

Check Point
SOFTWARE TECHNOLOGIES LTD.

VULNERABILITY PROTECTION

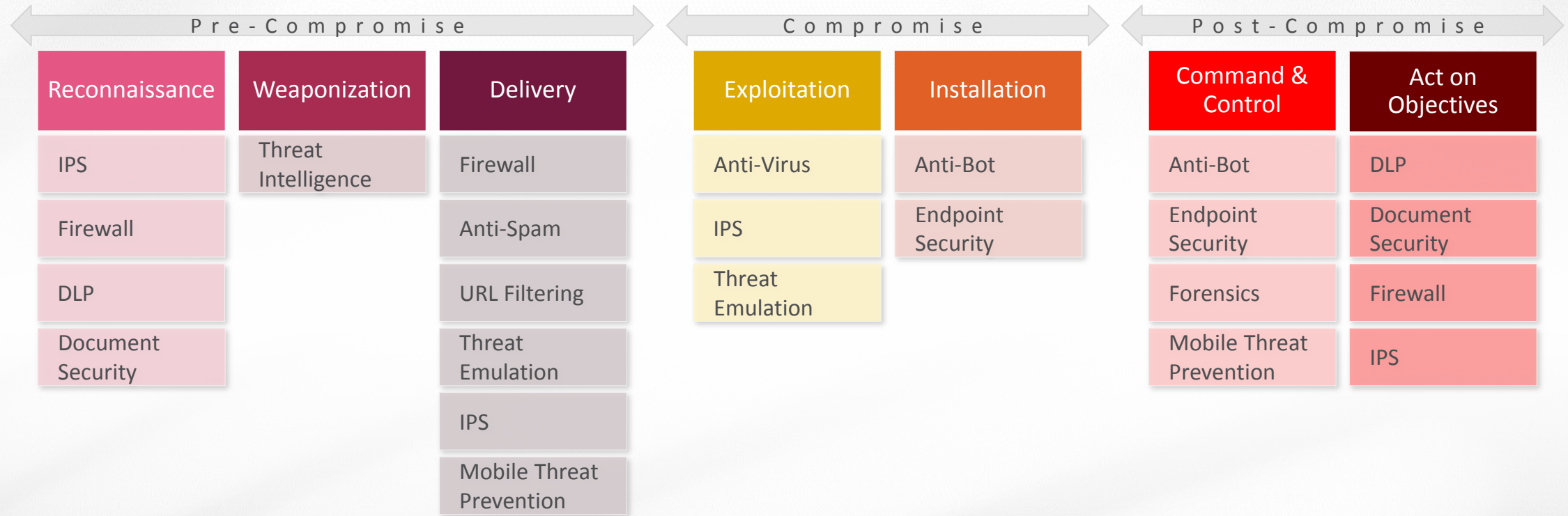
Eusebio Nieva
SE Manager for Iberia



Protection Cycle



Vulnerability Defense with Check Point



BEST INTELLIGENCE

- Over 150 research experts
- Collaboration with industry leading services
- Sharing across users community

BEST DETECTION

- Multi-layer architecture
- Evasion-resistant detection
- Comprehensive protection

BEST PREVENTION

- Proactive practical prevention
- Effective containment
- Clear visibility and insight

Multi Layered Vulnerability Prevention



Check Point
SOFTWARE TECHNOLOGIES LTD.

