CYBERCORE integration center

ICS 0Day Market Analysis:
An Emerging Market

Sarah Freeman

Idaho National Laboratory

Idaho National Laboratory

"There are known knowns"

There are known knowns; there are things we know we know.

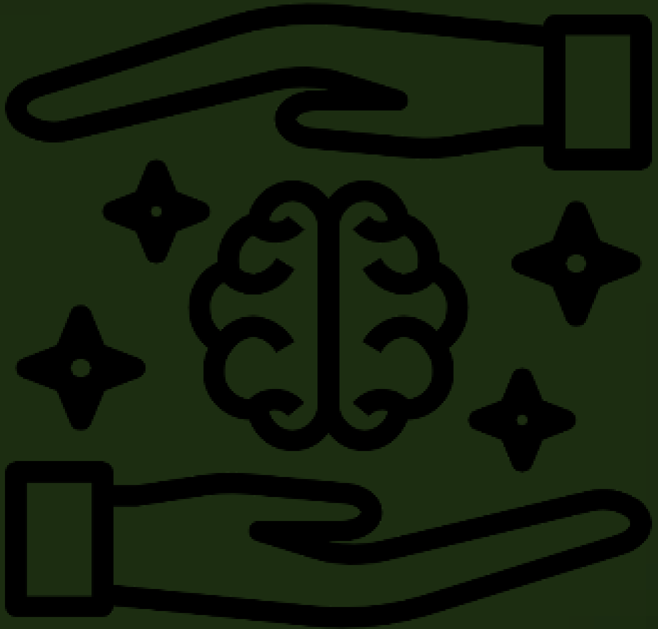
We also know there are known unknowns; that is to say we know there are some things we do not know.

But there are also unknown unknowns—the ones we don't know we don't know.

--- Donald Henry Rumsfeld, 2002 ---

Hypothesis

The 0day market space, and the associated public bug bounties, can be used as tripwires for future adversary activities and targeting.

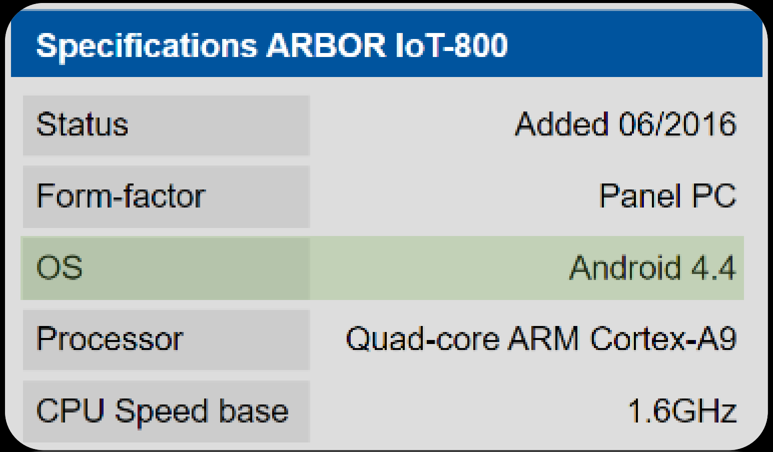


How are Bug Bounties Categorized?

Consider the sale of a vulnerability for an ARBOR IoT-800 HMI…

ARBOR IoT-800

How are Bug Bounties Categorized?

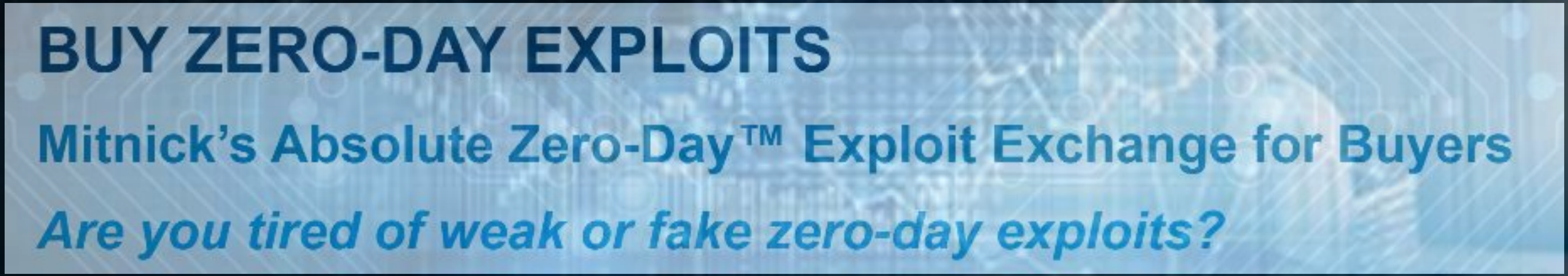


Specifications ARBOR IoT-800	
Status	Added 06/2016
Form-factor	Panel PC
OS	Android 4.4
Processor	Quad-core ARM Cortex-A9
CPU Speed base	1.6GHz

