



Proactive Security
Starts Here

From Buffer Overflows to Breaking AI

Two Decades of ZDI Vulnerability Research

Brian Gorenc
Exploit Historian



20

20



20



POC / 2015 / Slides

Andrei Costin, "Security of Embedded Devices' Firmware - Fast and Furious at Large Scale"

Brian Gorenc, Abdul-Aziz Hariri, Jasiel Spelman, "Analyzing Arcane Attack Vectors: Adversary Emulation"

Celli UNUVER & Ebubekir KARUL, "Breaking Font Parsers"

Florian Grunow, Felix Wilhelm, "Hacking IBM's GPFS"

Fyodor Yarochkin, Vladimir Kropotov, "Pearls of Non-exploitation Based Recon Tactics"

Gilgil, Yeongsik Moon, "Wireless(WPA) Network Based Packet Dissecting"

20



20



20

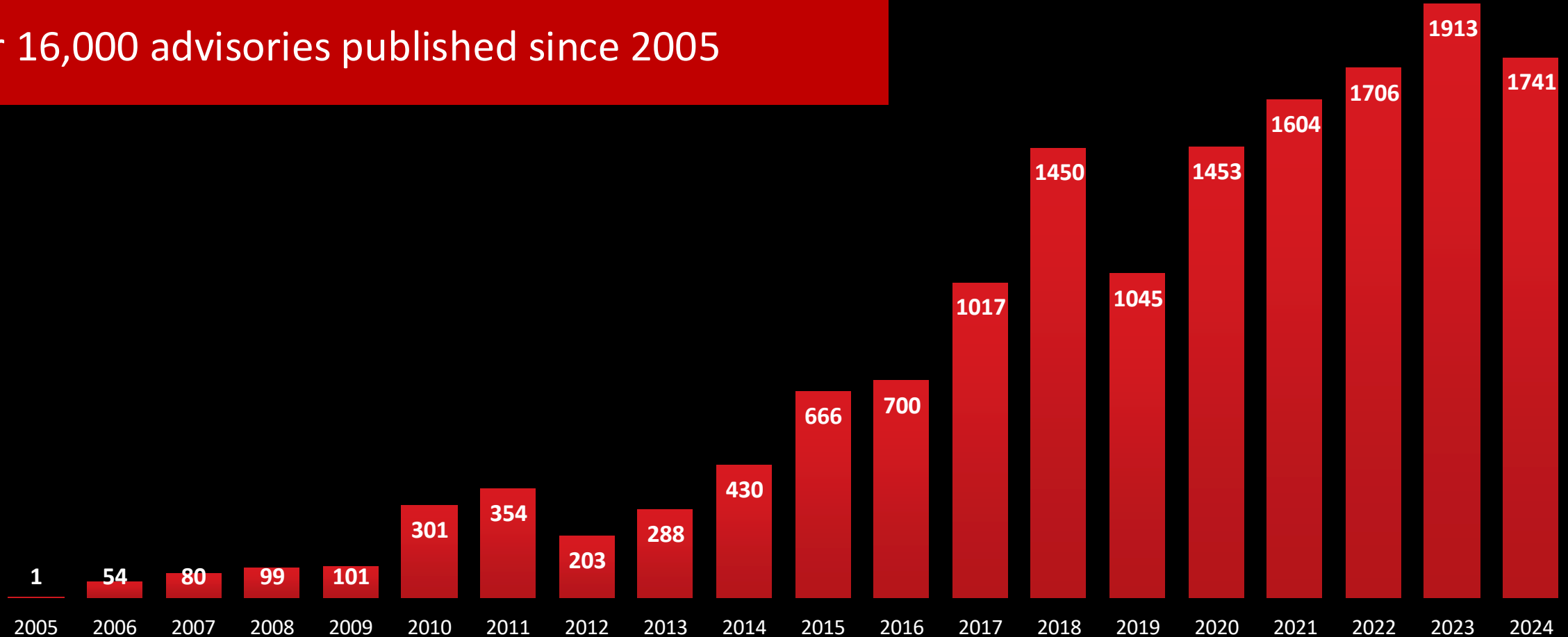




ZERO DAY INITIATIVE

Disclosures Per Year

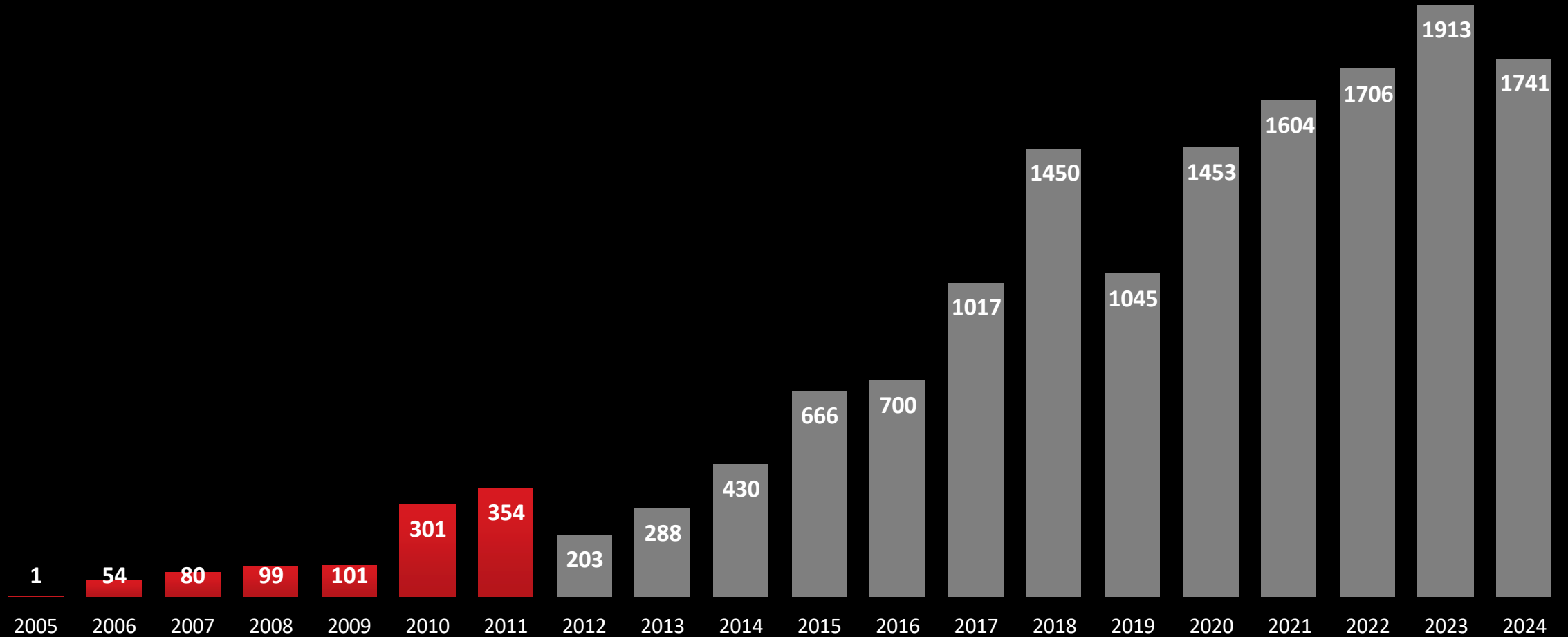
Over 16,000 advisories published since 2005



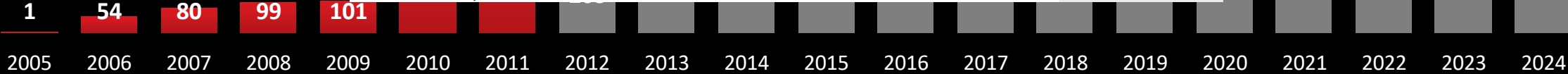
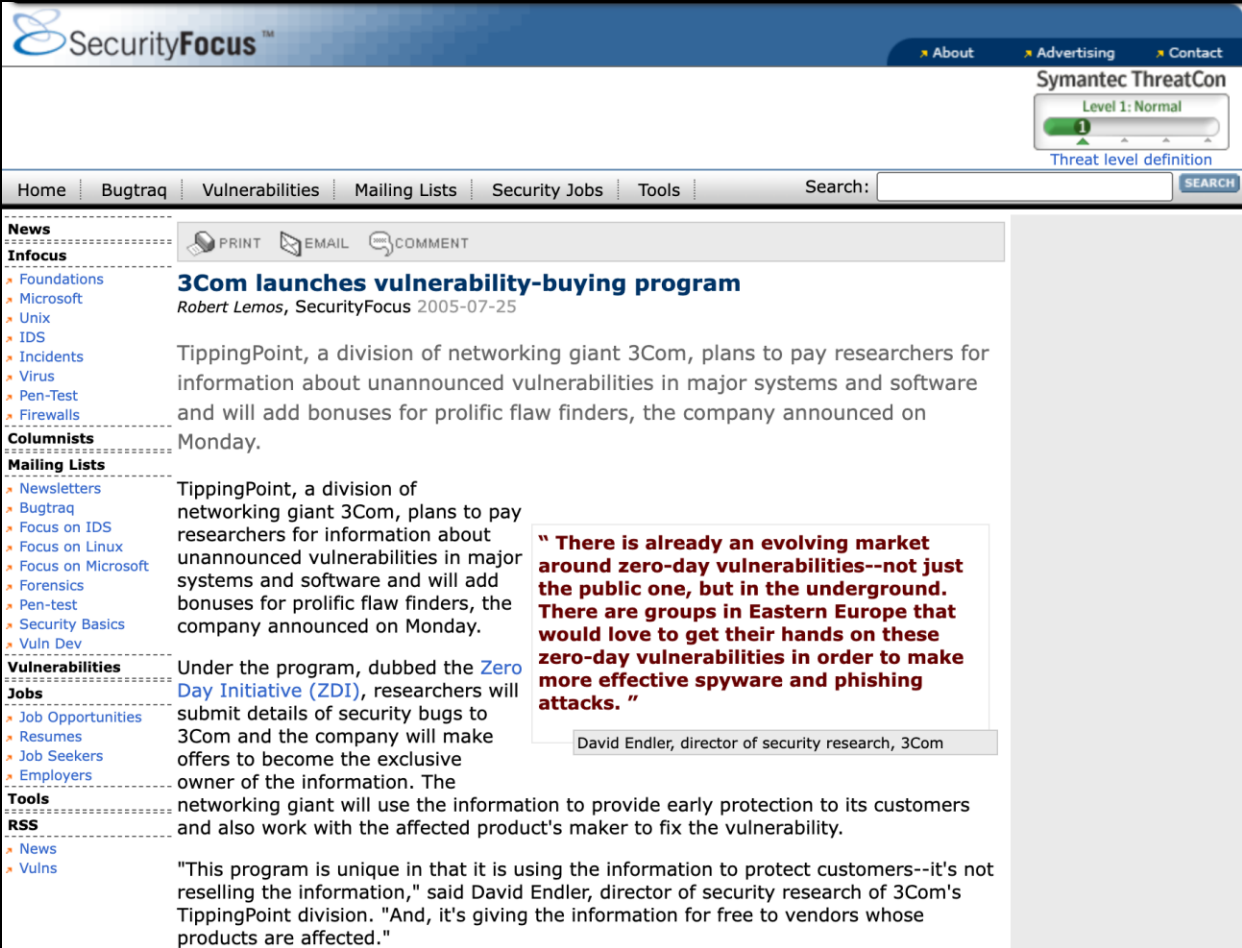
Six Phases



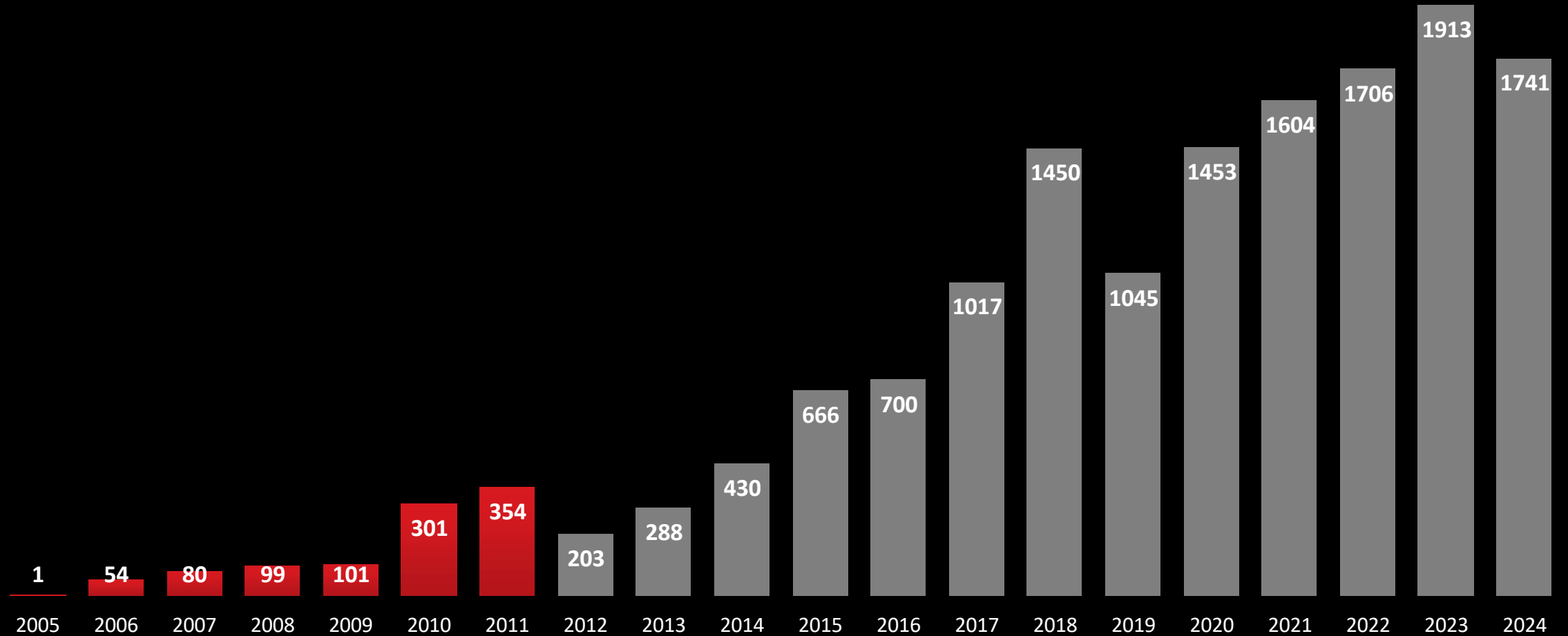
Foundational Years



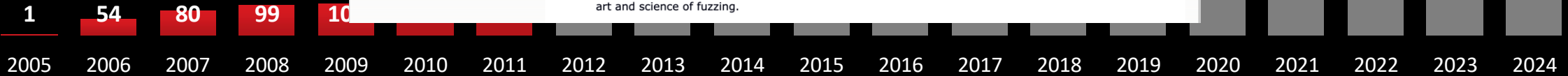
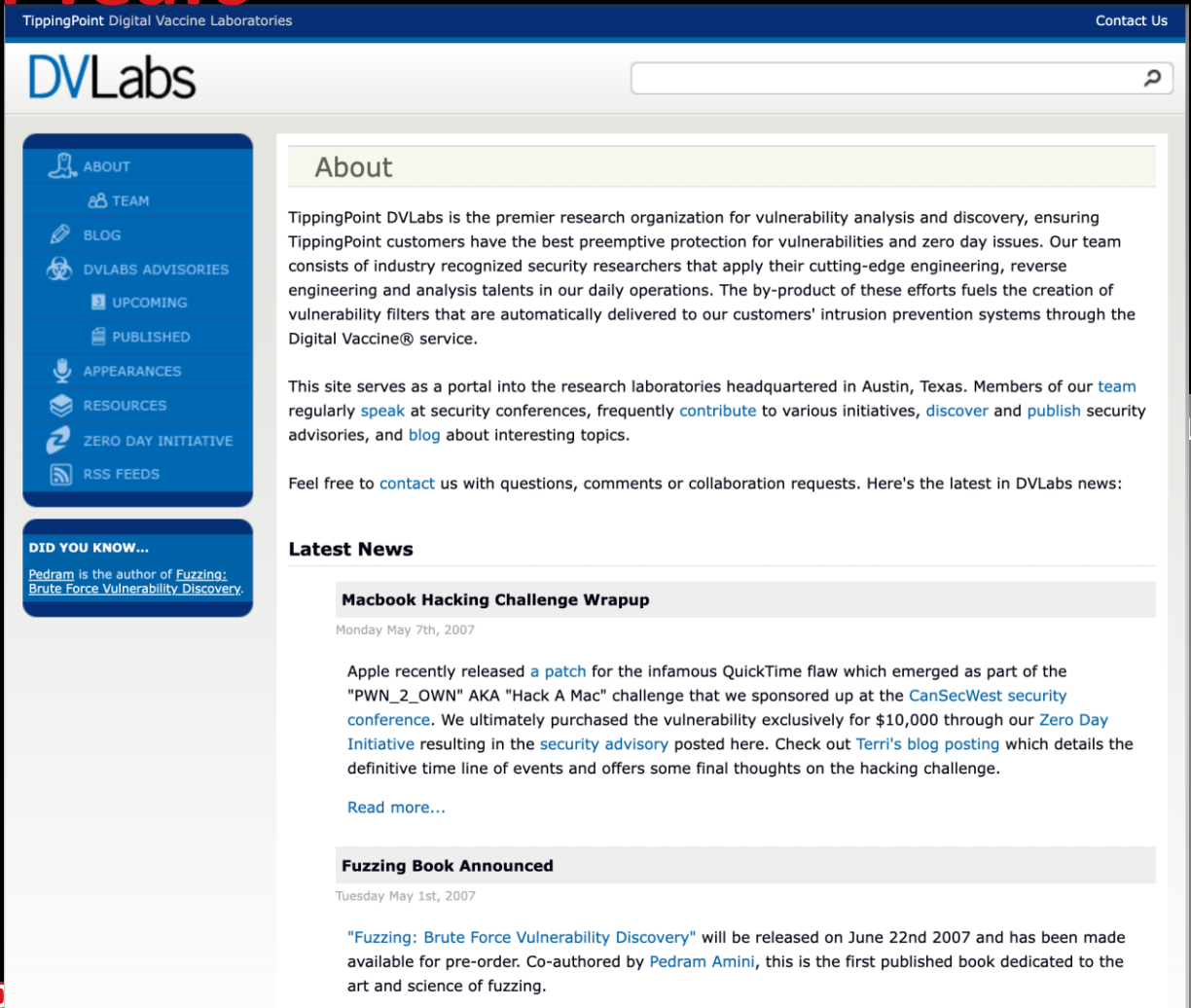
Foundational Years