IPS

prevents exploits of known vulnerabilities

Anti-Virus

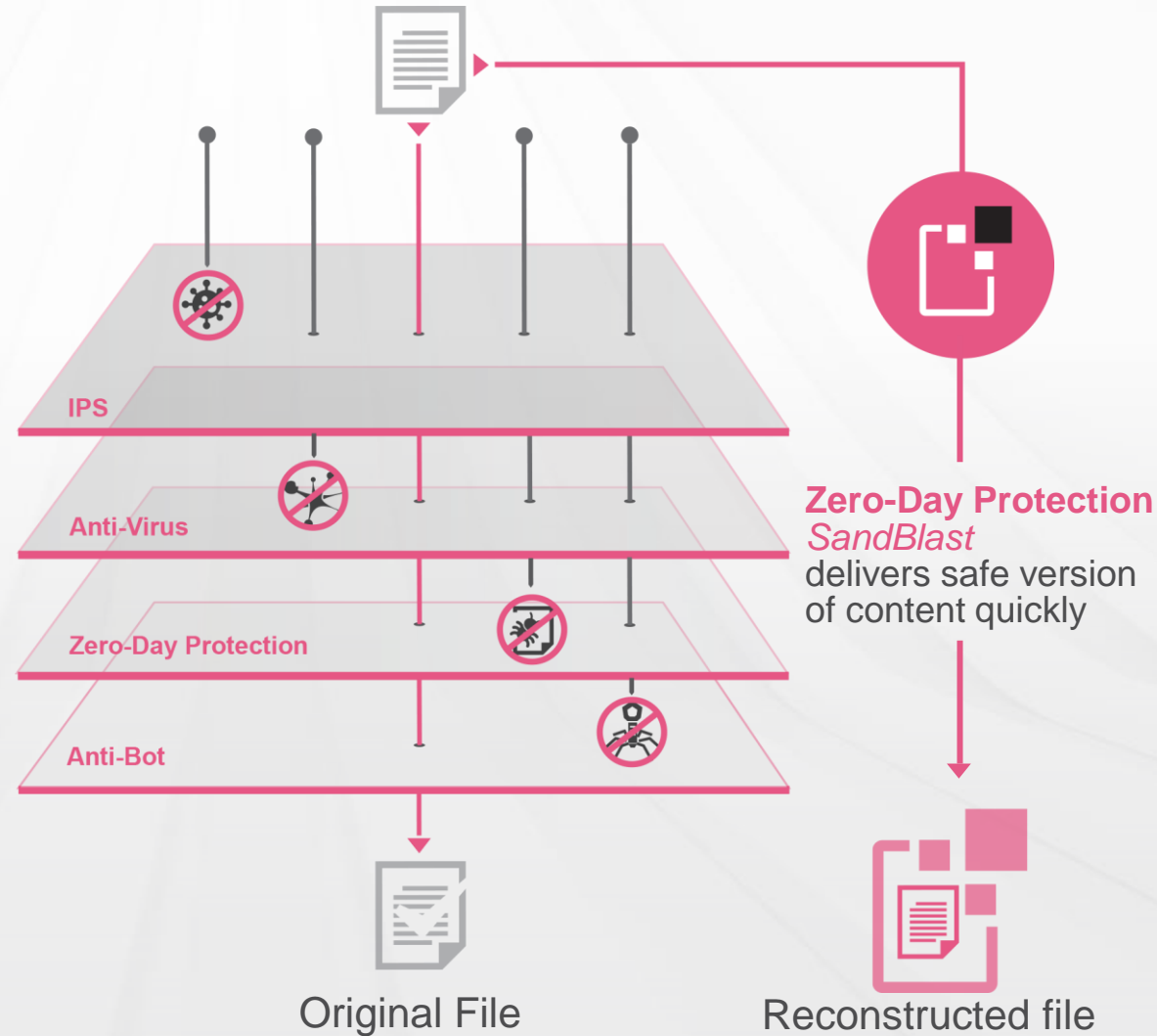
blocks download of known malware infested files