ARBOR IoT-800

Compact, versatile panel PC for visualizing, and responding to, what the Internet of Things (or any other system) is doing

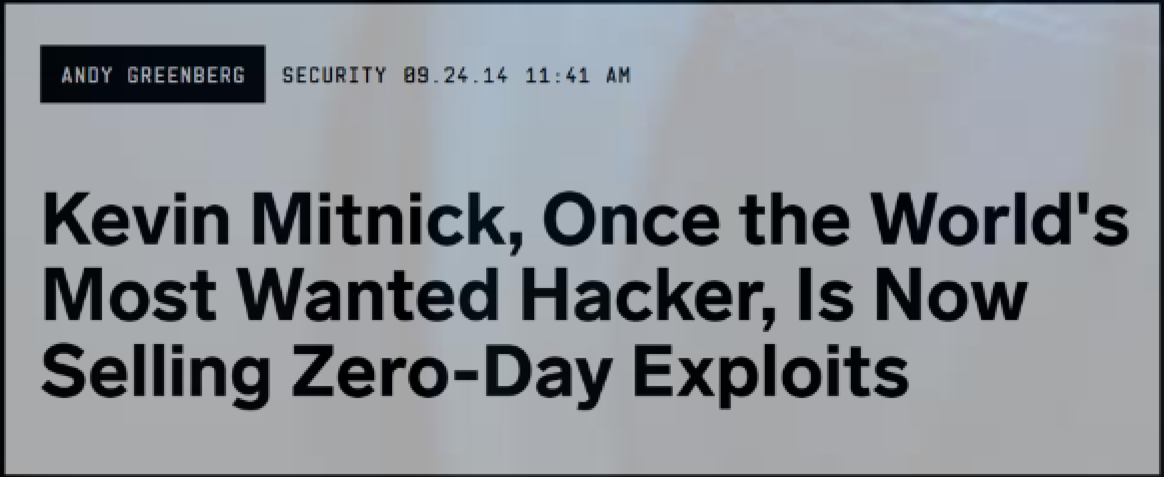
September 2014 - Absolute Zero-Day Established



BUY ZERO-DAY EXPLOITS

Mitnick's Absolute Zero-Day™ Exploit Exchange for Buyers

Are you tired of weak or fake zero-day exploits?



ANDY GREENBERG SECURITY 09.24.14 11:41 AM

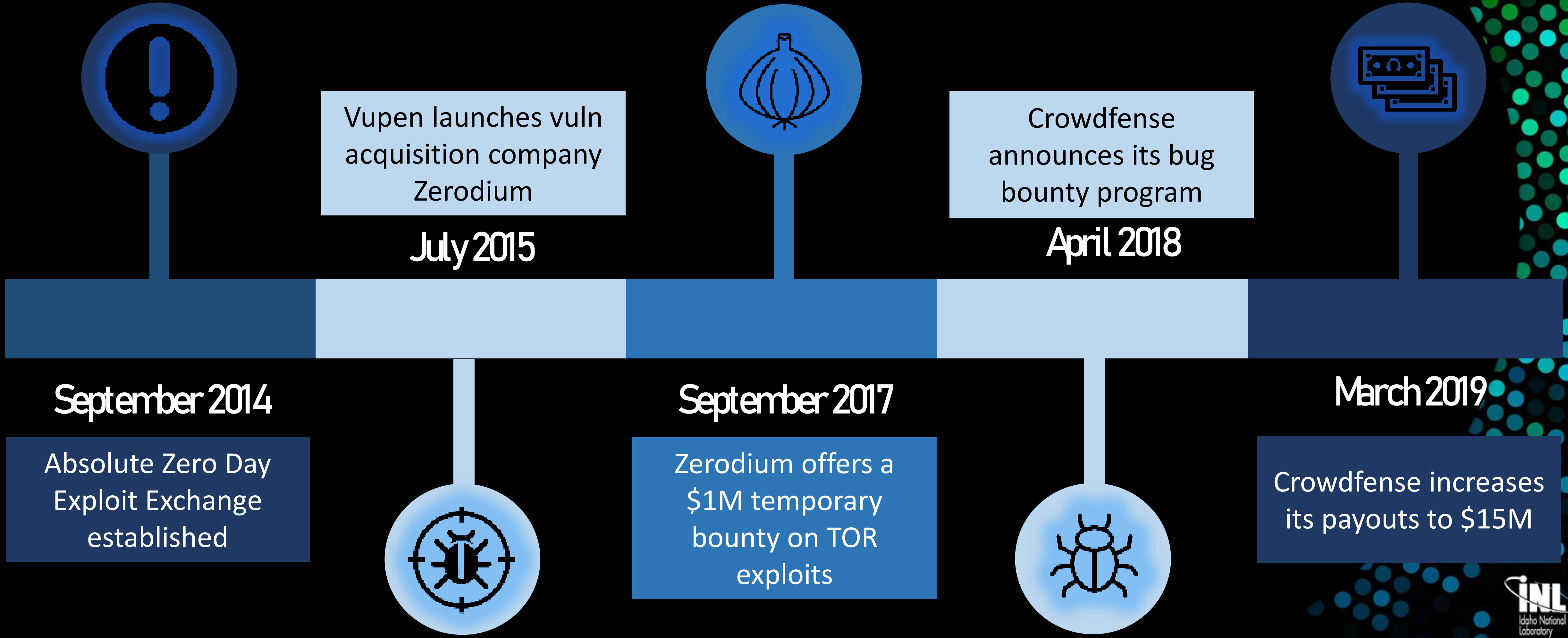
Kevin Mitnick, Once the World's Most Wanted Hacker, Is Now Selling Zero-Day Exploits