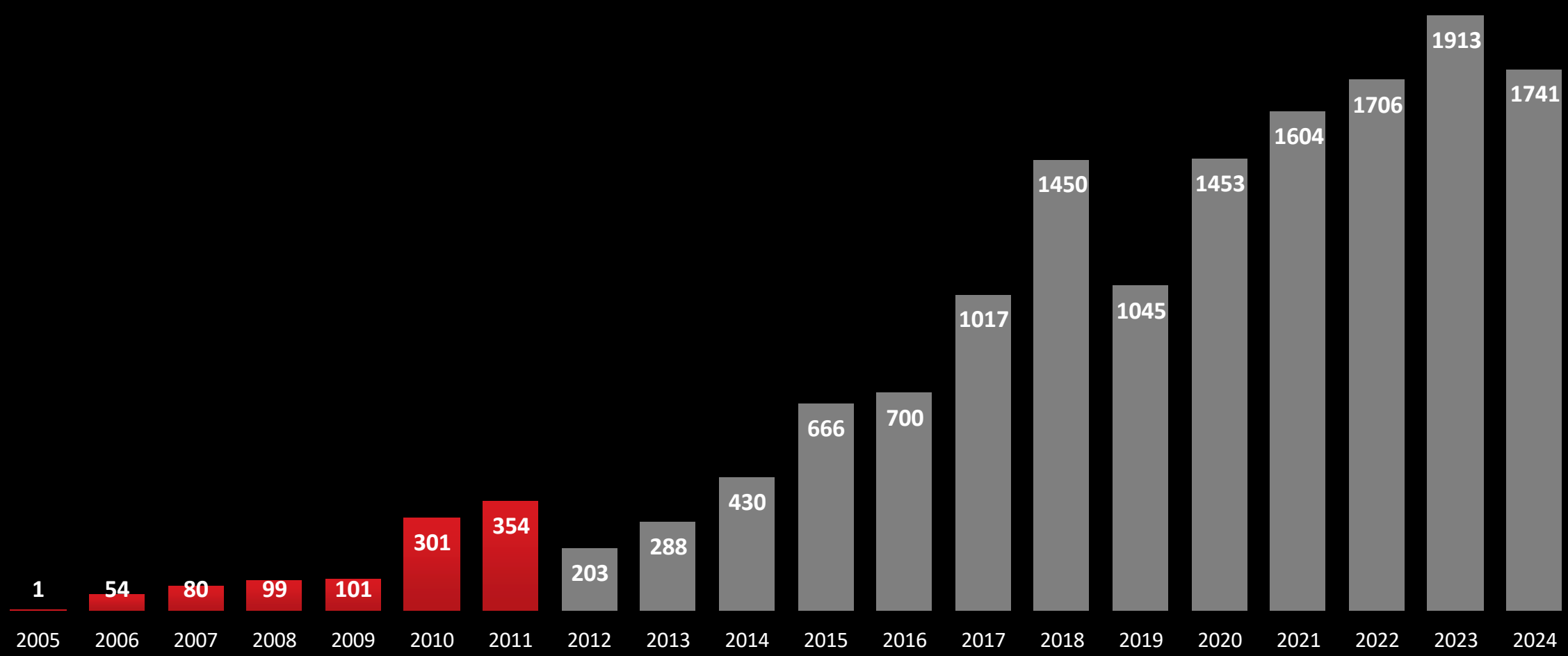
Foundational Years



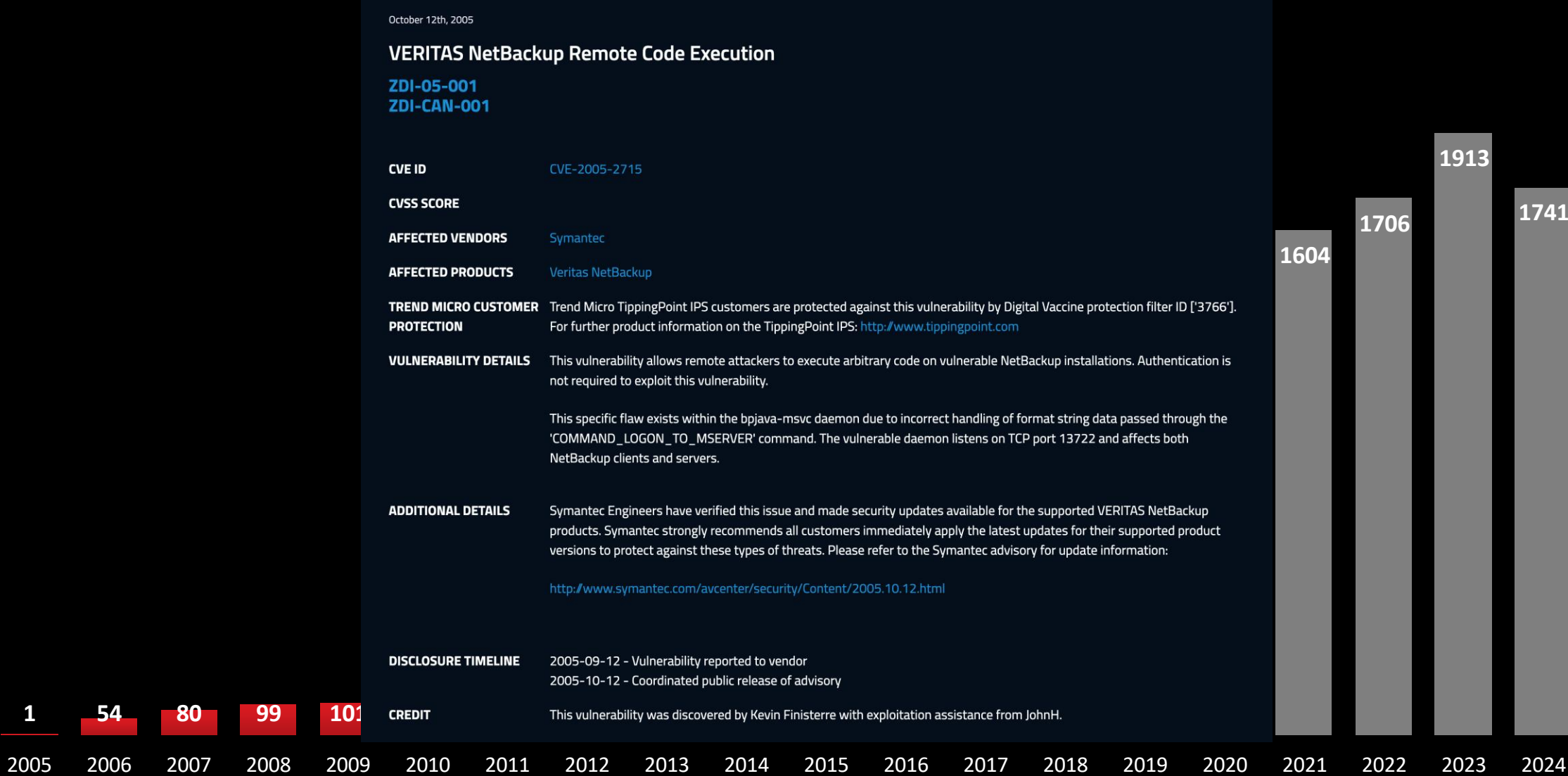
Foundational Years



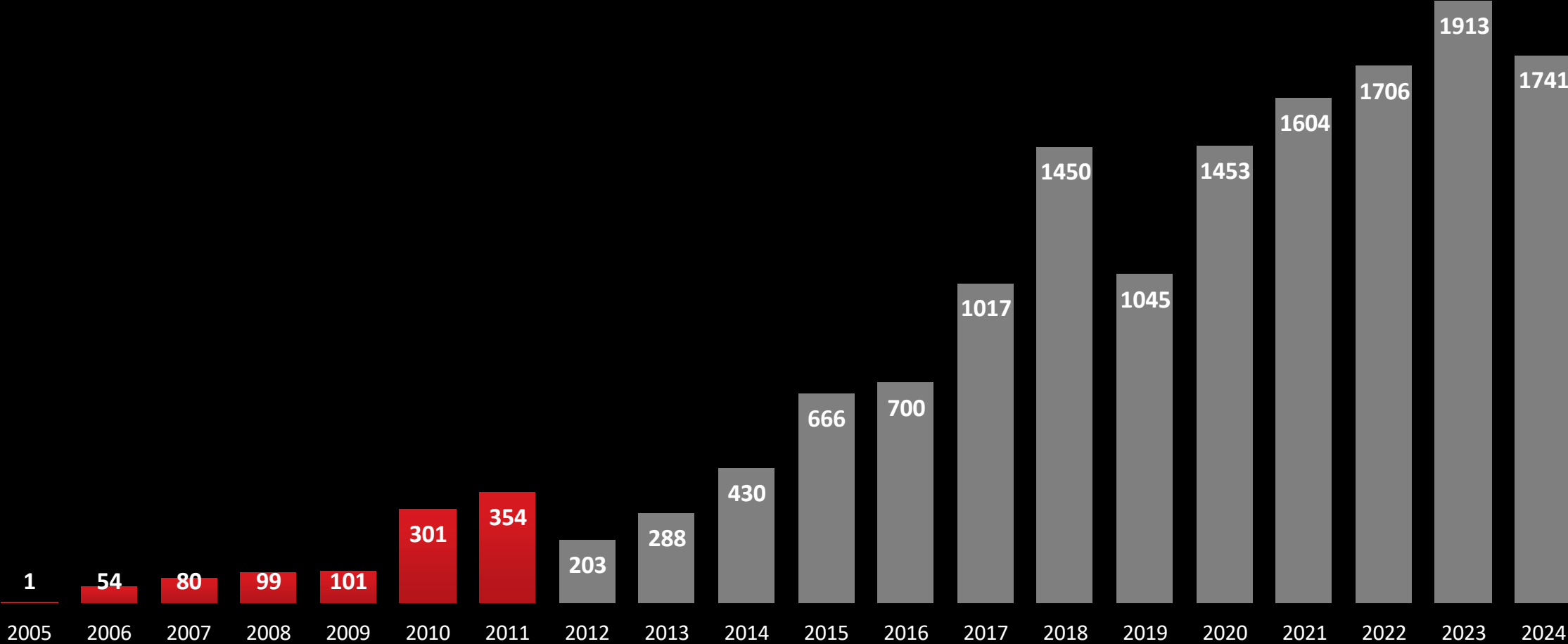
Foundational Years



Foundational Years



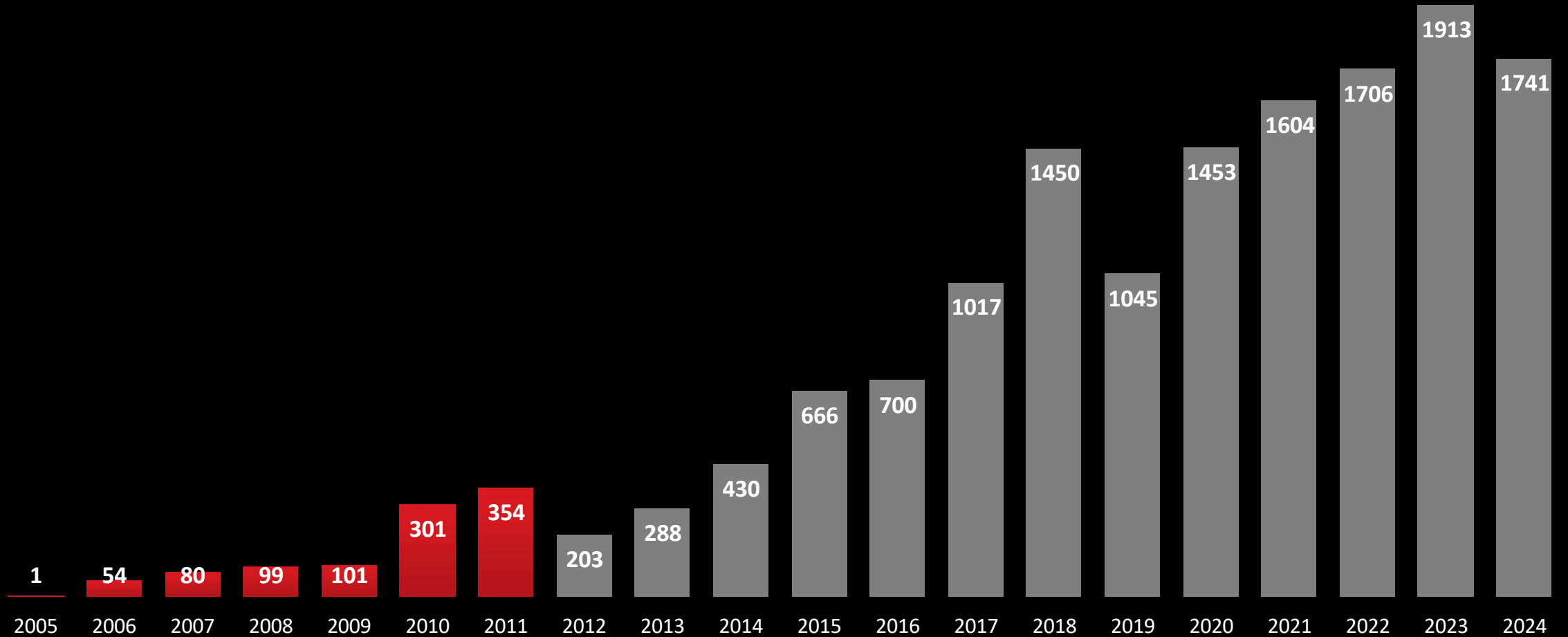
Foundational Years



Foundational Years



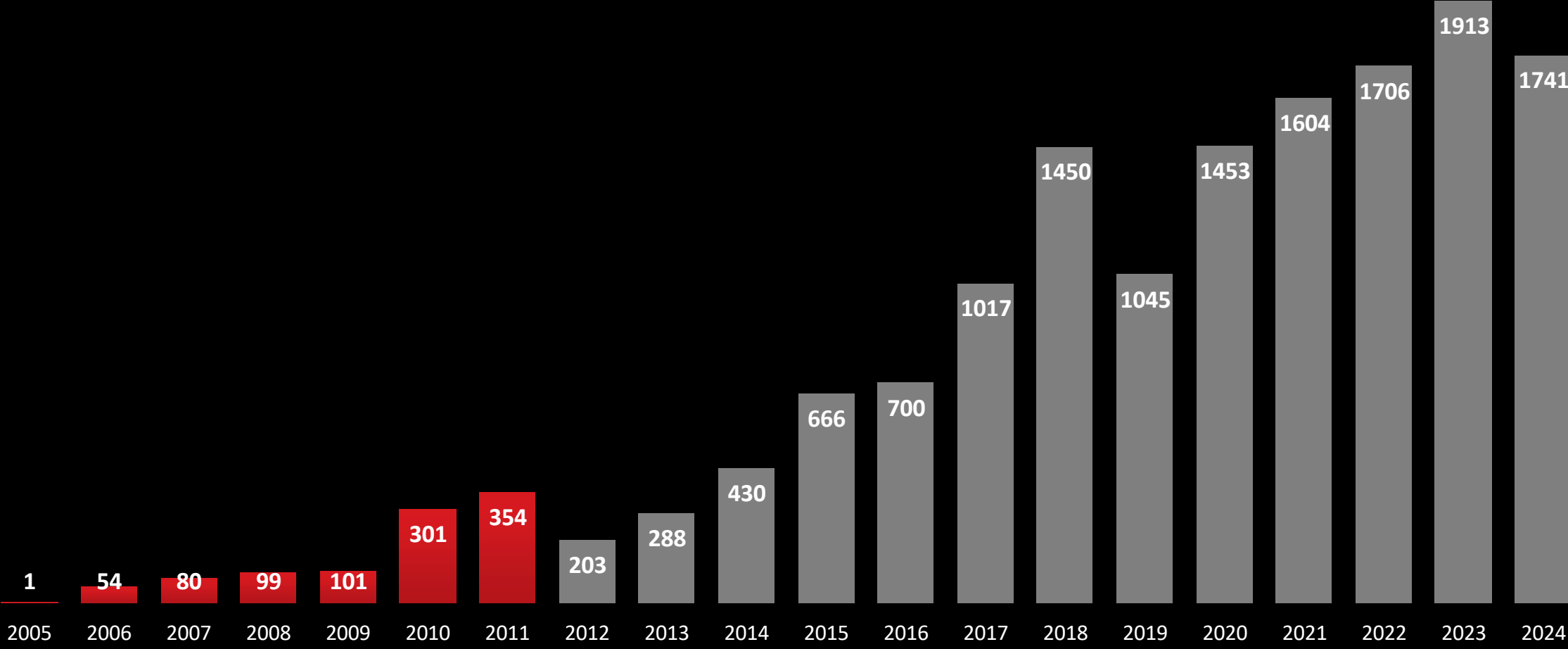
Foundational Years



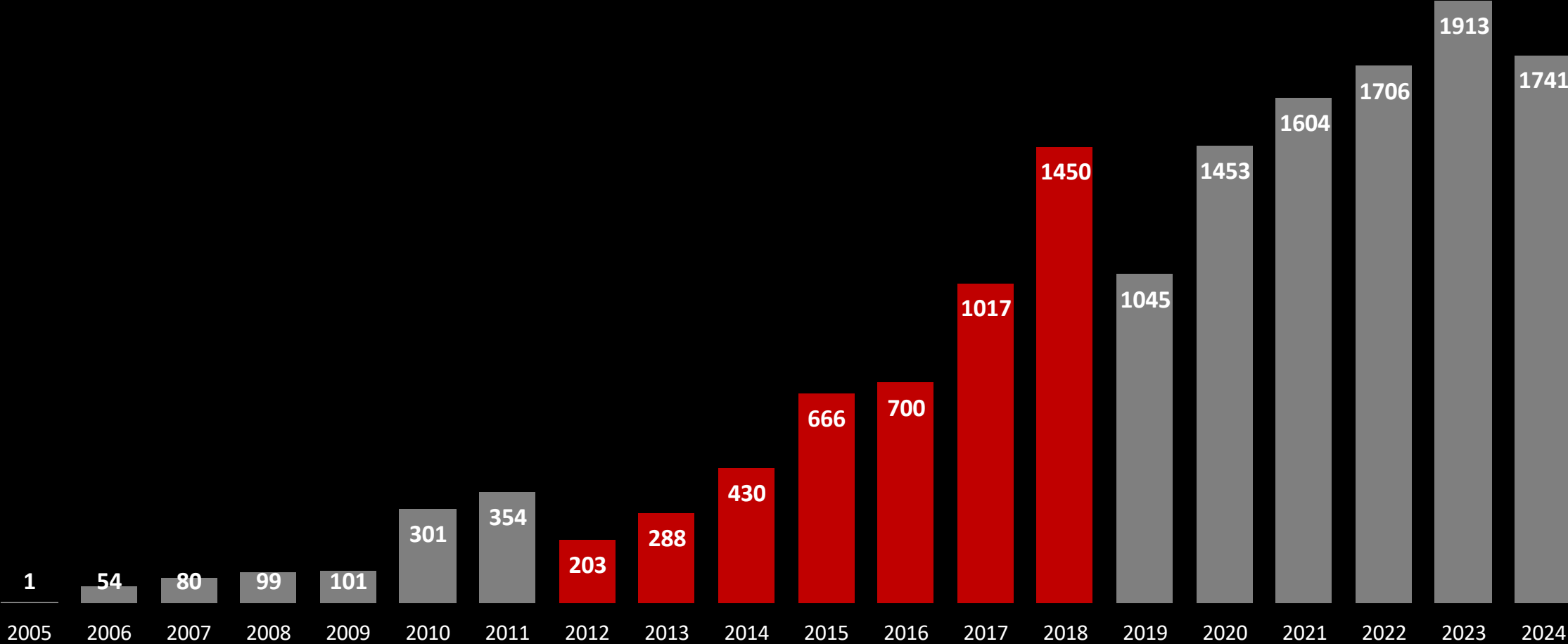
Foundational Years



Foundational Years



Transformational Years







Pwn2Own™
VANCOUVER

