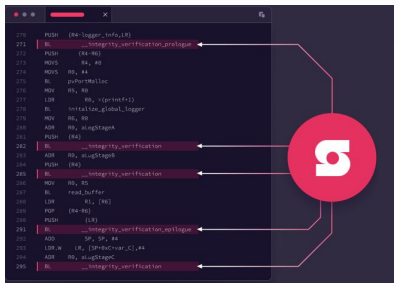
Customizable
views, dashboards, queries, alerts

AI-powered Security & Monitoring

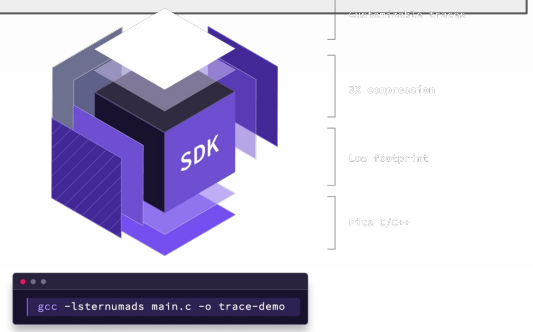
- Anomaly detection
- Threat intelligence

Device

Agentless Runtime Protection



Universal Telemetry & Monitoring SDK



Detection Layer: Overall system monitoring, AI-powered anomaly detection and policy setting: brute-force, DDoS, malicious connections, anti-malware etc

End-to-End Device Security

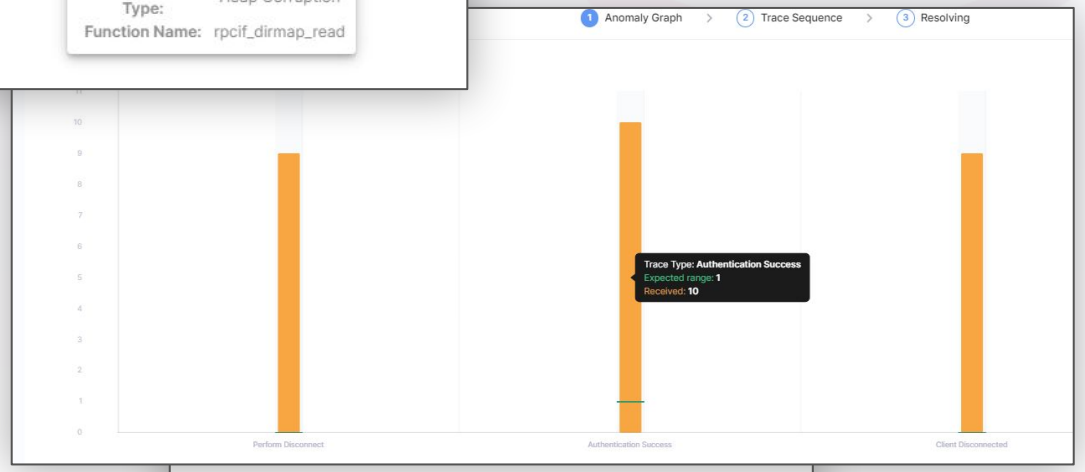
Embedded Prevention, AI Detection, Cloud Management and Response

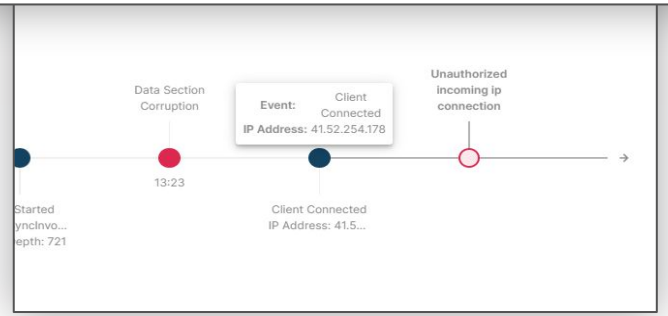
1 **Patented**: Memory Integrity Protection, fileless attacks, in-memory attacks (top threat – 70% of vulnerabilities)