Zerodium - Established July 2015

VUPEN Founder Launches New Zero-Day Acquisition Firm Zerodium

"ZERODIUM does not acquire theoretically exploitable or non-exploitable vulnerabilities. We only acquire zero-day vulnerabilities with a fully functional exploit whether including only one stage or multiple stages…"

Continual Market Growth



September 2014

Absolute Zero Day Exploit Exchange established

July 2015

Vupen launches vuln acquisition company Zerodium

September 2017

Zerodium offers a $1M temporary bounty on TOR exploits

April 2018

Crowdfense announces its bug bounty program

March 2019

Crowdfense increases its payouts to $15M

Bug Bounty Landscape

]HackingTeam[

EXODUS INTELLIGENCE

VUPEN security

zerODIUM

CROWDFENSE
VULNERABILITY RESEARCH HUB

[Re]Vuln

Pwn2Own

ZERO DAY INITIATIVE

Zer0Fest

Q-recon

Hack2Win

PWNbRAMA

hackerone

NETRAGARD™
We protect you from people like us™

packet storm

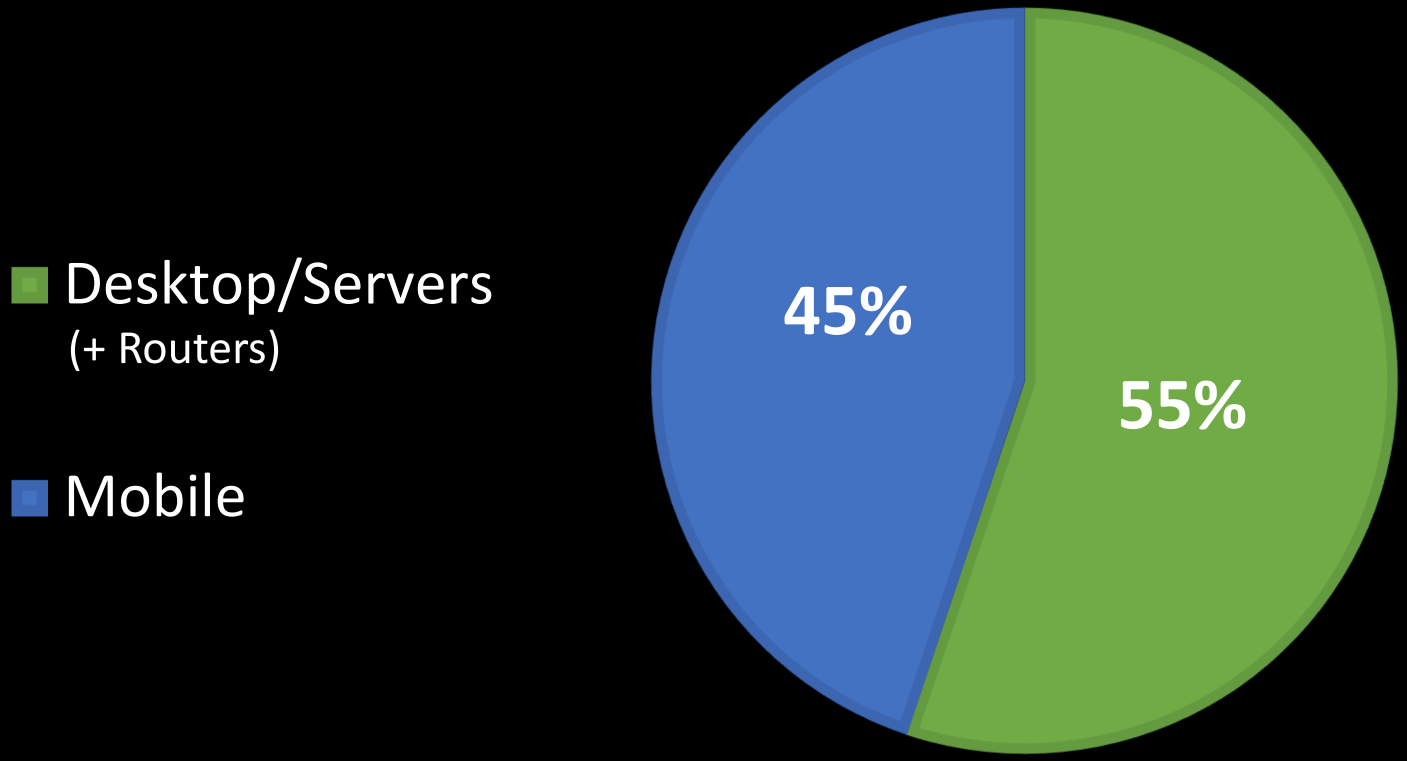
Variation in the Marketplace

- Not all purchases/bounties are created equal
- Zerodium and Crowdfense are distinct from their competitors
  - Purchase of exploitation chains rather than “vulnerabilities”
- Vulnerabilities must be exploitable in the wild and weaponized
  - Proof-of-concept exploit code must be submitted by researchers

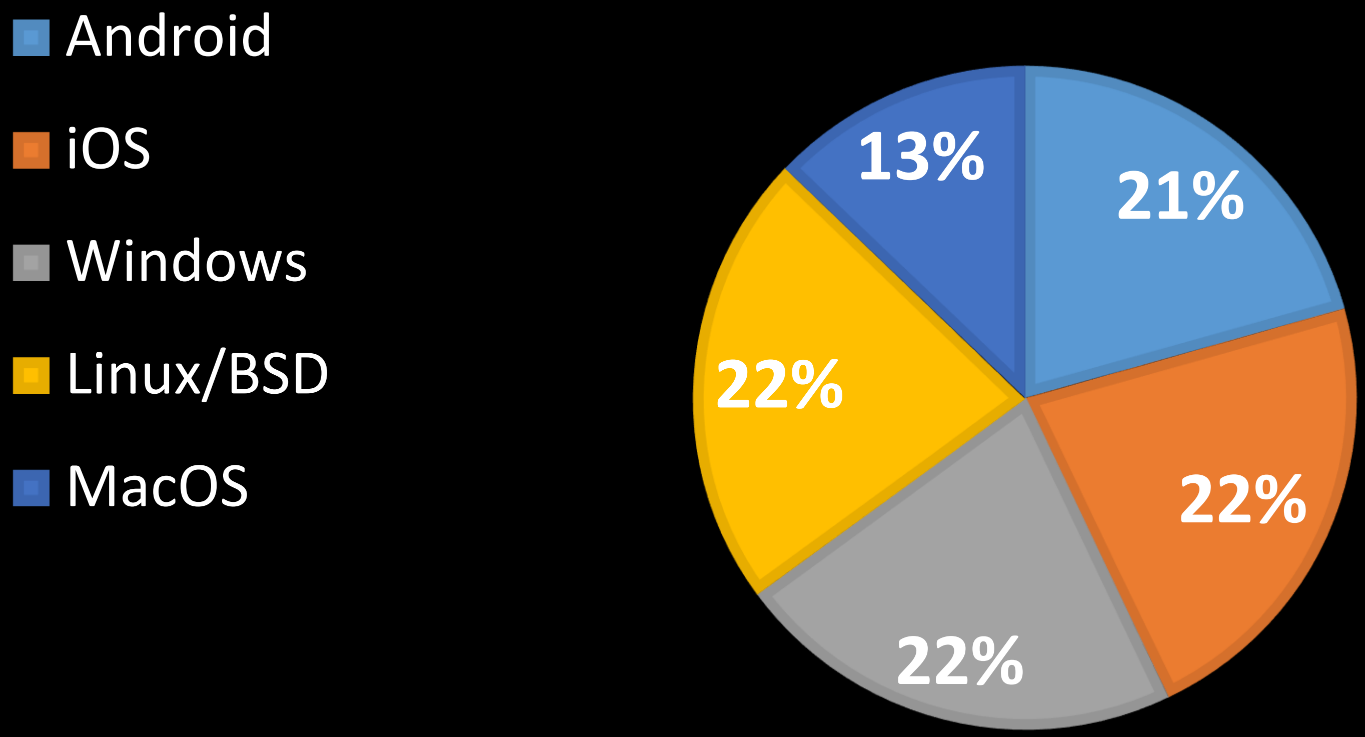
Overview of Data Set & Some Quick Caveats