Evolution of the Sandbox

In the beginning, Pwn2Own exploits only needed one vulnerability to win.

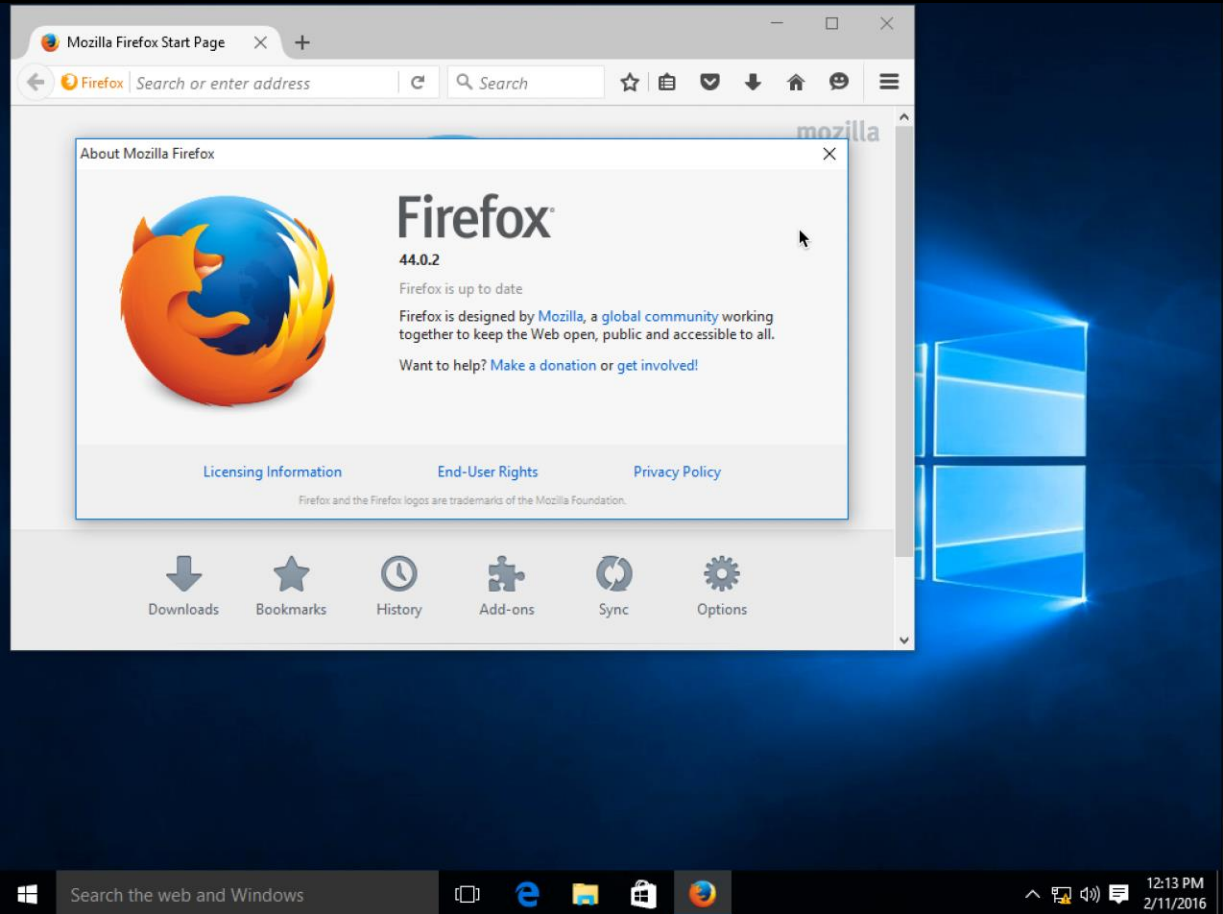
- Use-after-frees were very popular

Vendors implemented sandboxes to mitigate this issue.

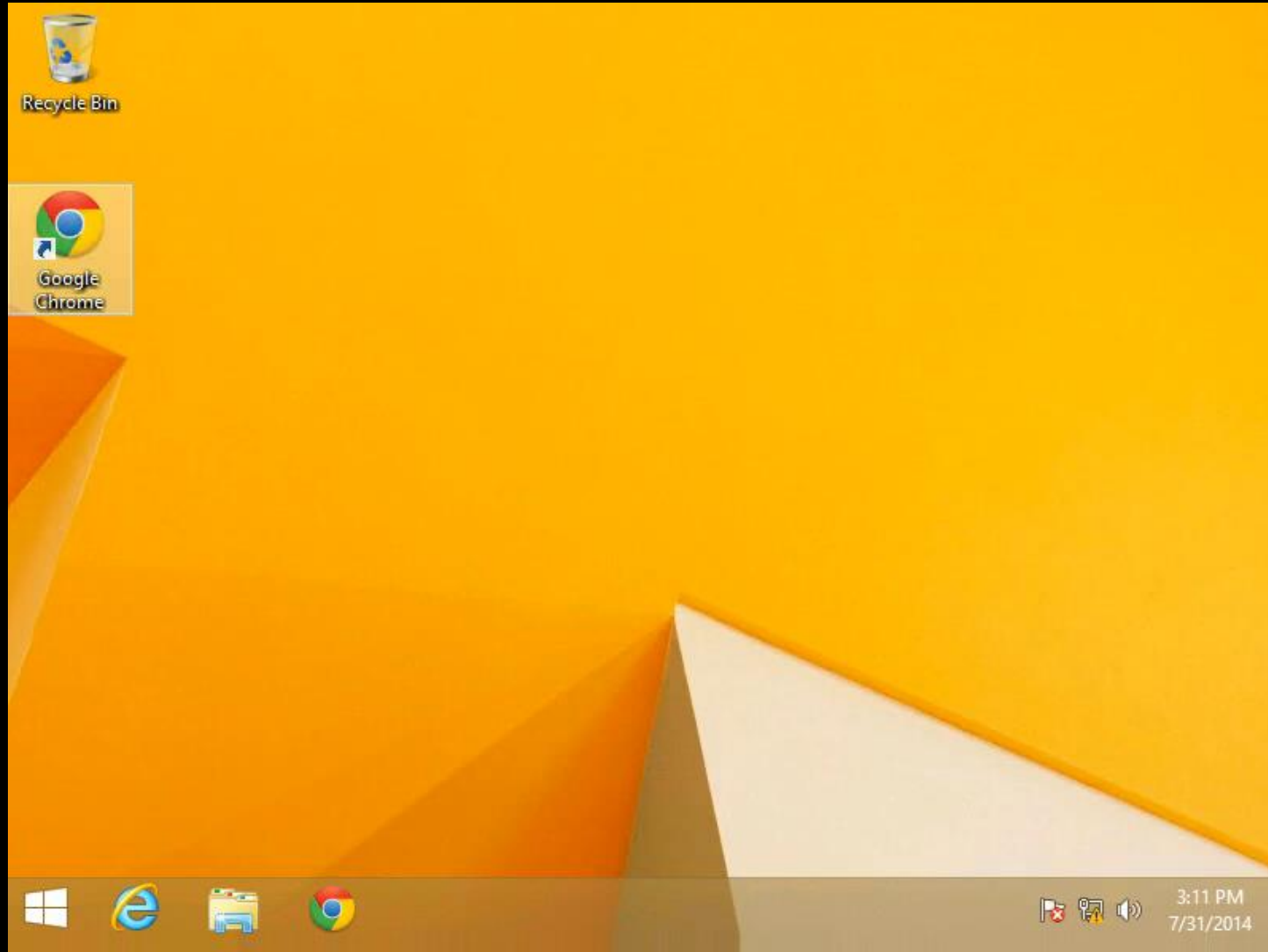
- Assume code execution vulnerabilities exist

Leveraged OS-based Protection Mechanisms

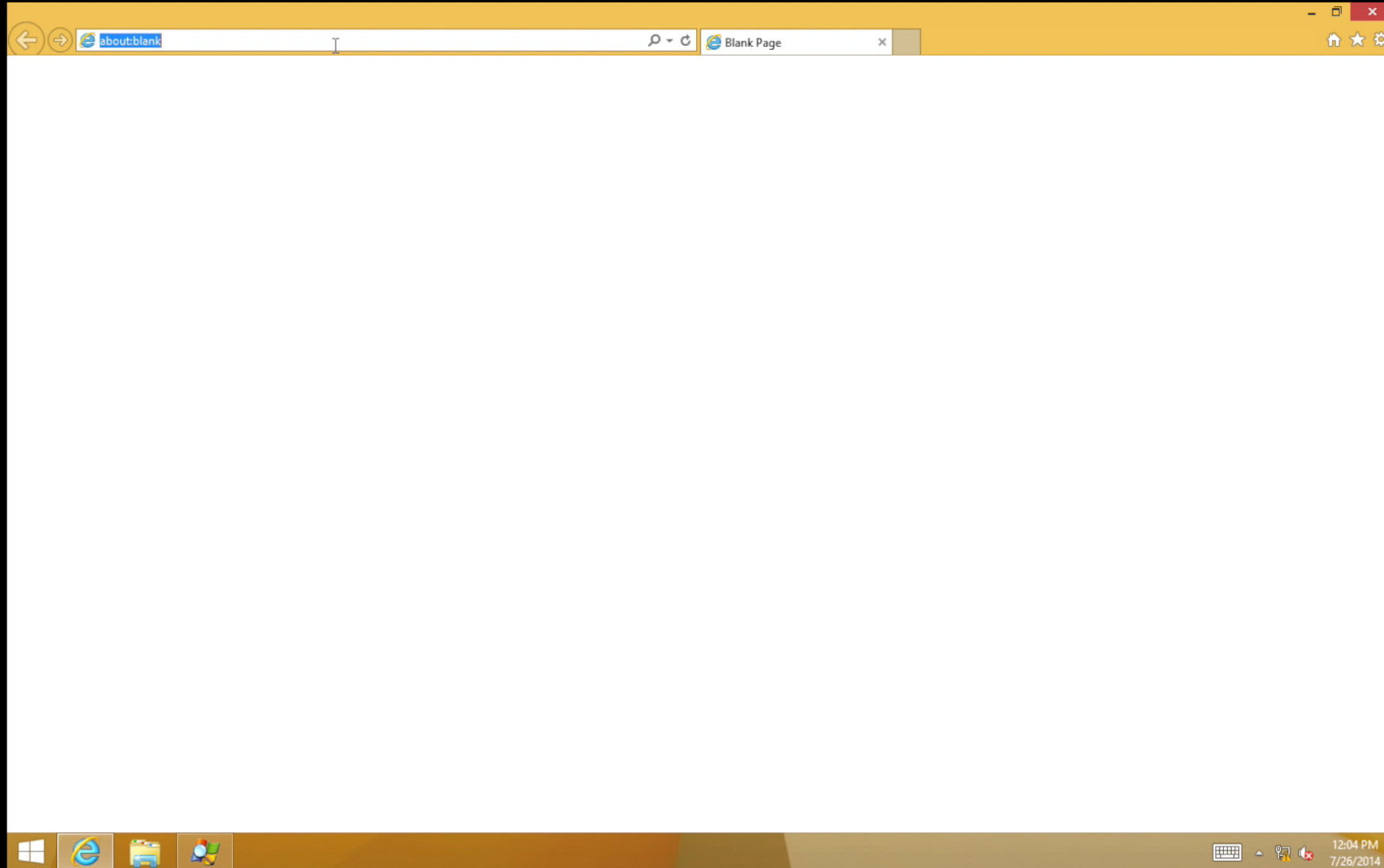
- Window Station and Desktop Isolation
- Job Object Limitations
- Mandatory Integrity Controls
- AppContainers