SandBlast Zero-Day Protection

Multiple technologies to protect against zero-day and unknown malware in files

Anti-Bot

detects bots and prevents command and control communications





IPS Virtual Patching



8360 Protections

Zero Days and Urgent Updates

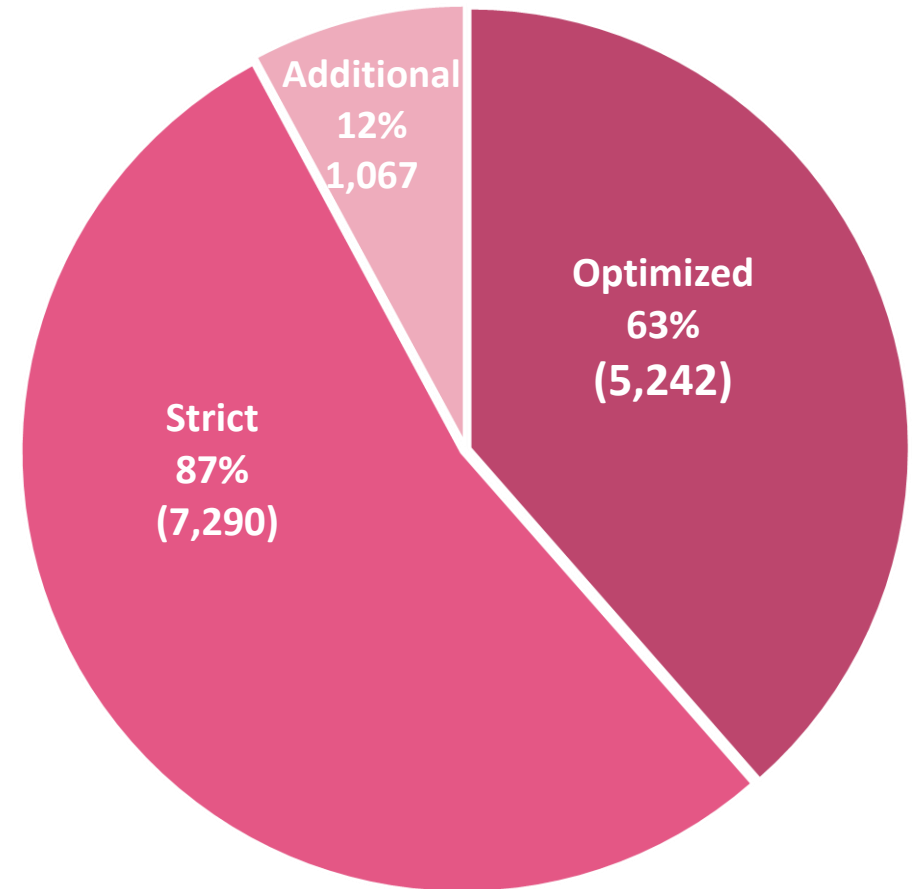
Almost **daily** updates

Microsoft Patch Tuesday

A large variety of **products** and **protocols**

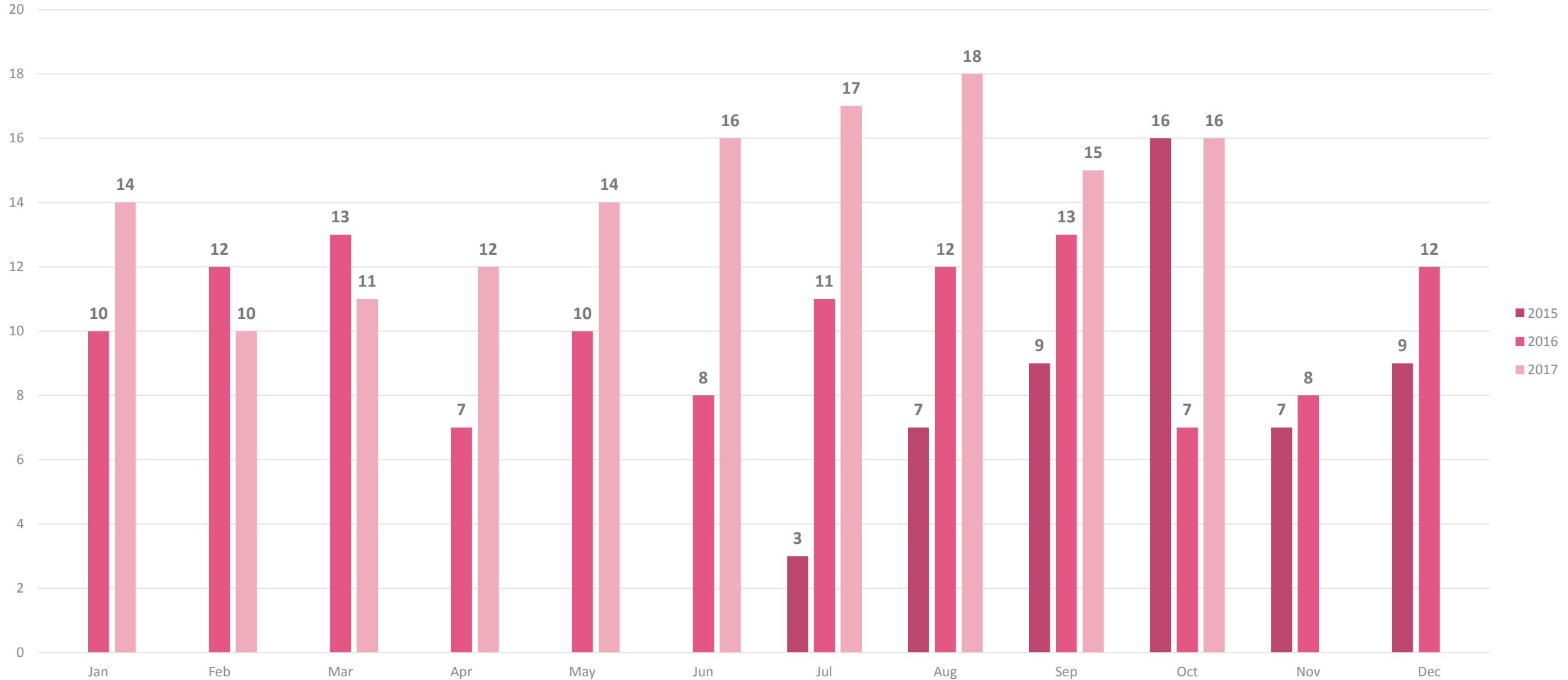
Internal Research

Customers' Response



IPS Package – Releases

Package Release per Month by Year

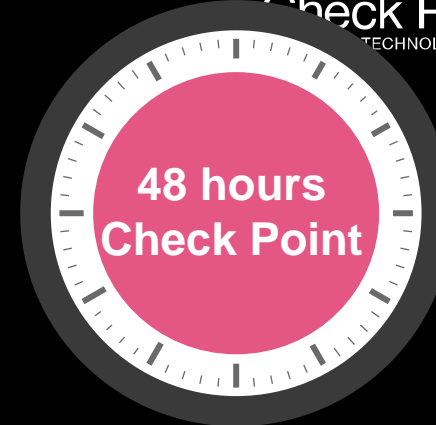


WELCOME TO THE FUTURE OF CYBER SECURITY

TO MAKE SURE OUR CUSTOMERS ARE NOT VULNERABLE ...



Check Point
TECHNOLOGIES LTD



Microsoft Patch
Tuesday



Apache Struts 2
CVE=2017-9805, CVE-2017-9791



Flash 0day
CVE-2017-11292



Disdain EK
CVE-2017-0037, CVE-2017-0059





Research

[Restricted] ONLY for designated groups and individuals

Response to Active Cyber Threat

- 24/7 0Days response
- Malspam, File infection techniques
- TCP and UDP Network Protocols exploitations – SMB, SSL, RDP, DNS, NTP
- Exploit Kits
- CMS - WordPress, Joomla, Drupal
- Hacking Tools, scanners. Evasion Techniques
- PowerShell lateral Movement
- IoT & Scada
- On demand protections to customers

Vulnerability Prevention Cooperation



Check Point
SOFTWARE TECHNOLOGIES LTD.