- Data covers the period from 2015-2019
- Publicly available information of requested bounties
  - Nearly 400 entries
- Includes temporary bounties and those introduced in press announcements/news articles
- Comprised primarily of requested bounties (e.g., Zerodium, Crowdfense, etc.) rather than reported vulnerabilities
  - Currently does not include competition bounties (e.g., Pwn2Own, etc.)
- This dataset is based on public bounties --- There likely are many targets/capabilities that are requested privately

Bounties by Target



Targeted Operating Systems



TARGETED OS (EXPANDED DATASET)

Total Payouts

- Data set includes payout amounts for various bounties since 2015
  - Maximum values for bounties are indicated
  - Total value – just under **$120 million****

- **Caveats:
  - May not be properly adjusted to account for combined bounties (i.e., payouts that are provided from the same group of funds
  - In some cases, the bounties are carried over likely due to a lack eligible submissions

Highest Payouts (by Bounty)

Exploit	Date	Maximum Payout	Provider

Android zero-click remote code execution (RCE) + privilege escalation (PE)	Apr. 2018;
	Jun. 2018;
	Mar. 2019
		$3 million	Crowdfense

Android zero-click RCE	Apr. 2018	$3 million	Crowdfense

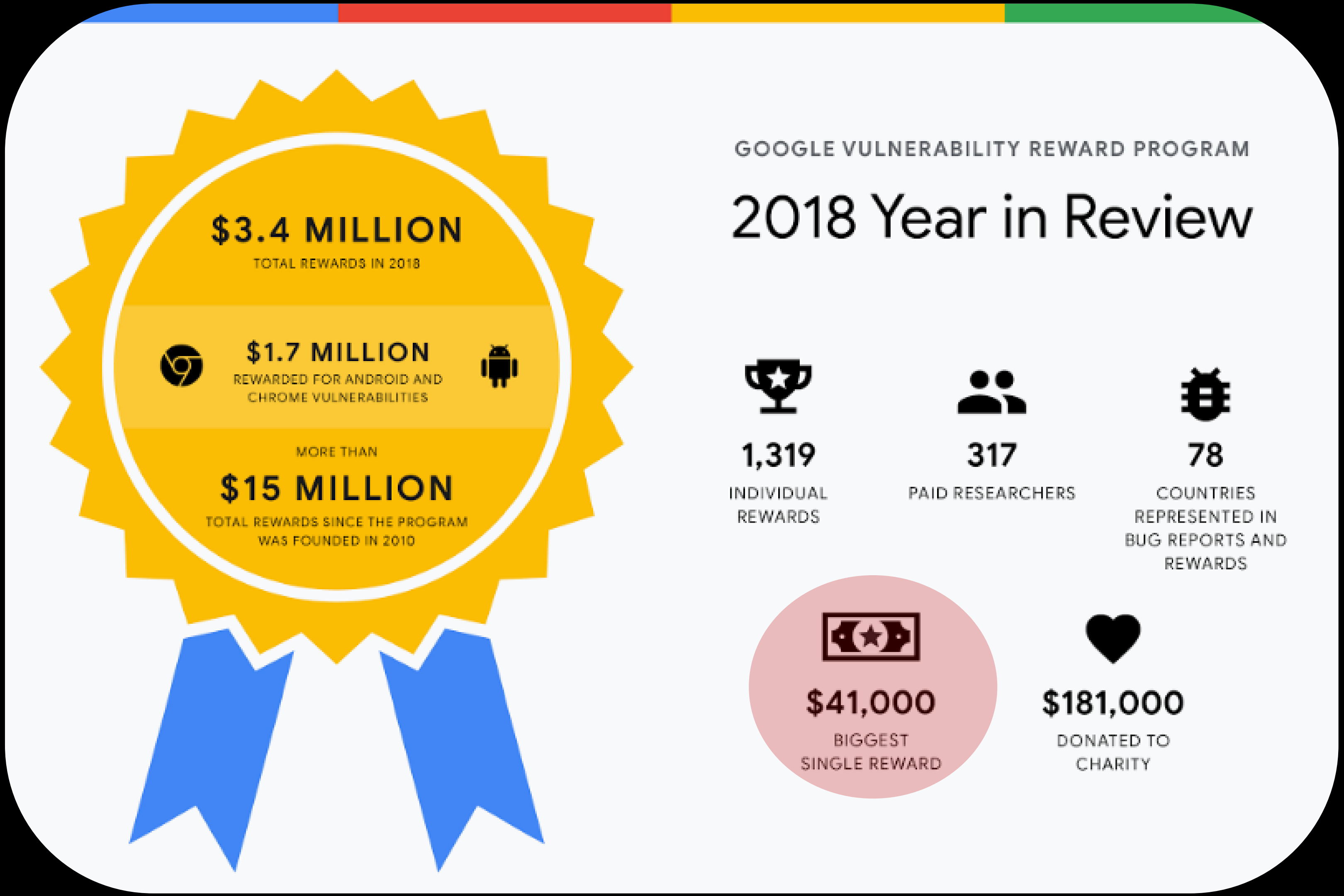
iOS zero-click RCE + PE	Apr. 2018;
	Jun. 2018;
	Mar. 2019
		$3 million	Crowdfense