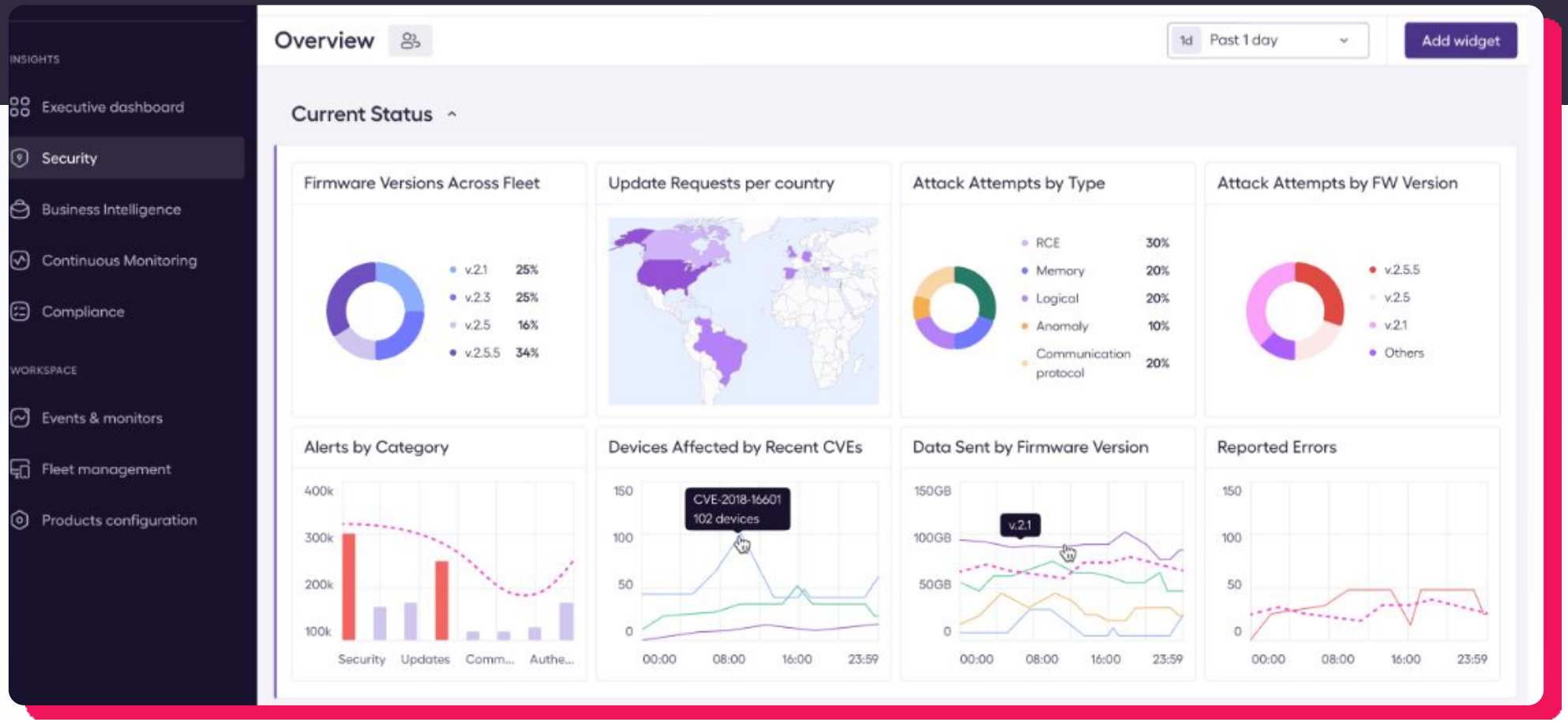
2 **Patented** control flow integrity for embedded systems, execution integrity (remote code execution prevention)