TOC

Threat Intelligence

Incidence Response

Malware Research

Exploit Research

Anti-Bot Research

Threat Response



Check Point Vulnerability Research



Check Point[®]
SOFTWARE TECHNOLOGIES LTD.

- **Assessment** – Regularly assess common software, devices and Internet platforms that can affect enterprise and home user security.
- **Disclosure** - Report findings to vendors prior to public disclosure, pushing towards a more secure eco-system.
- **Prevention** - Create protections in Check Point products to prevent future attacks.
- **Share** - Share knowledge via reports and infosec conferences worldwide to educate the community and public.

Over 40 Responsible Disclosures CVEs since 2014

Exploit Kits



RIG



Magnitude



Sundown



Neptune

RIG

Sundown

Magnitude

Neutrino

Neptune

HanJuan

Fiesta

Archie

Astrum

Gondad

Disdain

Hunter

Sedkit

BlackHole

WordPress Protection

- WordPress Core, Plugins & Themes Vulnerabilities
- Automated WordPress Attacks
- Dedicated Scanners (i.e.: WPScan)
- Web shells & Server Ransomwares
- Over 100 IPS protections –Sep 2017
- <http://blogs.checkpoint.com/yardenko/weaponized-wordpress-tools/>



• Zero Day Vulnerabilities

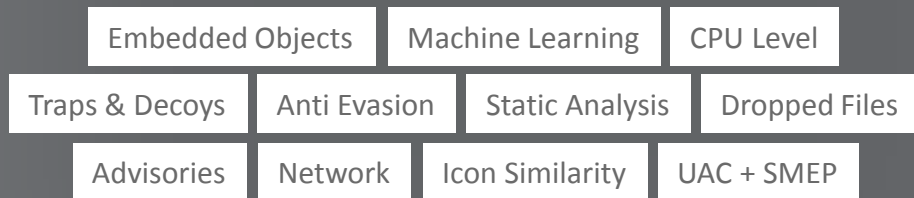
Ej: Spectre, Meltdown, Bashware



SANDBLAST THREAT EMULATION

Blocks unknown malware
and zero-day attacks

Detection engines



HIGHEST CATCH RATE

100% catch-rate for email unknown malware*
99.4% overall breach detection rate

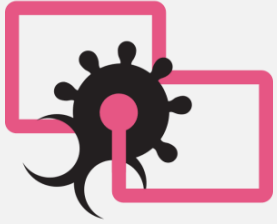
EVASION RESISTANT

100% evasion resistant sandbox*

EFFICIENT AND FAST

Average of 3 mins per unique file

EXAMPLE:



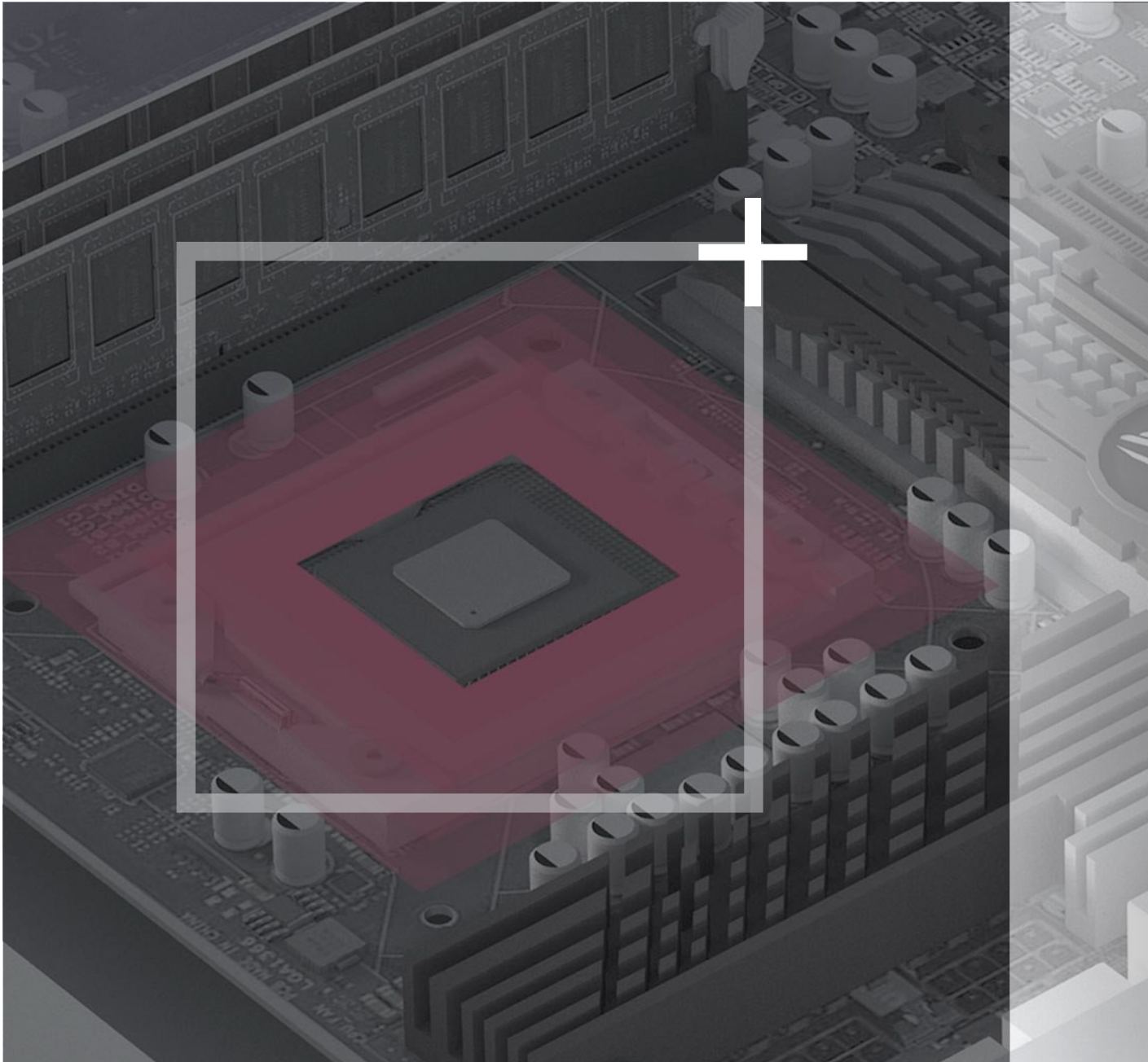
CPU-LEVEL DETECTION ENGINE

And Additional Static and Heuristic Engines



SANDBLAST DETECTS EXPLOITATIONS BY IDENTIFYING CPU LEVEL ANOMALIES

Before the malware is downloaded
and before the evasion code can execute



LEVERAGING THE HASWELL CPU

- Tracks the flow of branch operations.
- Deterministic exploit detection

**PATENTED TECHNOLOGY,
EXCLUSIVE TO CHECK POINT**

3rd LINE OF DEFENSE

FORENSIC ANALYSIS



COLLECT FORENSICS DATA AND TRIGGER REPORT GENERATION

2 Report generation automatically triggered upon detection of network events or 3rd party AV

1 Forensics data continuously collected from various OS sensors

4 Digested incident report sent to SmartEvent



3 Advanced algorithms analyze raw forensics data

User Name: xxxxxx
Computer: xxxxxx
Incident ID: wcry_full_attack_analysis1494...
Trigger: c:\users\xxxxxx\downloads\wcry.exe
Triggered By: SandBlast Agent Anti-Ransomware Blade E80.65
Trigger Time: 5/15/2017, 3:52:53 PM

Need insight? [Email us.](#)
INCIDENT RESPONSE TEAM
CHECK POINT

Entry Point

How did it enter the system?
Accessed [172.217.16.163] in chrome.exe

What were the action taken to remediate?