Android zero-click RCE + PE	Apr. 2018	$2.5 million	Zerodium

iOS Safari RCE + PE	Apr. 2018;
	Jun. 2018;
	Mar. 2019
		$2.5 million	Crowdfense

iOS Safari RCE	Apr. 2018	$2.5 million	Crowdfense

Comparison to Other Bug Bounty Programs



GOOGLE VULNERABILITY REWARD PROGRAM

2018 Year in Review

$3.4 MILLION
TOTAL REWARDS IN 2018

$1.7 MILLION
REWARDED FOR ANDROID AND CHROME VULNERABILITIES

MORE THAN
$15 MILLION
TOTAL REWARDS SINCE THE PROGRAM WAS FOUNDED IN 2010

1,319
INDIVIDUAL REWARDS

317
PAID RESEARCHERS

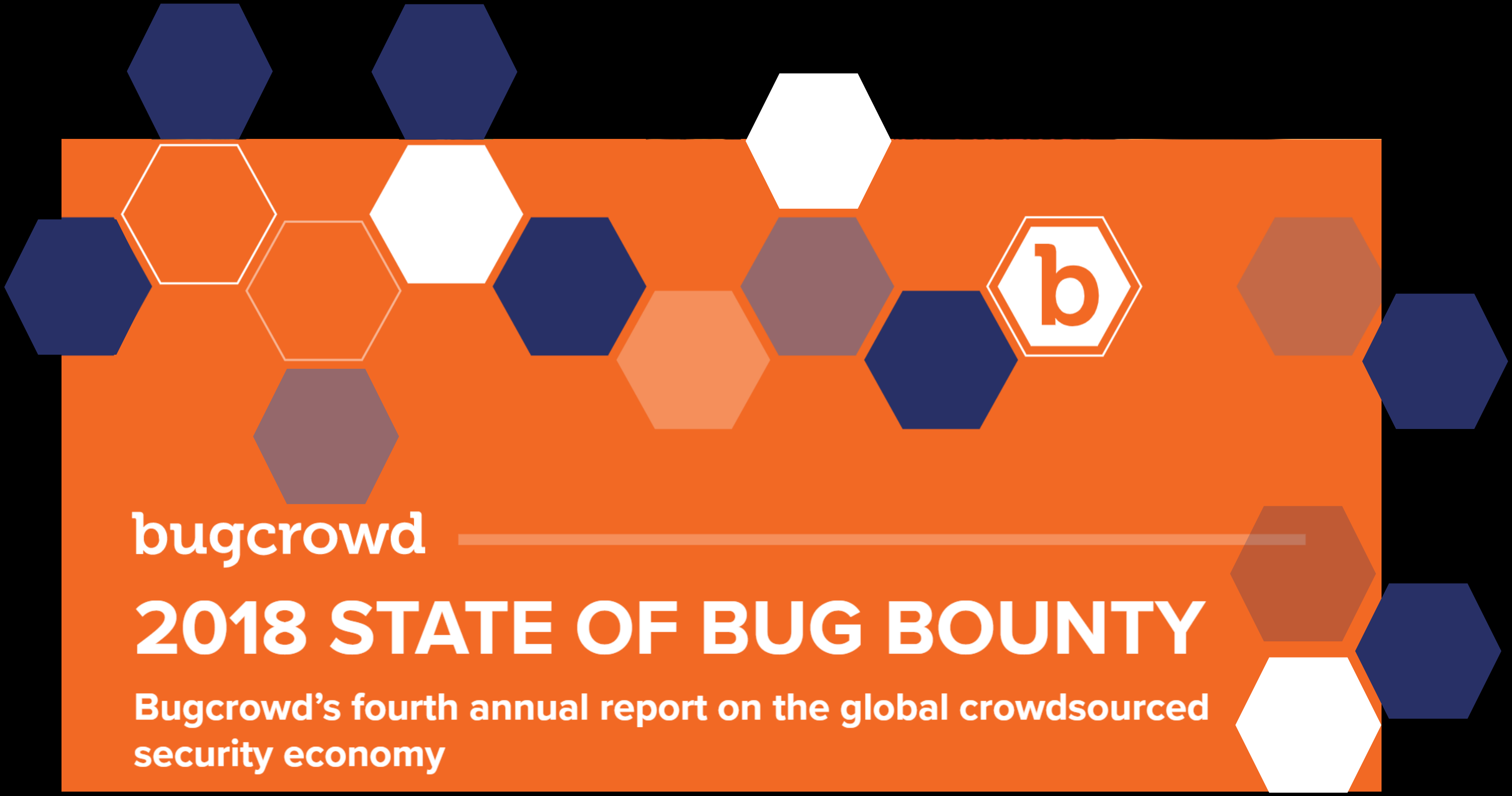
78