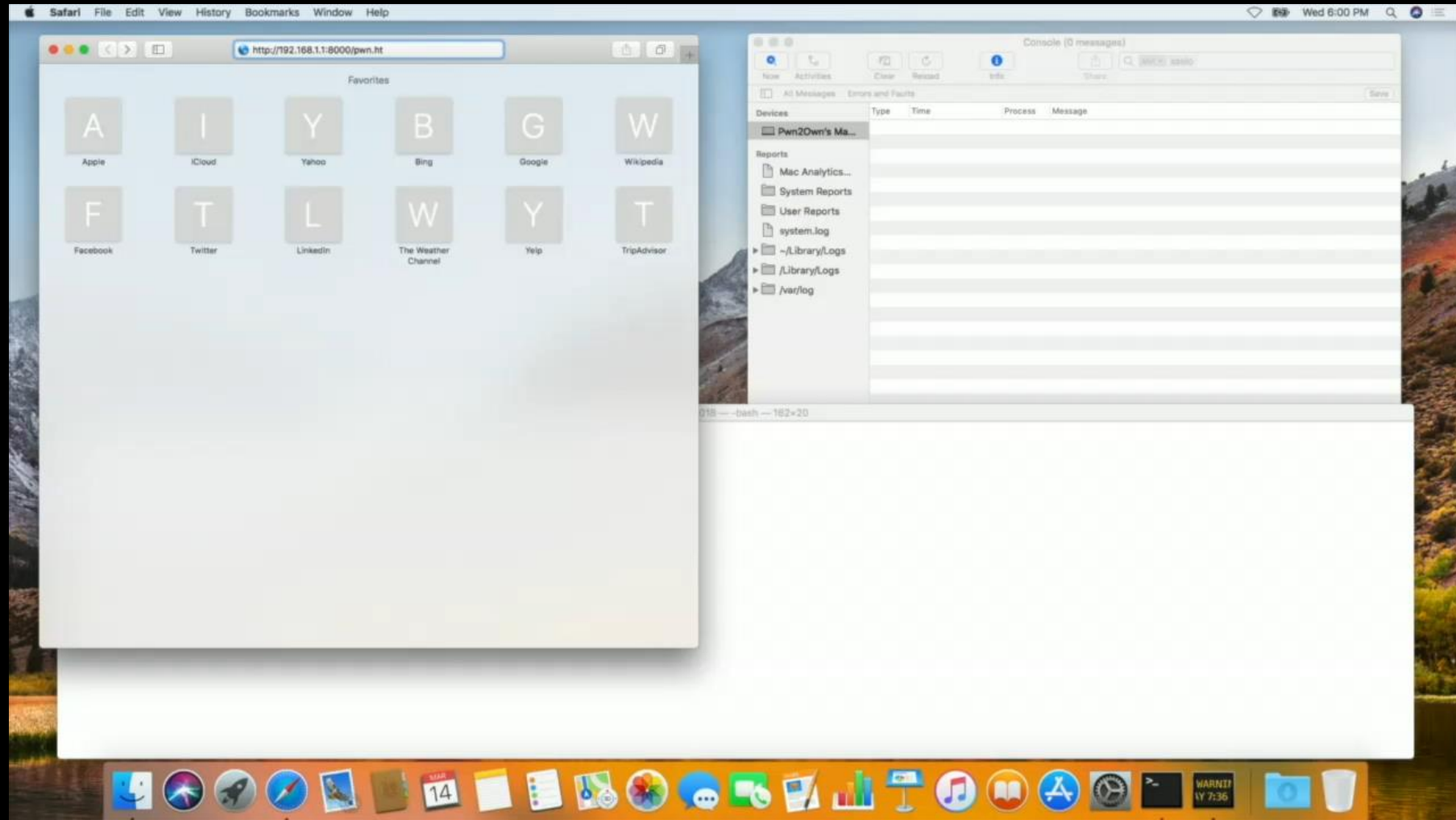
Undocumented Features



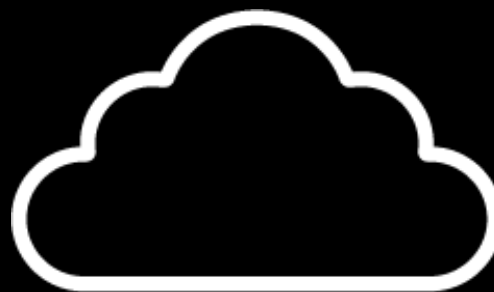
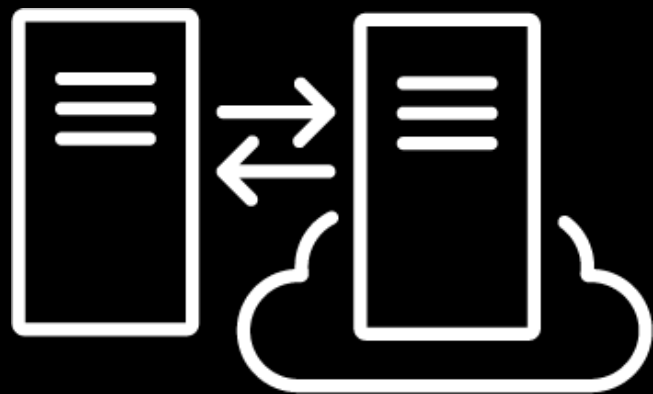
Internet Explorer localhost Sandbox Bypass



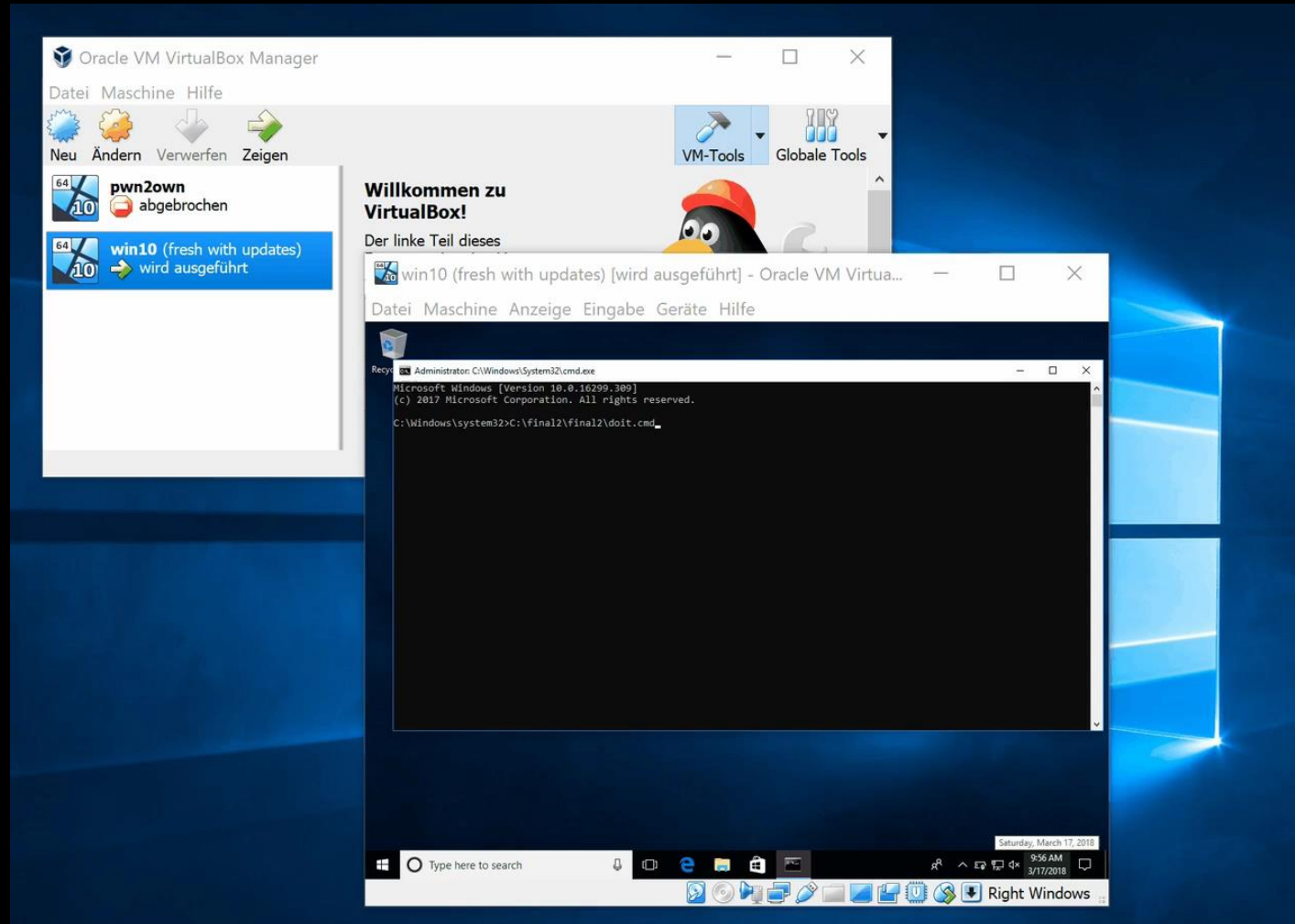
JIT Exploitation in Safari



Shifting Attack Surface



Escaping Oracle VirtualBox



VMware Escapes



Recycle Bin



VMware Workstat...



ProcExp

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-6FGL507\ZDI]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	User Name	Image Type	Integrity
nvxdsvnc.exe	< 0.01	10,588 K	23,856 K	1728			<access denied>		
nvscapiisvr.exe		2,832 K	7,592 K	1516	Stereo Vision Control Panel ...	NVIDIA Corporation	<access denied>		
svchost.exe		13,728 K	21,960 K	1532	Host Process for Windows S...	Microsoft Corporation	<access denied>		
igfxCUIService.exe		1,704 K	8,052 K	1876	igfxCUIService Module	Intel Corporation	<access denied>		
svchost.exe	0.02	2,864 K	9,584 K	2008	Host Process for Windows S...	Microsoft Corporation	<access denied>		
audiodg.exe	4.36	26,944 K	35,300 K	4288			<unable to open t...	64-bit	
RtkAudioService64.exe		1,680 K	7,292 K	1632	Realtek Audio Service	Realtek Semiconductor	<access denied>		
RAVBg64.exe		5,820 K	13,184 K	2192			<access denied>		
svchost.exe		3,340 K	11,476 K	2248	Host Process for Windows S...	Microsoft Corporation	<access denied>		
svchost.exe		4,008 K	12,776 K	2372	Host Process for Windows S...	Microsoft Corporation	<access denied>		
spoolsv.exe		5,896 K	14,460 K	2484	Spooler SubSystem App	Microsoft Corporation	<access denied>		
AdminService.exe		2,664 K	7,752 K	2724	Windows Setup API	Windows (R) Win 7 DDK p...	<access denied>		
IntelCpHDCPSvc.exe		1,424 K	7,072 K	2760	IntelCpHDCPSvc Executable	Intel Corporation	<access denied>		
svchost.exe		6,416 K	21,344 K	2780	Host Process for Windows S...	Microsoft Corporation	<access denied>		
esif_uf.exe		1,608 K	6,356 K	2812	Intel(R) Dynamic Platform a...	Intel Corporation	<access denied>		
esif_assist_64.exe	< 0.01	1,008 K	3,800 K	2148			DESKTOP-6FGL5...	64-bit Medium	
svchost.exe		7,292 K	19,776 K	2952	Host Process for Windows S...	Microsoft Corporation	<access denied>		
vmnat.exe	< 0.01	1,888 K	6,856 K	2960	VMware NAT Service	VMware, Inc.	<access denied>		
vmnetdhcp.exe		7,404 K	4,788 K	2968	VMware VMnet DHCP service	VMware, Inc.	<access denied>		
WavesSysSvc64.exe		5,908 K	11,872 K	2996	WavesSysSvc Service Appli...	Waves Audio Ltd.	<access denied>		
vmware-authd.exe	0.08	4,204 K	11,436 K	3032	VMware Authorization Service	VMware, Inc.	<access denied>		
vmware-vmx.exe	0.29	536,520 K	2,541,480 K	5496	VMware Workstation VMX	VMware, Inc.	DESKTOP-6FGL5...	64-bit Medium	
vmware-usbarbitrator64.exe	< 0.01	2,408 K	9,984 K	3040	VMware USB Arbitration Ser...	VMware, Inc.	<access denied>		
MsMpEng.exe	0.04	121,532 K	120,292 K	3064	Antimalware Service Execut...	Microsoft Corporation	<access denied>		
IntelCpHeciSvc.exe		1,964 K	7,604 K	3112	IntelCpHeciSvc Executable	Intel Corporation	<access denied>		
vmware-hostd.exe	< 0.01	27,568 K	47,228 K	3560			<access denied>		
svchost.exe		1,592 K	6,760 K	3608	Host Process for Windows S...	Microsoft Corporation	<access denied>		
NisSrv.exe		15,188 K	7,828 K	3968	Microsoft Network Realtime ...	Microsoft Corporation	<access denied>		
SearchIndexer.exe		26,768 K	23,784 K	880	Microsoft Windows Search I...	Microsoft Corporation	<access denied>		
svchost.exe		4,084 K	18,724 K	1768	Host Process for Windows S...	Microsoft Corporation	DESKTOP-6FGL5...	64-bit Medium	

CPU Usage: 7.35% Commit Charge: 30.64% Processes: 77 Physical Usage: 32.67%



Ask me anything



3:08 PM
3/22/2017

Browser to VMware Escape

Edge VM - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

My Computer

Windows

Flash VM

VMware

Edge VM

Firefox V

Adobe R

Windows

Ubuntu V

Shared VMs

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-6FGL507\ZDI]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	User Name	Image Type	Integrity
vmnetdhcp.exe		7,476 K	4,852 K	2968	VMware VMnet DHCP service	VMware, Inc.	<access denied>		
WavesSysSvc64.exe		5,908 K	11,872 K	2996	WavesSysSvc Service Appli...	Waves Audio Ltd.	<access denied>		
vmware-authd.exe		4,036 K	11,464 K	3032	VMware Authorization Service	VMware, Inc.	<access denied>		
vmware-vmx.exe	0.41	460,664 K	3,048,516 K	4640	VMware Workstation VMX	VMware, Inc.	DESKTOP-6FGL5...	64-bit Medium	
vmware-usbarbitrator64.exe	< 0.01	2,392 K	10,000 K	3040	VMware USB Arbitration Ser...	VMware, Inc.	<access denied>		
MsMpEng.exe	0.05	122,052 K	103,644 K	3064	Antimalware Service Execut...	Microsoft Corporation	<access denied>		
IntelCpHeciSvc.exe		1,908 K	7,712 K	3112	IntelCpHeciSvc Executable	Intel Corporation	<access denied>		
vmware-hostd.exe	< 0.01	27,356 K	47,460 K	3560			<access denied>		
svchost.exe		1,624 K	6,828 K	3608	Host Process for Windows S...	Microsoft Corporation	<access denied>		
NisSrv.exe		8,088 K	200 K	3968	Microsoft Network Realtime ...	Microsoft Corporation	<access denied>		
SearchIndexer.exe	0.01	28,984 K	26,956 K	880	Microsoft Windows Search I...	Microsoft Corporation	<access denied>		
svchost.exe		3,908 K	18,796 K	1768	Host Process for Windows S...	Microsoft Corporation	DESKTOP-6FGL5...	64-bit Medium	
lsass.exe	< 0.01	4,080 K	12,728 K	756	Local Security Authority Pro...	Microsoft Corporation	<access denied>		
csrss.exe	0.05	2,736 K	7,512 K	684			<access denied>		
winlogon.exe		2,060 K	11,168 K	920			<access denied>		
dwm.exe	0.83	274,776 K	325,756 K	424			<access denied>		
igfxEM.exe		3,672 K	12,968 K	3096	igfxEM Module	Intel Corporation	DESKTOP-6FGL5...	64-bit Medium	
explorer.exe	0.25	47,692 K	105,676 K	2140	Windows Explorer	Microsoft Corporation	DESKTOP-6FGL5...	64-bit Medium	
MSASCuiL.exe		2,960 K	13,076 K	5168	Windows Defender notificati...	Microsoft Corporation	DESKTOP-6FGL5...	64-bit Medium	
RtkNGUI64.exe		4,440 K	12,720 K	5232	Realtek HD Audio Manager	Realtek Semiconductor	DESKTOP-6FGL5...	64-bit Medium	
RAVBg64.exe		5,848 K	13,788 K	5256	HD Audio Background Proce...	Realtek Semiconductor	DESKTOP-6FGL5...	64-bit Medium	
WavesSvc64.exe	0.06	13,644 K	21,992 K	5332	Waves MaxxAudio Service A...	Waves Audio Ltd.	DESKTOP-6FGL5...	64-bit Medium	
OneDrive.exe		7,176 K	28,448 K	5768	Microsoft OneDrive	Microsoft Corporation	DESKTOP-6FGL5...	32-bit Medium	
procexp.exe		2,764 K	9,656 K	5880	Sysinternals Process Explorer	Sysinternals - www.sysint...	DESKTOP-6FGL5...	32-bit Medium	
procexp64.exe	0.45	20,012 K	35,020 K	3516	Sysinternals Process Explorer	Sysinternals - www.sysint...	DESKTOP-6FGL5...	64-bit Medium	
vmware.exe	0.01	62,364 K	98,356 K	4968	VMware Workstation	VMware, Inc.	DESKTOP-6FGL5...	32-bit Medium	
vmware-unity-helper.exe	< 0.01	5,456 K	18,092 K	2384	VMware Unity Helper	VMware, Inc.	DESKTOP-6FGL5...	32-bit Medium	
vmware-tray.exe	< 0.01	1,608 K	8,324 K	5900	VMware Tray Process	VMware, Inc.	DESKTOP-6FGL5...	32-bit Medium	
CamRecorder.exe	10.22	873,944 K	784,296 K	600			DESKTOP-6FGL5...	64-bit High	

CPU Usage: 17.68% Commit Charge: 34.26% Processes: 80 Physical Usage: 40.75%

To direct input to this VM, click inside or press Ctrl+G.