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

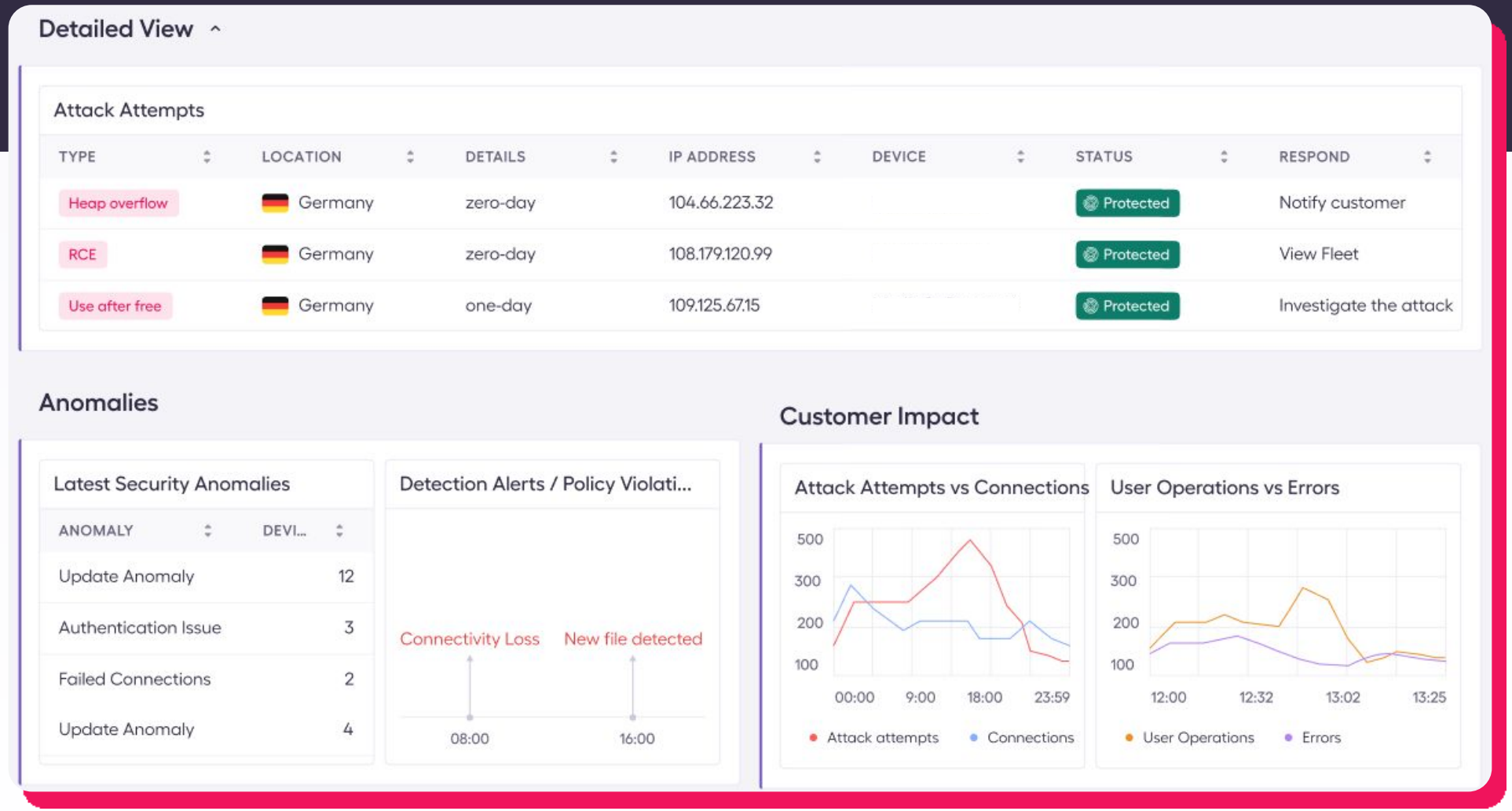
4



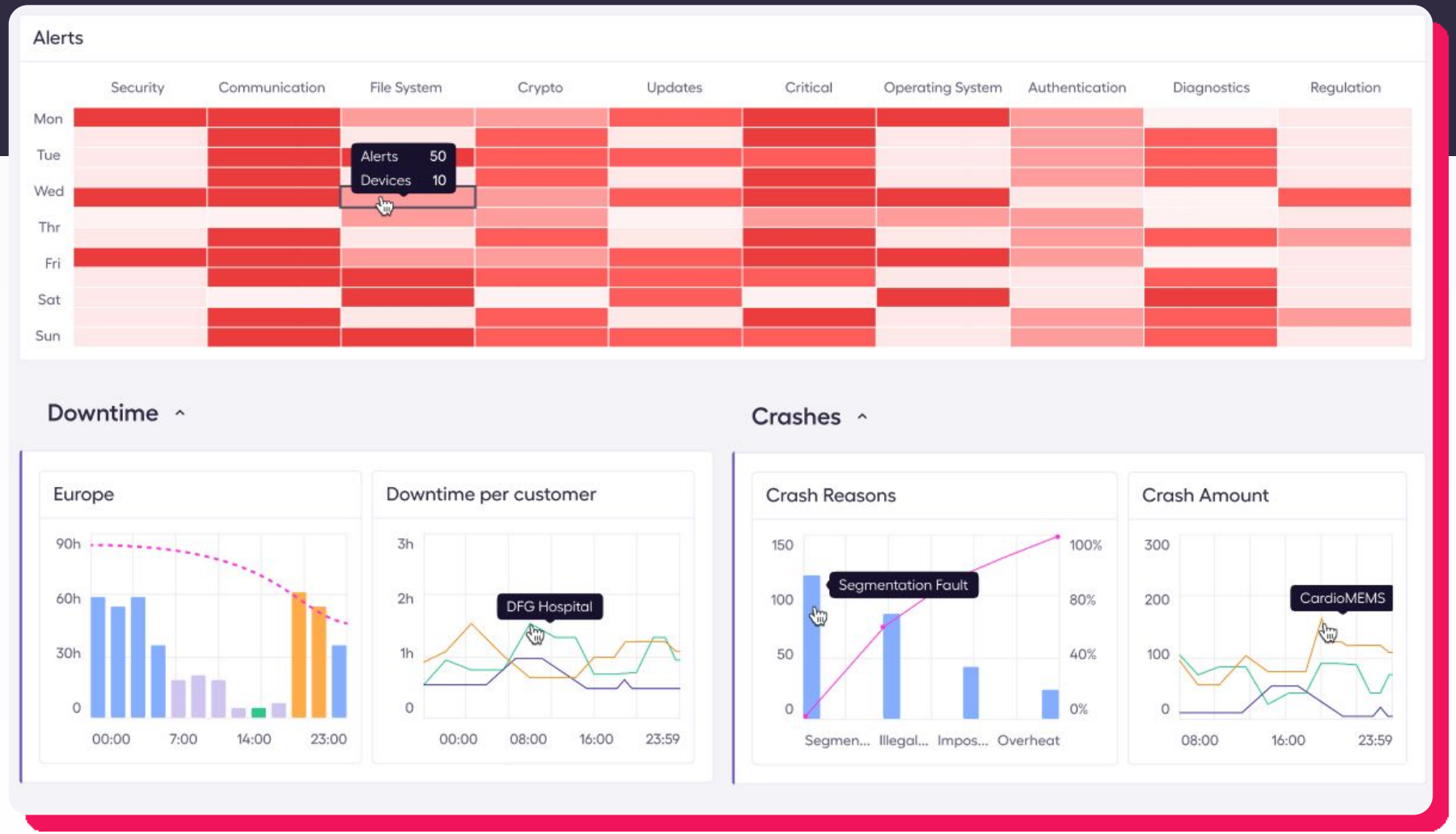




This is simulated data *Screenshot from the next version of our platform, currently in development