COUNTRIES REPRESENTED IN BUG REPORTS AND REWARDS

$41,000
BIGGEST SINGLE REWARD

$181,000
DONATED TO CHARITY

- During 2018 – Crowdfense and Zerodium offered 7 bounties for Chrome:
  - ❖$2M
  - ❖$1.5M
  - ❖$250K
  - ❖$150K
  - ❖$100K
  - ❖$50K
  - ❖$50K

Comparison to Other Bug Bounty Programs



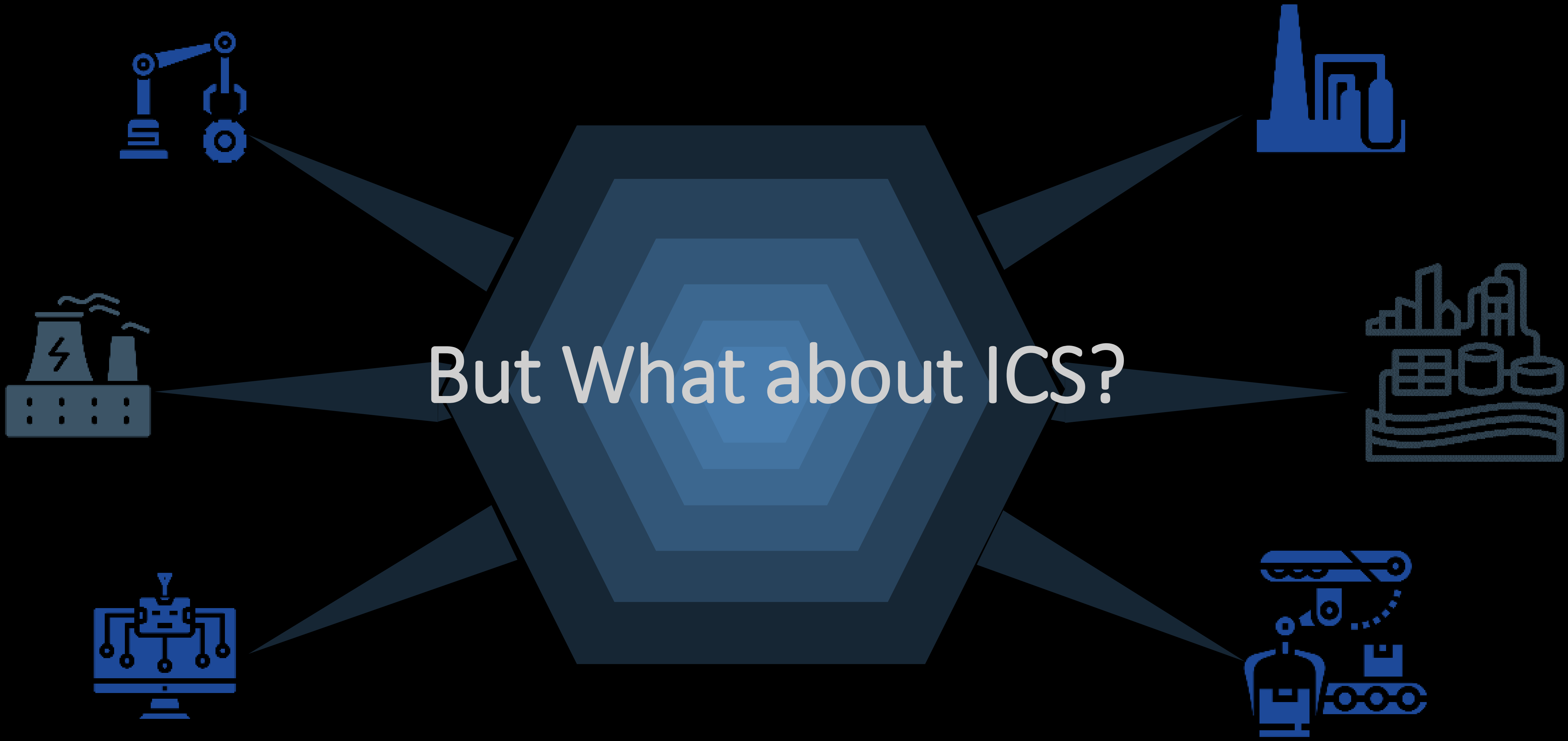
bugcrowd

2018 STATE OF BUG BOUNTY

Bugcrowd's fourth annual report on the global crowdsourced security economy

- 2018 Bugcrowd –
  - Average payout per vulnerability - $781
  - 2.5% IoT payouts

But What about ICS?