Ask me anything

3:49 PM 3/22/2017

Apple iPhone Rogue Application



Pwn2Own Inspired Improvements



Challenges with Adapting “Assume Breach”

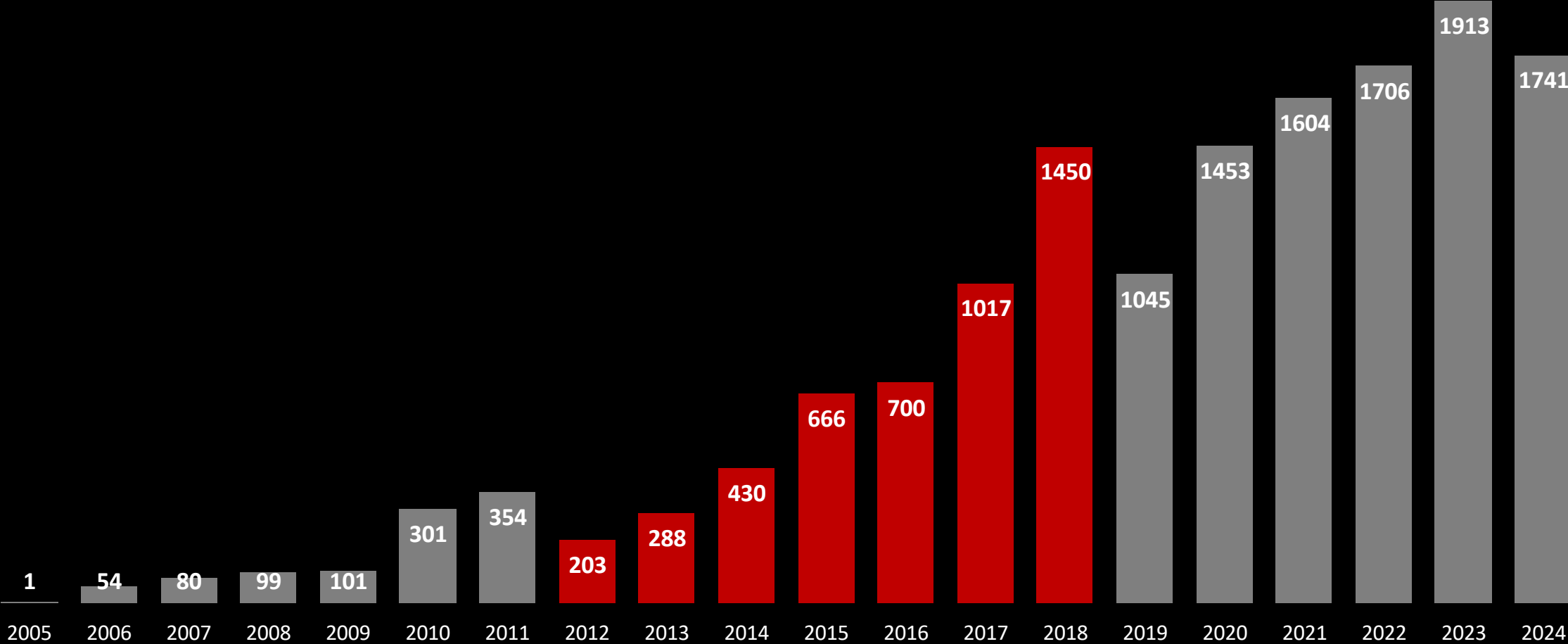
- Mitigations are primarily reactive if driven by ITW data
- Reactive mitigations take time to develop
- New products do not get appropriate mitigations – until they are attacked
- We do not get accurate metrics on exploit and attack development

PWN2OWN & Data Influenced Mitigations

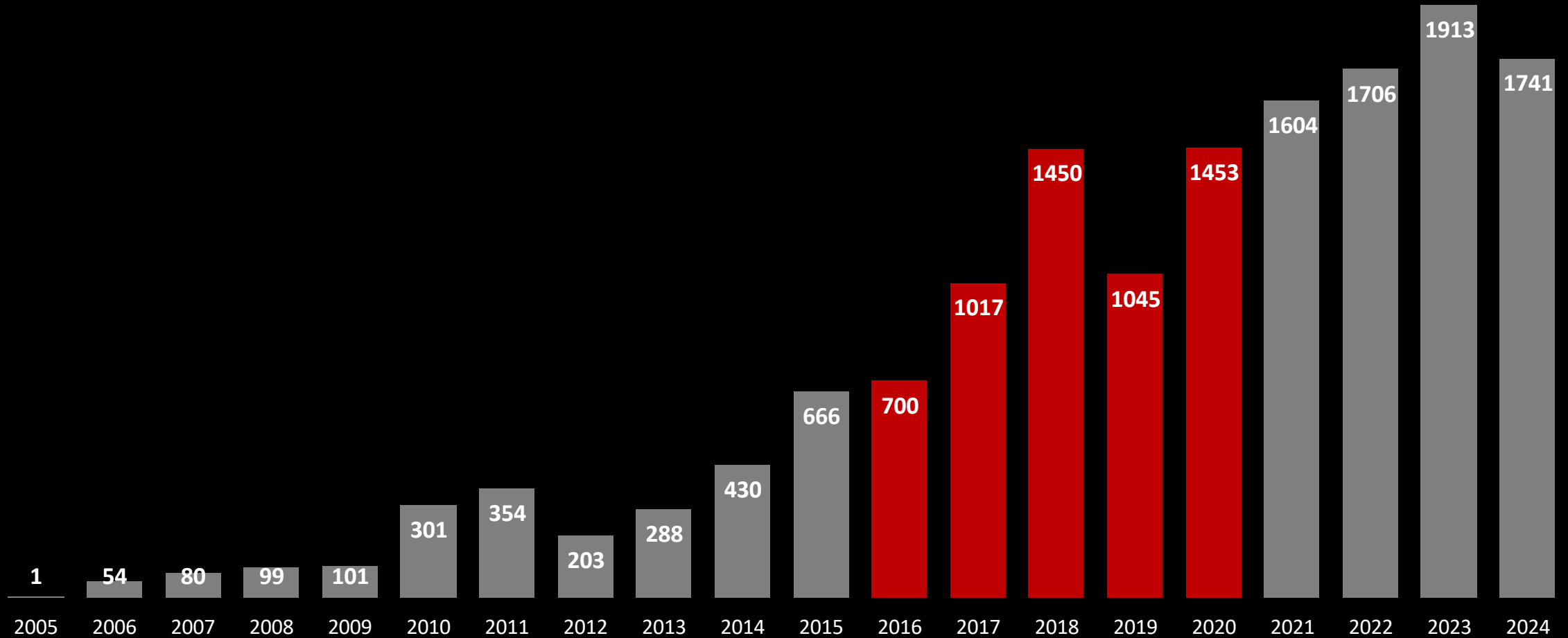
CFG: suppress sensitive APIs
Flash: Eliminate RWX ATL thunks
Junctions: Prevent sandbox processes from creating NTFS junctions – TH1
Fonts: Move font parsing to user mode sandbox
Edge: Prevent content processes from creating child processes
Edge: Enable win32k system call restrictions

How do we design effective mitigations proactively?

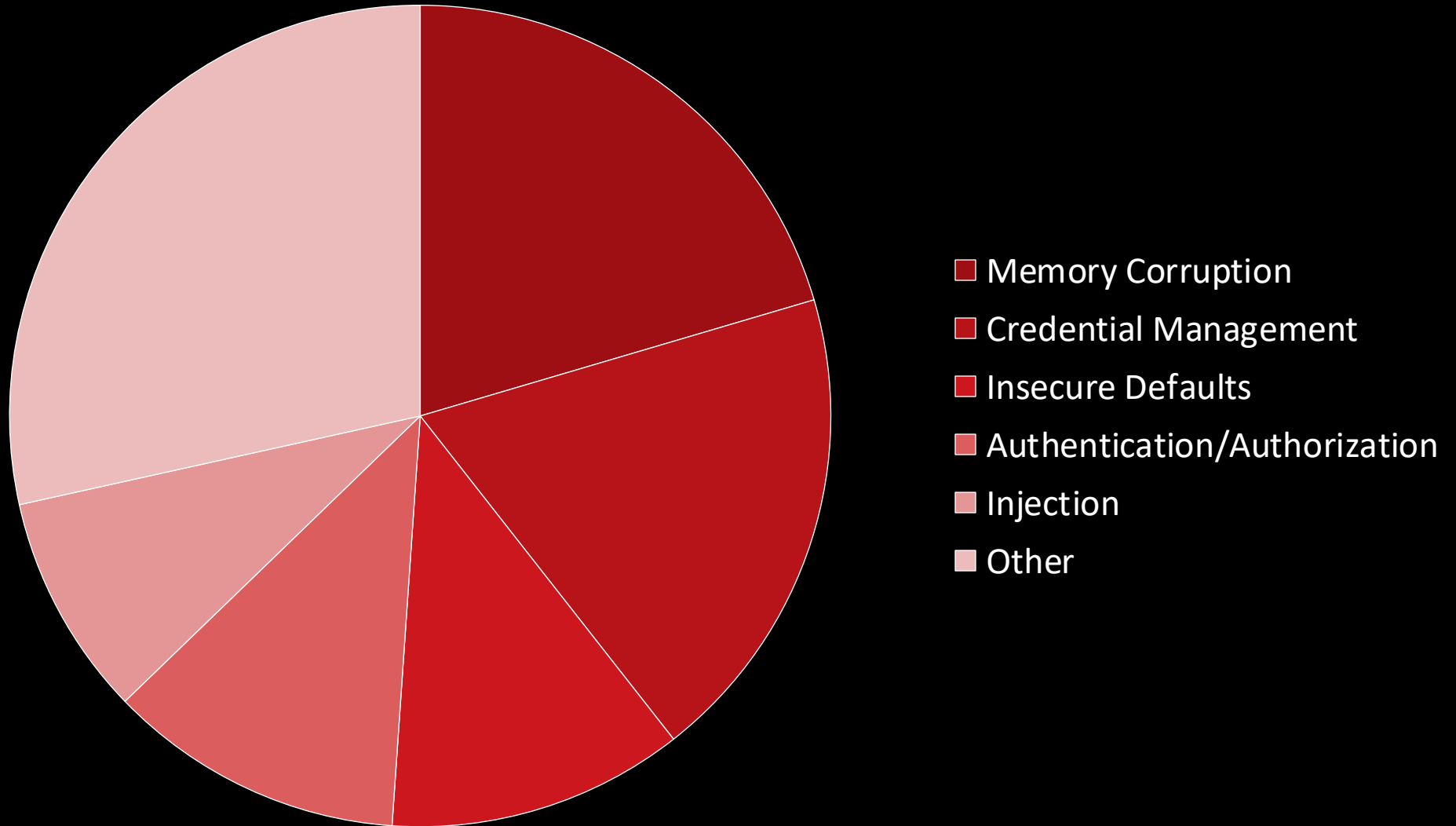
Transformational Years



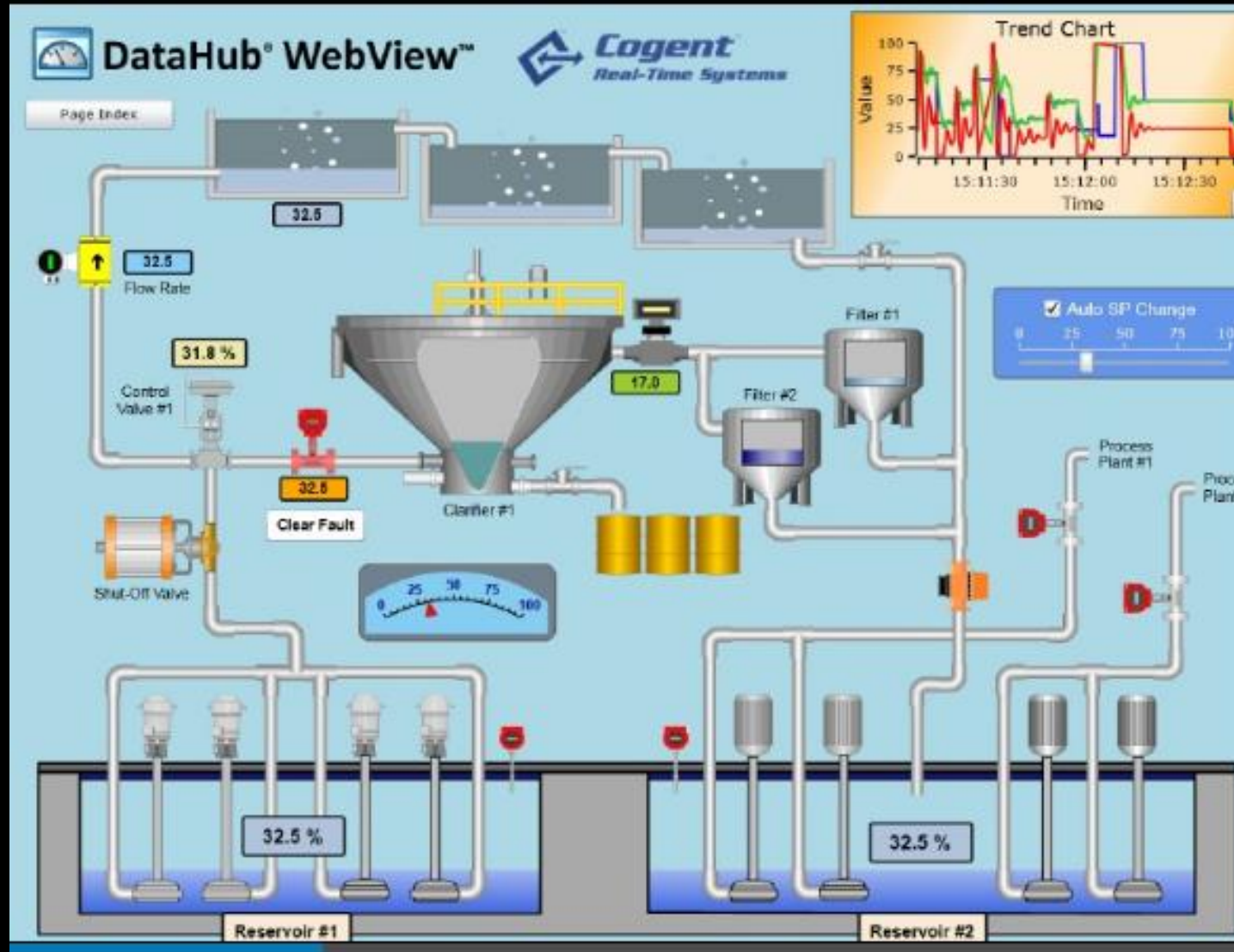
ICS/SCADA Year



Common Problems



Cogent DataHub Overview



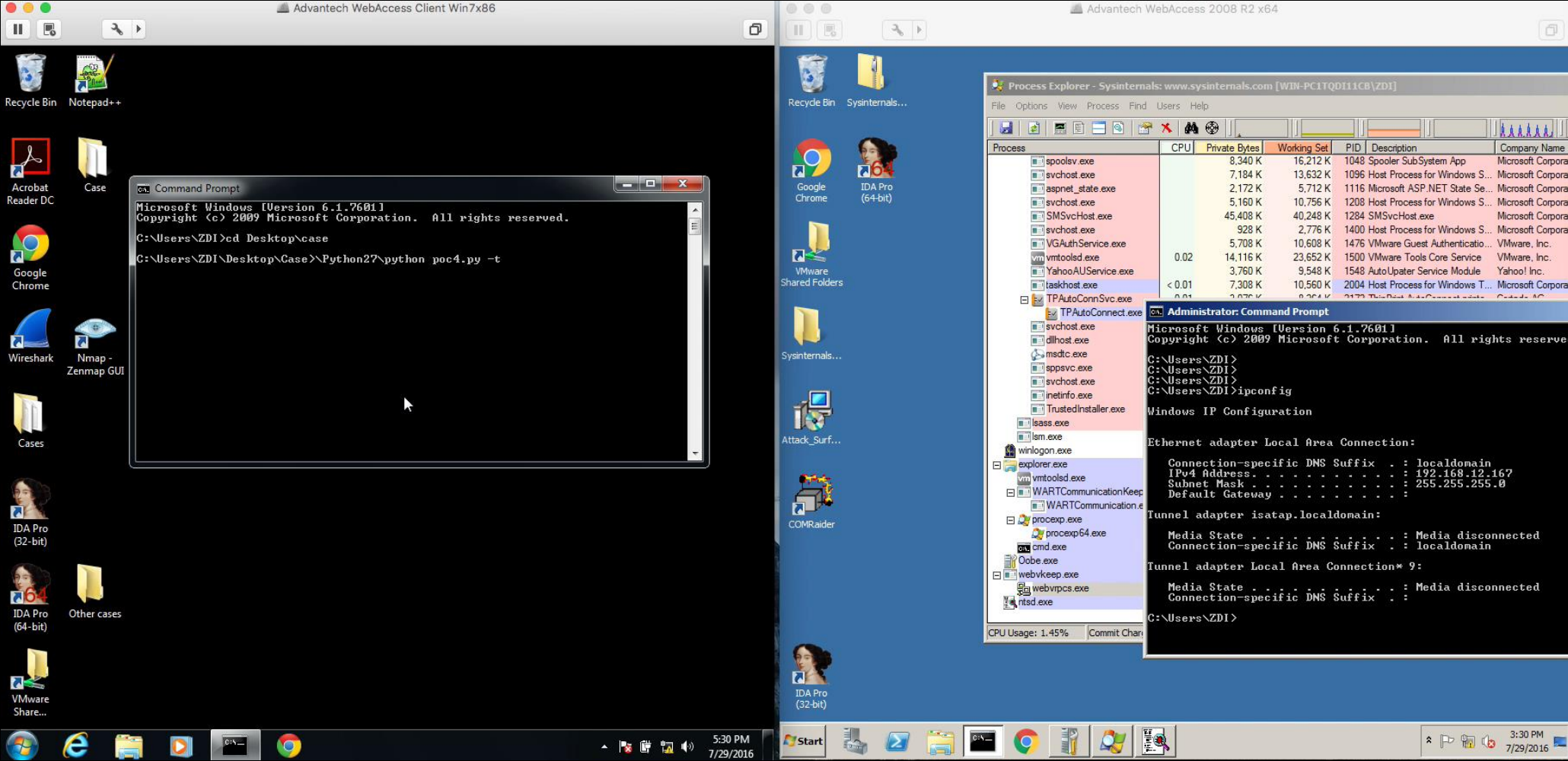
Cogent DataHub Remote Code Execution

The screenshot displays a Windows desktop environment with a blue background. On the left sidebar, icons for Recycle Bin, VMware Share..., procepx, Cogent DataHub, DataSim, and DataPid are visible. The main area features a web browser window titled "DataHub Web Server" at the URL "http://localhost/demo.asp". The page content includes a message: "You have successfully configured the DataHub to run as a web server... capabilities of the DataHub's Java, AJAX and ASP web support. For more information, visit the DataHub WebView here." Below this, a red banner reads "Please start the DataPid process" with a "Start DataPid Now" button. The page is divided into "Web Server Demo Pages" and "AJAX" sections, each with a list of examples.