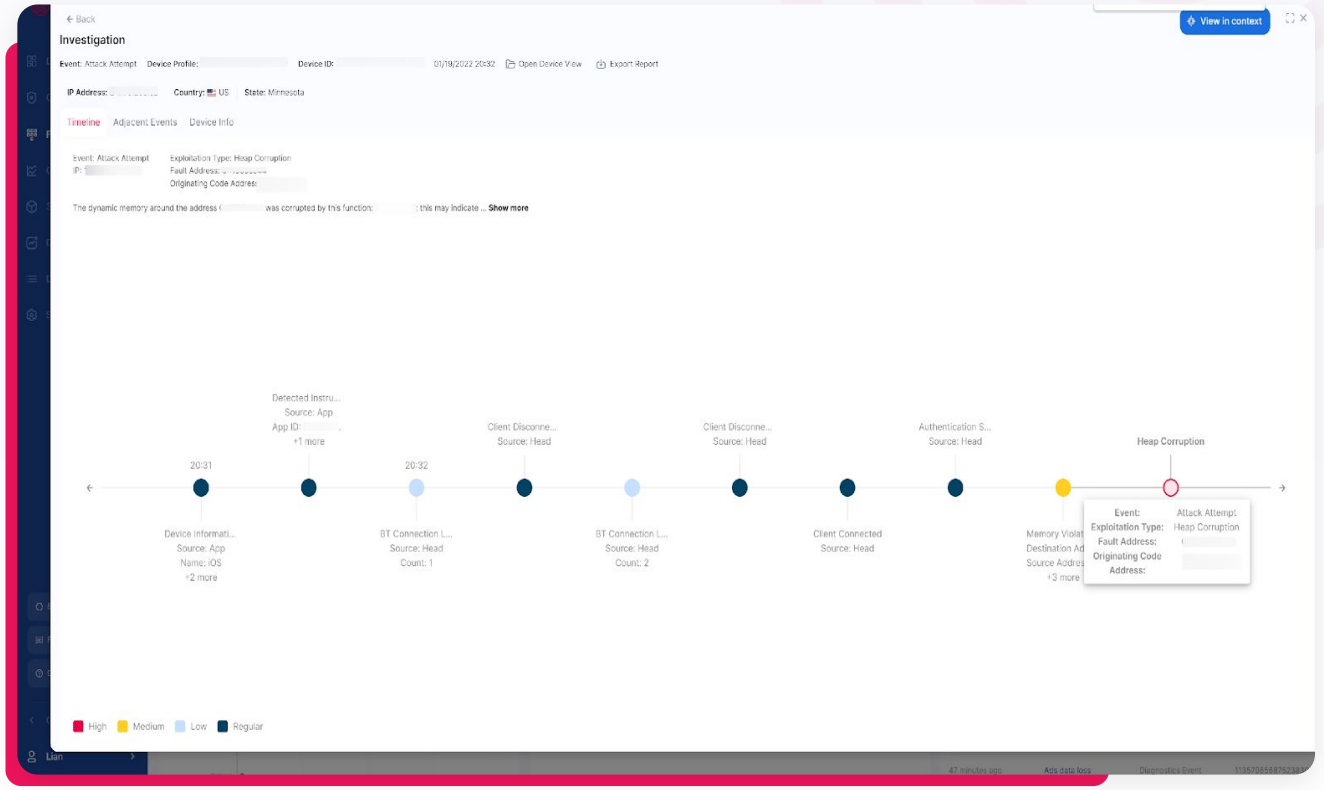
This is simulated data *Screenshot from the next version of our platform, currently in development



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 NXP TX

Undisclosed Fortune 50 Company

Telit VIBRANT Zephyr Project ARM

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