Remediation (32 files)

Was an infection present and removed?

REPUTATION	FILE NAME	FULL PATH	STATUS
★	@wanadecryptor@.exe	c:\users\xxxxxx\downloads\@wanadecryptor@.exe	🗑️
★	@wanadecryptor@.exe	c:\users\xxxxxx\downloads\@wanadecryptor@.exe	🔧
★	@wanadecryptor@.exe	c:\users\xxxxxx\downloads\@wanadecryptor@.exe	🔧
★	@wanadecryptor@.exe	c:\users\xxxxxx\downloads\@wanadecryptor@.exe	🔧
★	@wanadecryptor@.exe	c:\users\xxxxxx\downloads\@wanadecryptor@.exe	🔧
★	@wanadecryptor@.exe	c:\users\xxxxxx\downloads\@wanadecryptor@.exe	🔧
★	@wanadecryptor@.exe	c:\users\xxxxxx\downloads\@wanadecryptor@.exe	🔧

3

Business Impact (242 events)

What was the damage?

What was the business impact

DAMAGE	FILE NAME	FULL PATH
📄	2014-financial-statements-en.pdf	c:\users\xxxxxx\desktop\2014-financial-statements-en.pdf
📄	g-example-donor-report.doc	c:\users\xxxxxx\documents\g-example-donor-report.doc
📄	g-finance-manual-maf.pdf	c:\users\xxxxxx\documents\g-finance-manual-maf.pdf
📄	g-finance-staff-jd.doc	c:\users\xxxxxx\documents\g-finance-staff-jd.doc
📄	g-procurement-manual.doc	c:\users\xxxxxx\documents\g-procurement-manual.doc
📄	g-sample-jds.rtf	c:\users\xxxxxx\documents\g-sample-jds.rtf
📄	g_budget-worksheet-example.xls	c:\users\xxxxxx\documents\g_budget-worksheet-example.xls

2

Suspicious Activity (15 categories)

What happened in the system?

SEVERITY	EVENT CATEGORY
●●●●●	Shadow Copy Deletion (2 events)
●●●●●	Tor Communication (5 events)
●●●●●	Tor Application Download (1 event)
●●●●●	File Access Control List Modification (1 event)
●●●●●	Privilege Change (3 events)
●●●●●	Script Execution (1 event)
●●●●●	Dropped File Deletion (2 events)

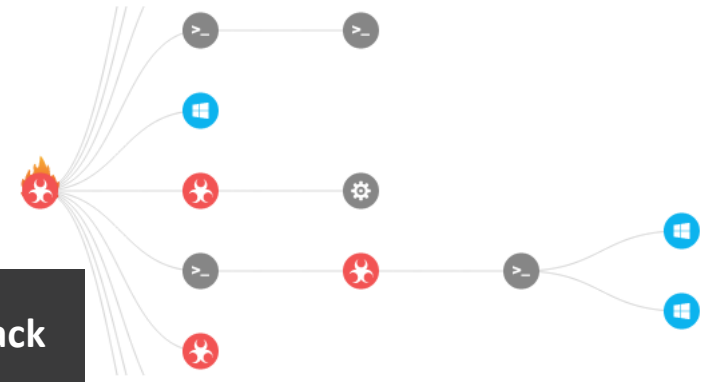
1

**Is this attack Real?
What events occurred?**

Incident Details (26 processes)

How do I analyze further?

Show me the attack flow



A man in a dark suit and striped tie stands next to a woman in a black dress. They are both looking at a tablet computer held by the woman. The background is a blurred indoor setting. The entire image is overlaid with a semi-transparent pink gradient.

Thank You