Overlaid on the desktop is the "Process Explorer" window from Sysinternals. It shows a list of running processes with columns for Process, CPU, Private Bytes, Working Set, PID, Description, and Company Name. The "CogentDataHubV7.exe" process is highlighted in blue, showing a CPU usage of 2.50%, 28,956 K private bytes, and 36,328 K working set. Other processes like "explorer.exe" and "iexplore.exe" are also visible.

A terminal window titled "ZDI-CAN-2981 - bash - 77x20" is open in the foreground, showing a command prompt with the text "mishap:ZDI-CAN-2981 mishap\$".

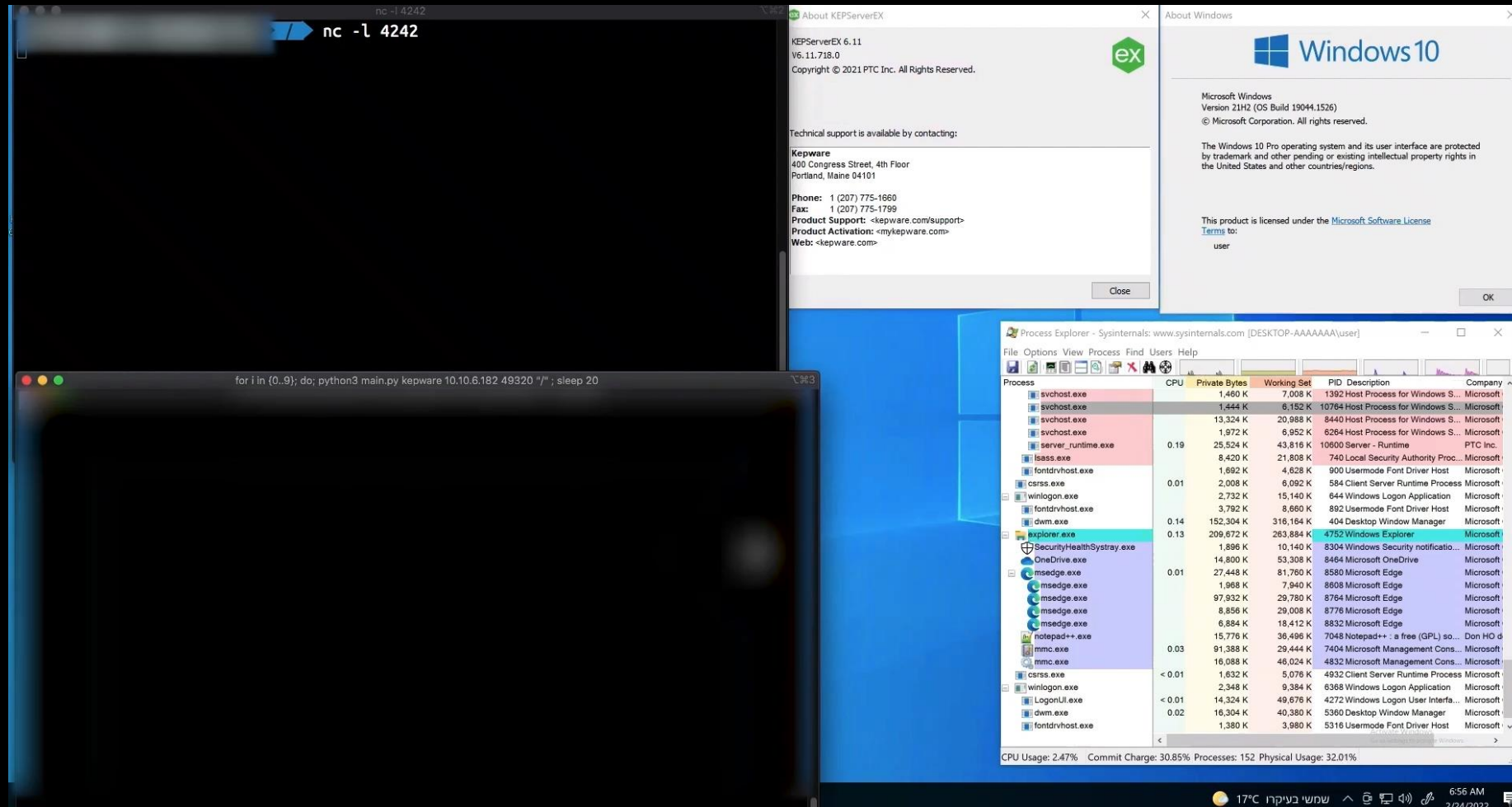
Advantech WebAccess

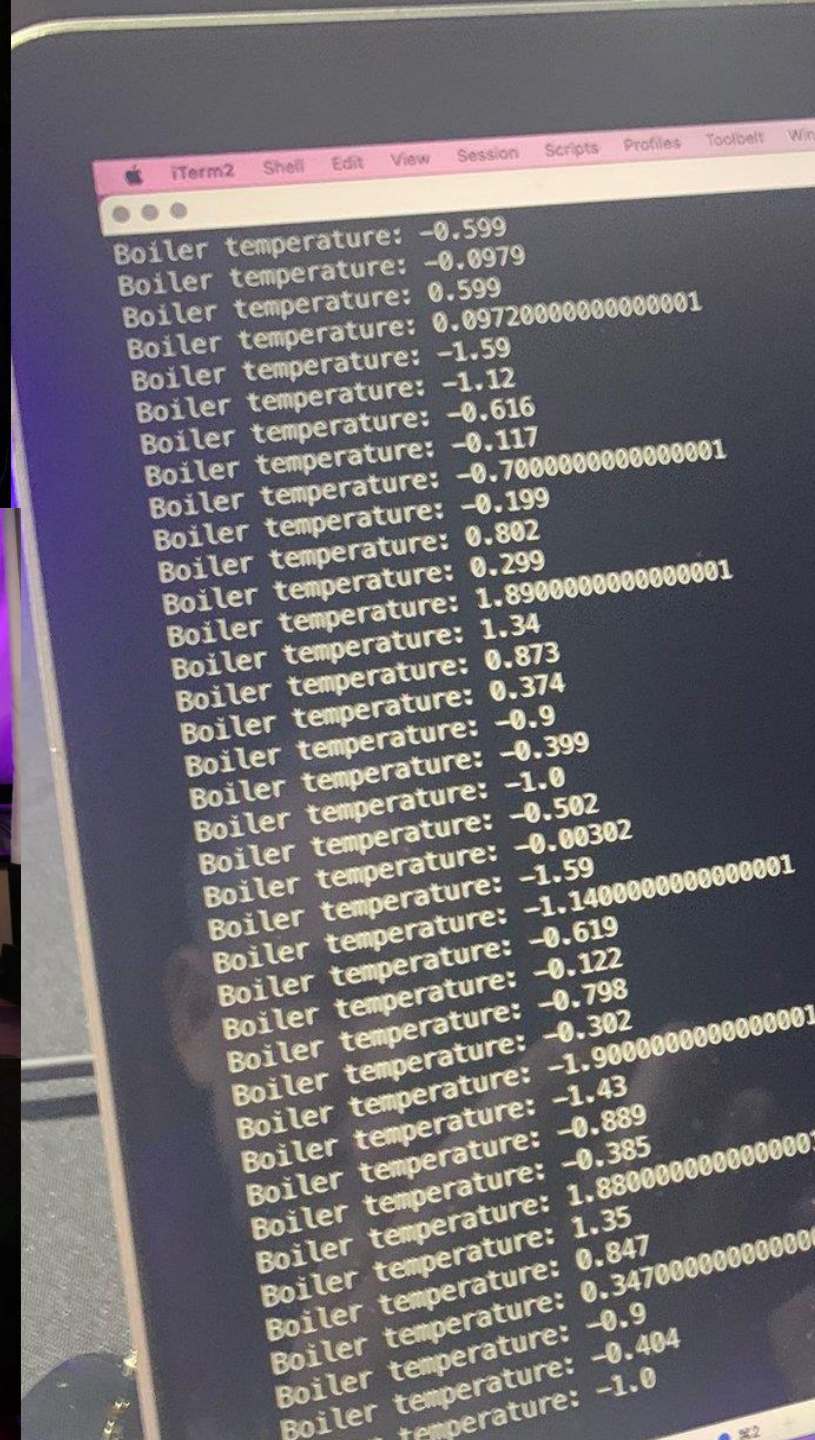
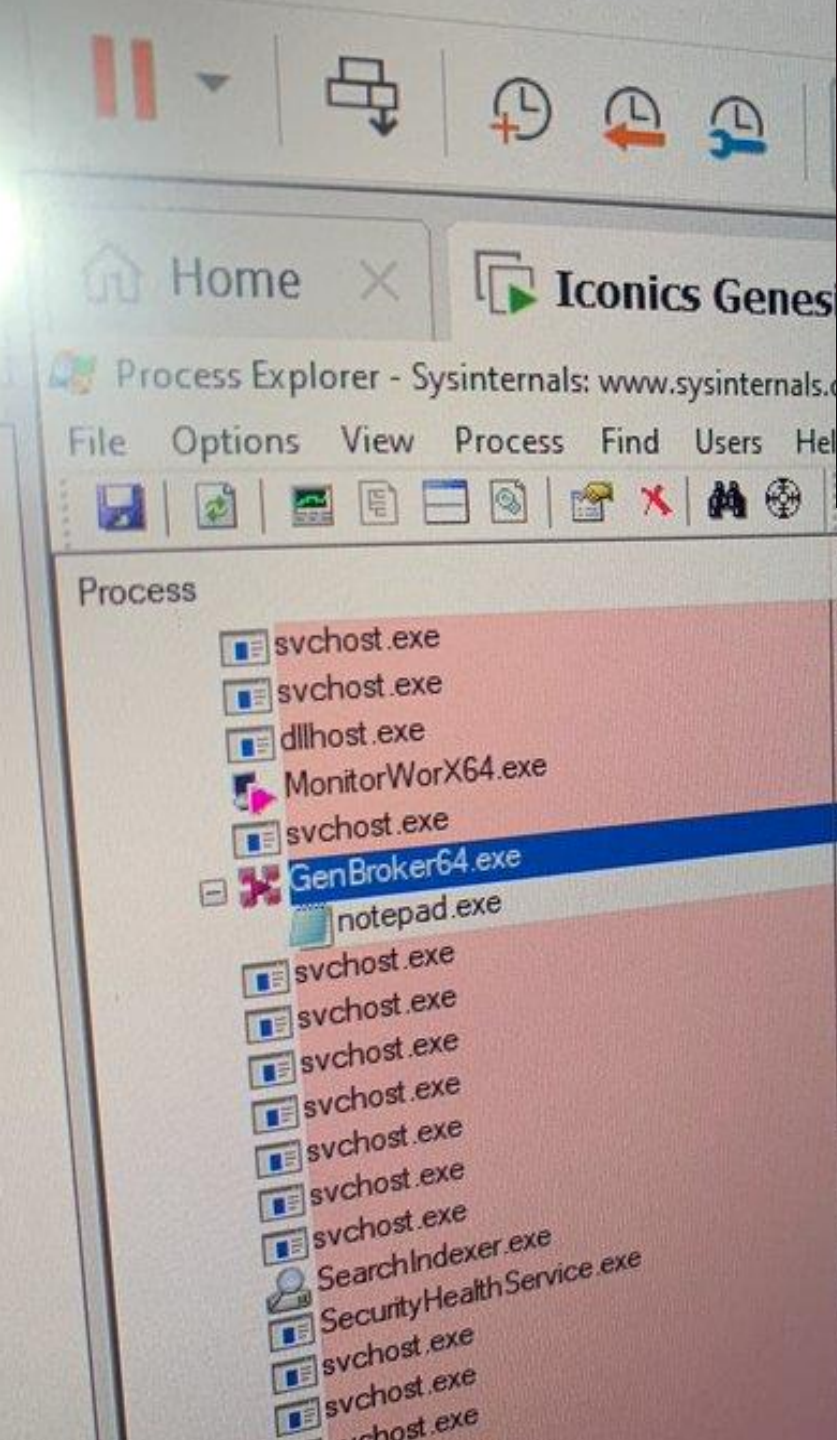




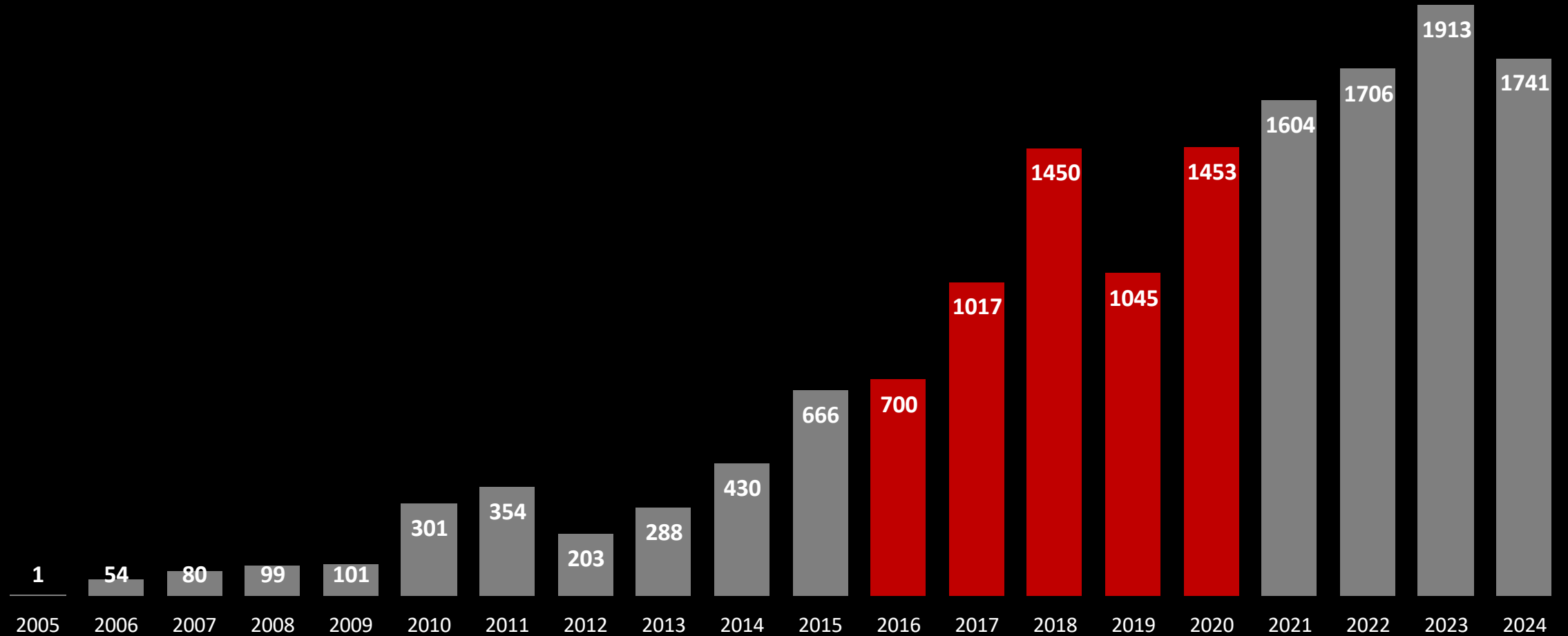
Pwn2Own
Miami

Kepware KEPServerEx

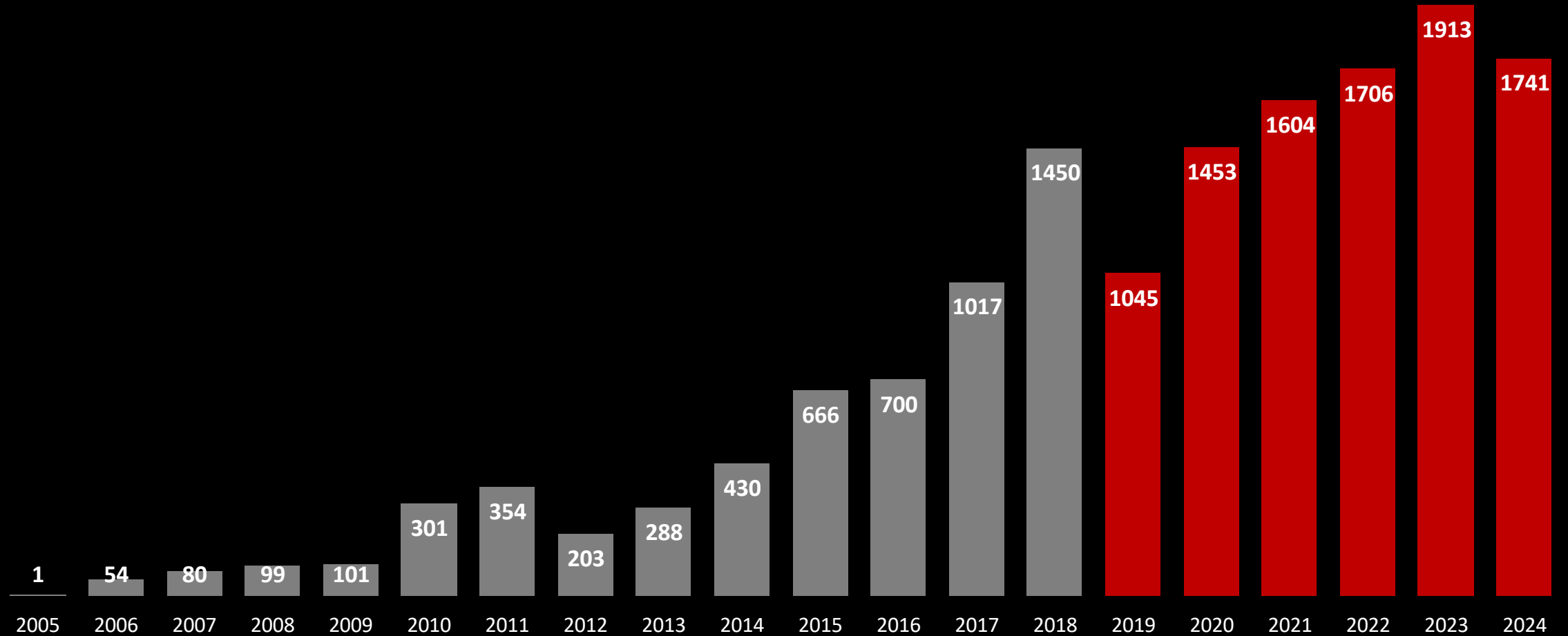




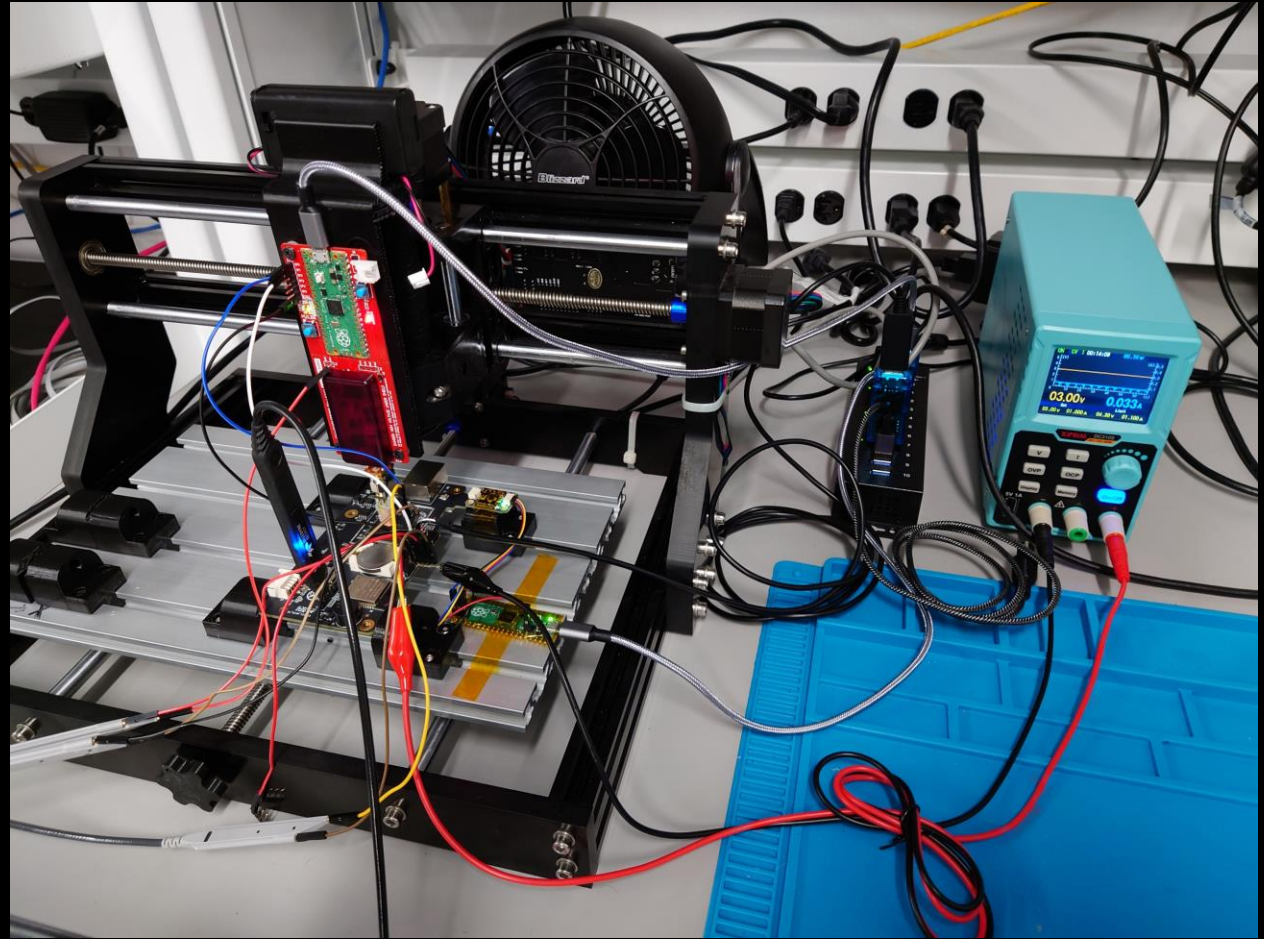
ICS/SCADA Years



IoT/Embedded Years



Glitching





四、五、六

<https://www.ui.com/>

Welcome to UVC AI Pro! (v5.1.97.67.19d7cd1.250917.0517)

```
I Pro 6-5.1.97# id
uid=0(ui) gid=0(admin)
I Pro 6-5.1.97#
```

```

QWAP_netpoeskr.cgi
RSS
a
ajax_obj
apps
cgi-bin
cgi.conf
cgi_load.html
clearauthcache.html
diag_blkdevMonitor.cgi
errors
flower.jpg
help
images
index.html
indexnas.cgi
jc
libs
logoot.html
redirect.html
robots.txt
sh.cgi
share.cgi
share.html
sharelink
share_file.html
share_folder.html
share_video.html
tools.js
v3_menu
wsd
sh-3.2#

```

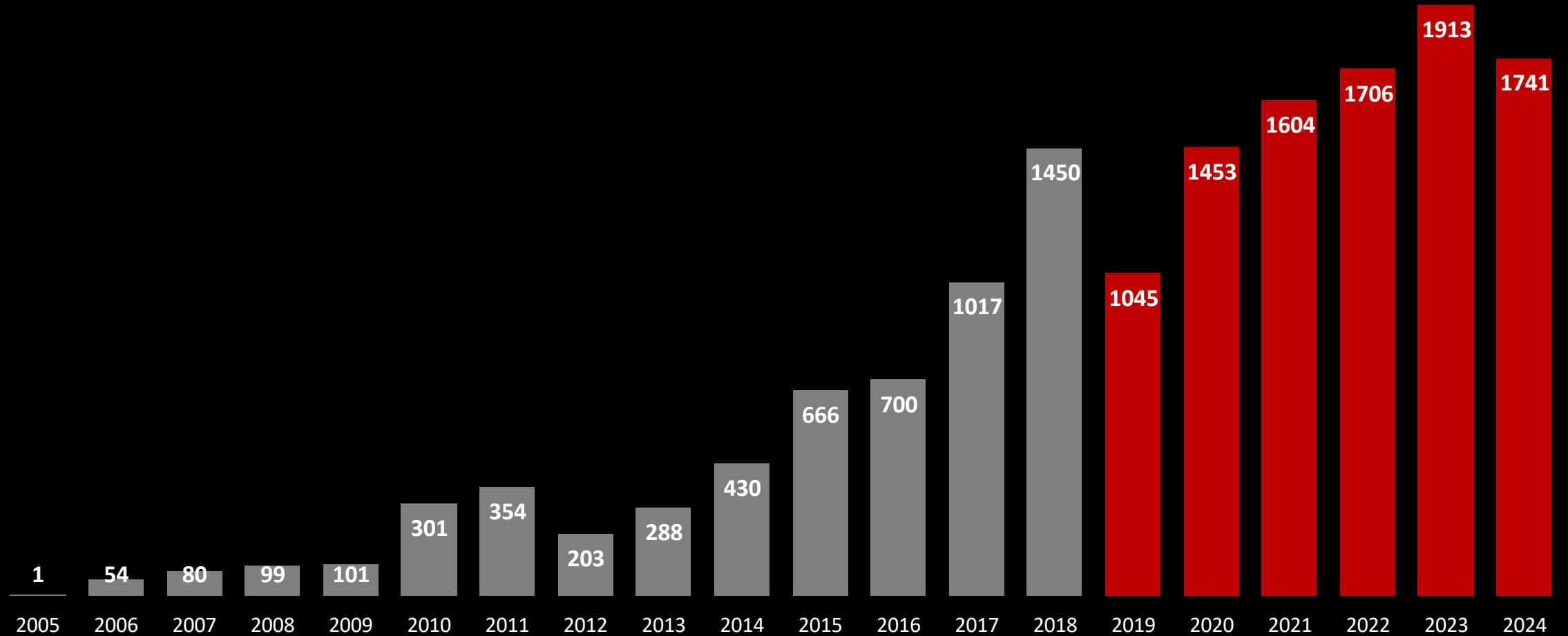
@ 13 0:~* 28m 0.49 3.2GHz 929M28% 29G58% 2025-10-22 18:0



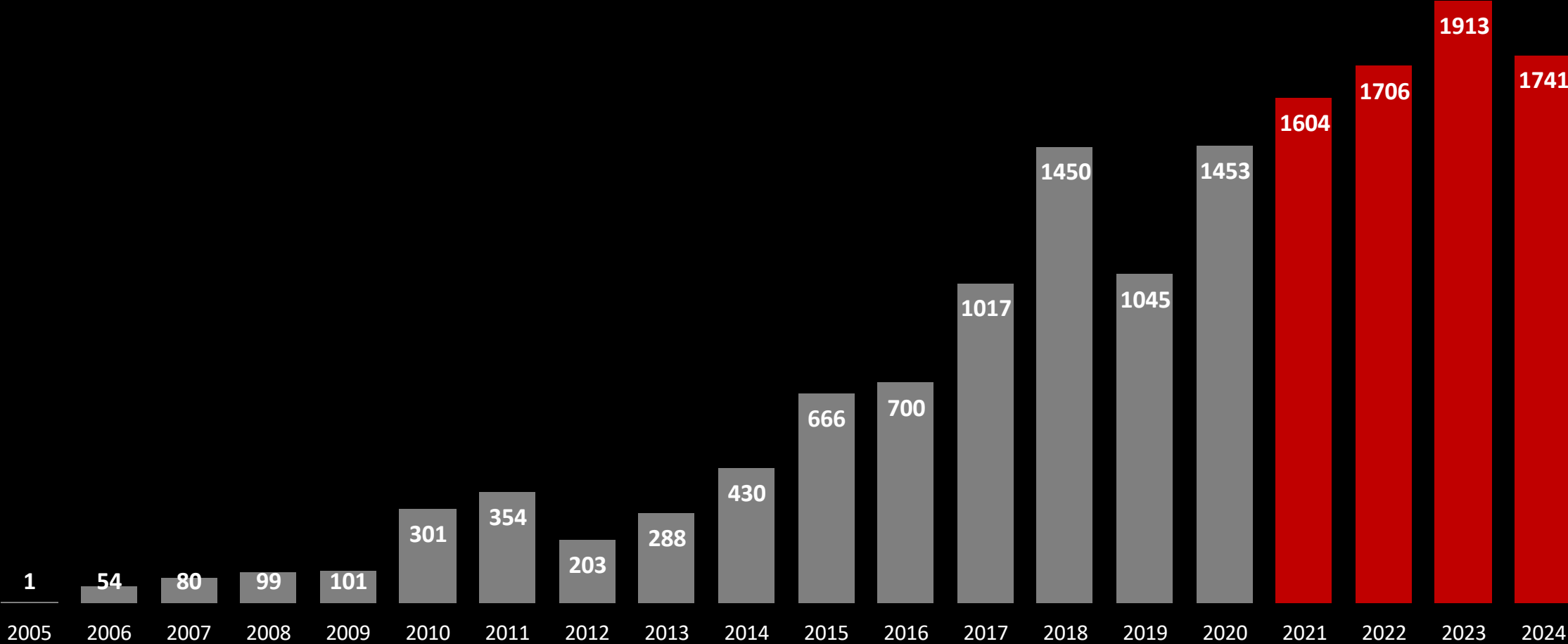
Observation



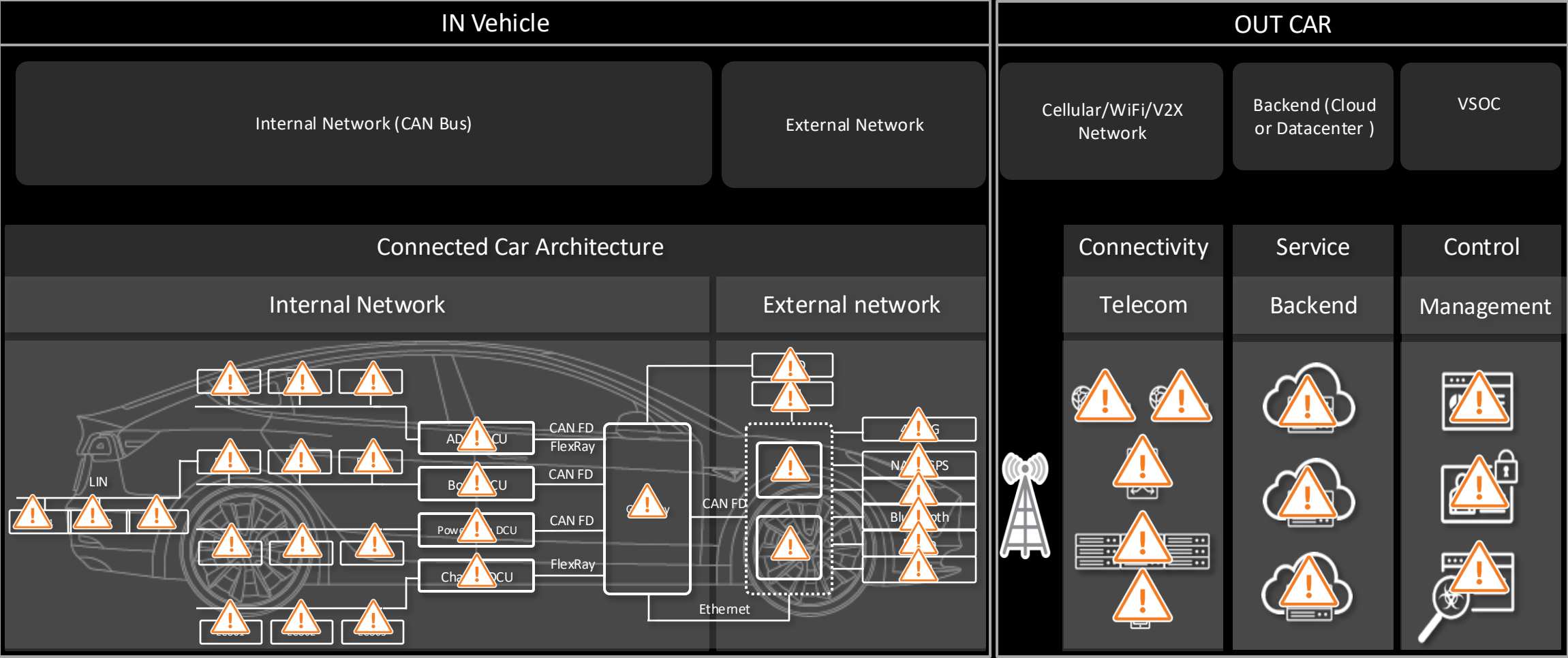
IoT/Embedded Years



Automotive Years



Automotive Attack Surface

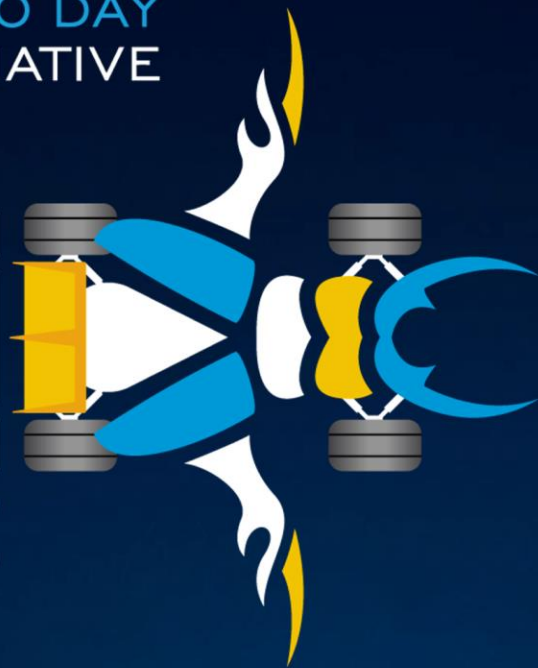




ZERO DAY
INITIATIVE

PWN2017

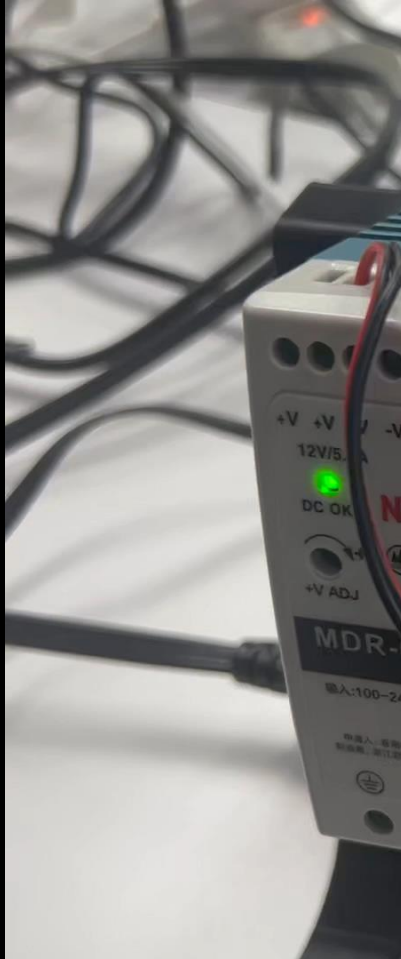
AUTOMOTIVE



In-Vehicle Infotainment



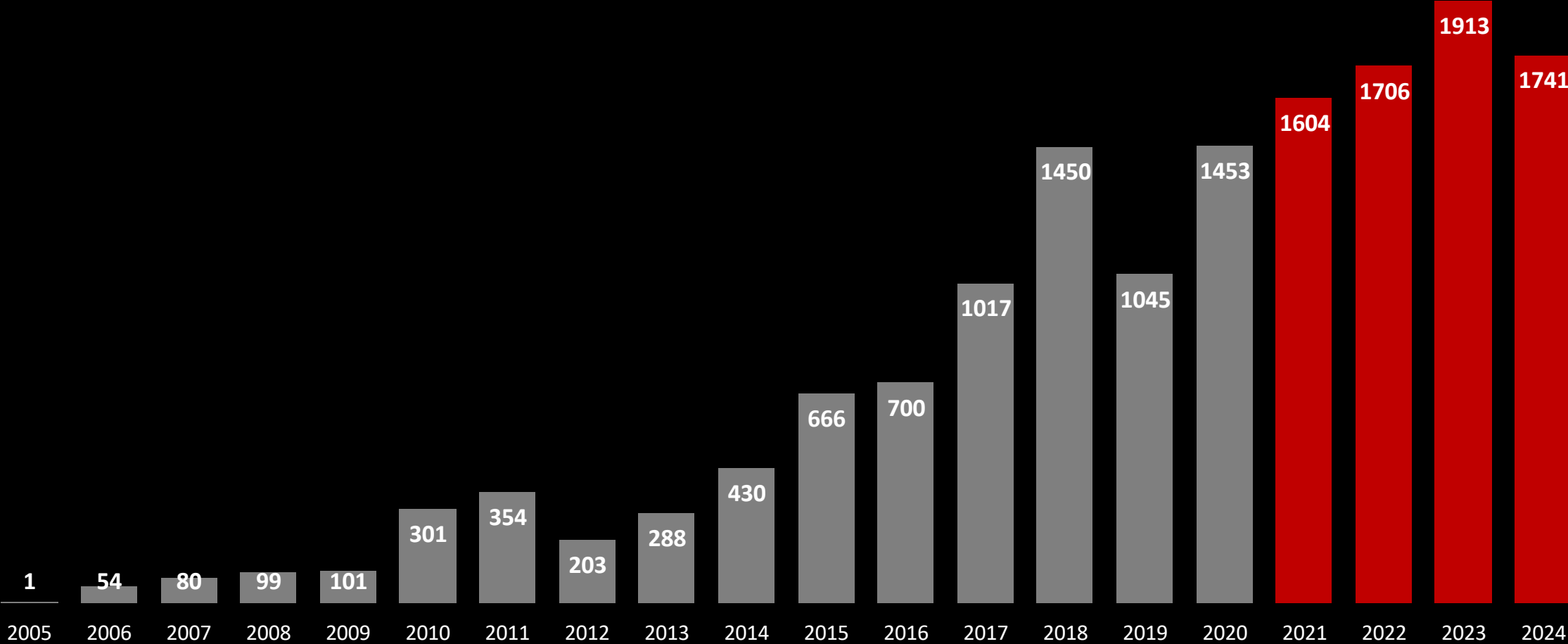
EV Chargers



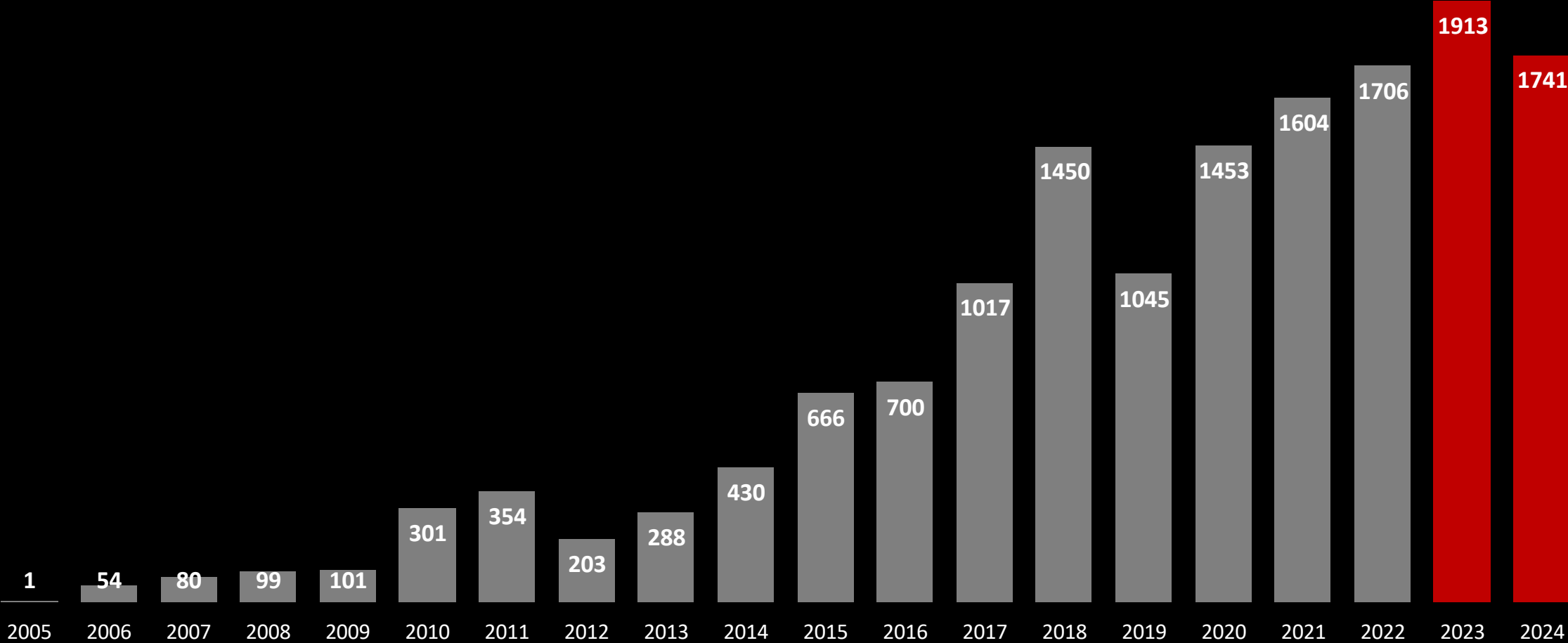
Tesla Model 3



Automotive Years



AI Years



Increasing Interest

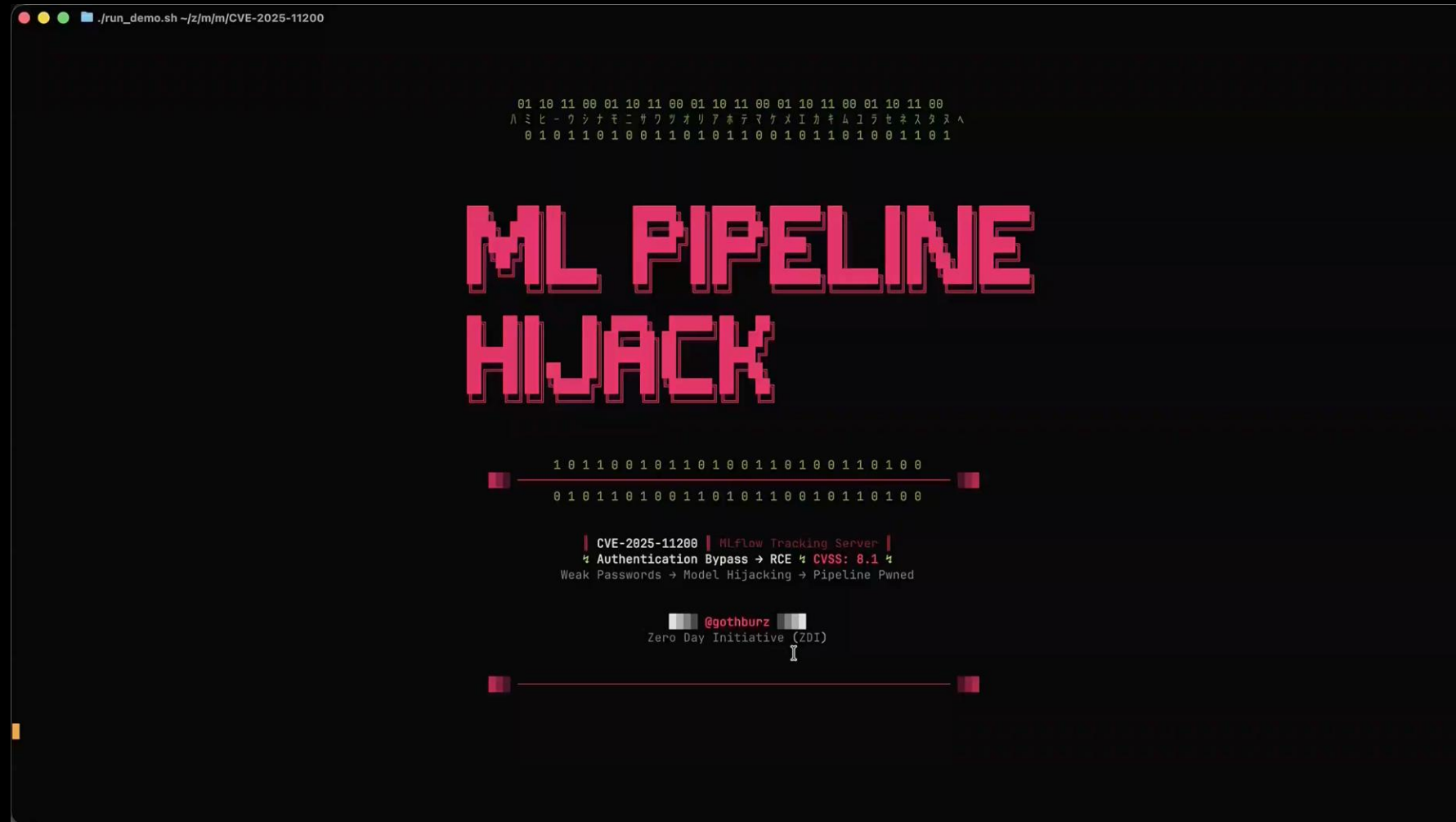
- 100+ AI related vulnerabilities going through disclosure process
- Most of the flaws are in MCP implementations
- Rest in ML Frameworks, Agentic AI Frameworks, and AI tool chains such as AI workflow orchestrators
- Top Bug Classes
 - Deserialization of Untrusted Data
 - OS Command Injection



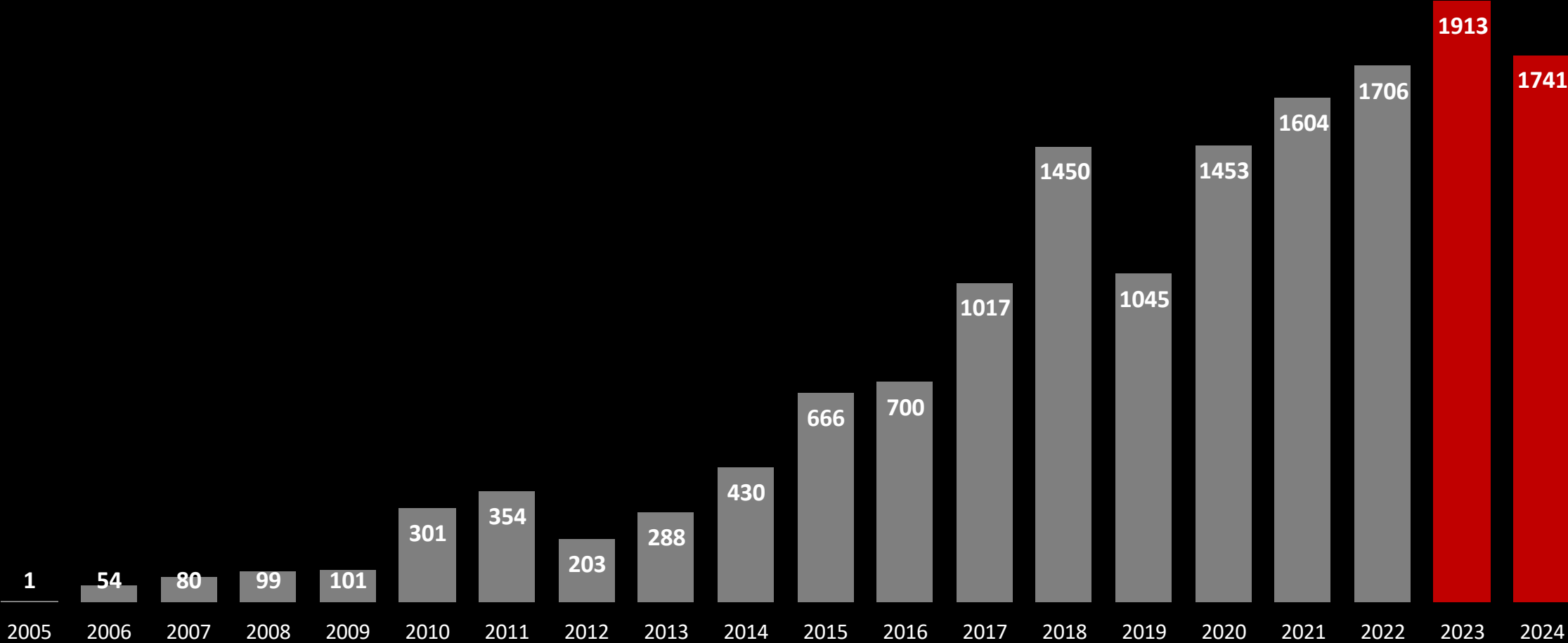
NVIDIA Isaac GROOT



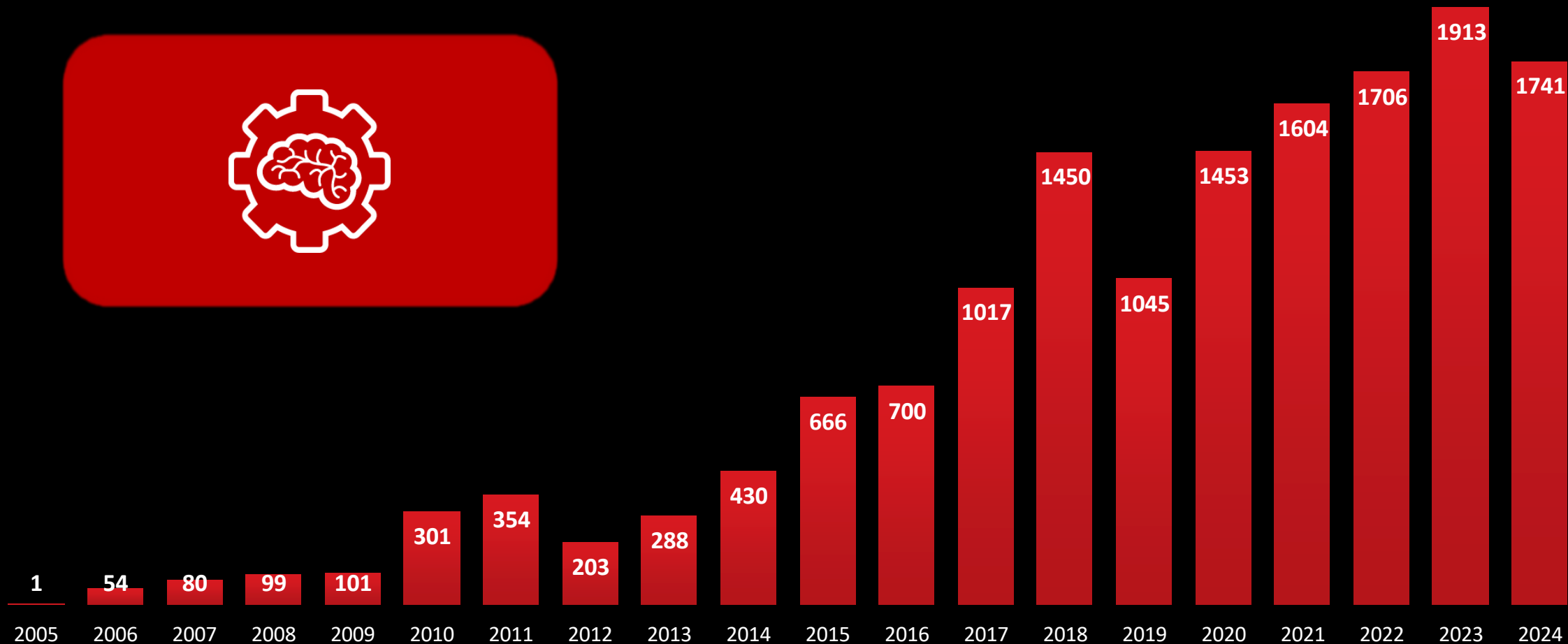
MLflow Remote Code Execution



AI Years



Insights



Future of Vulnerability Discovery



AARDVARK — Vulnerability Discovery Agent Workflow