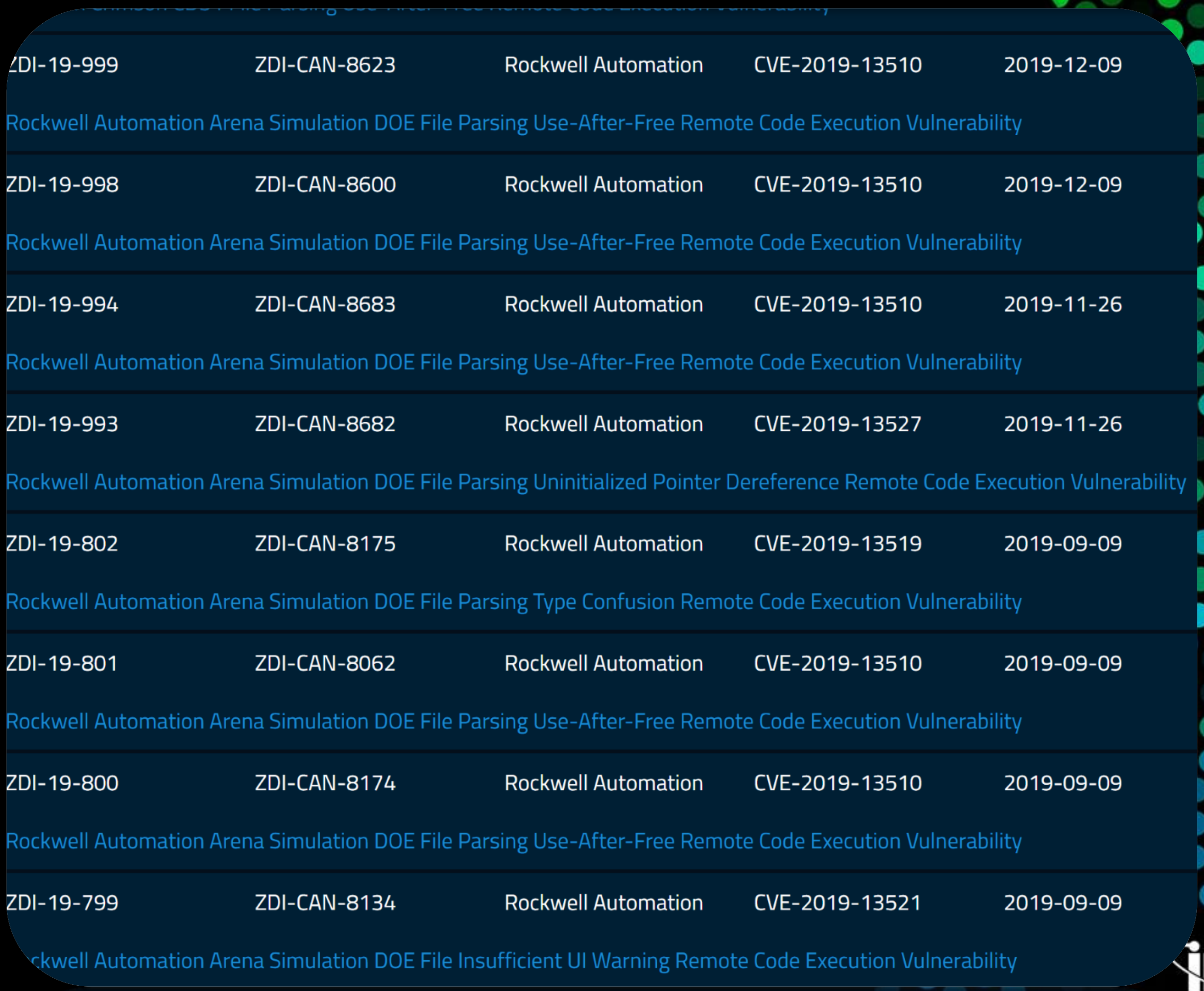


Zero Day Initiative ICS Alerts

SCADA bugs continue to soar. In 2017, we saw 21 bugs in Schneider Electric, but 2018 trounced their number with Advantech rising to the number one spot on our list.

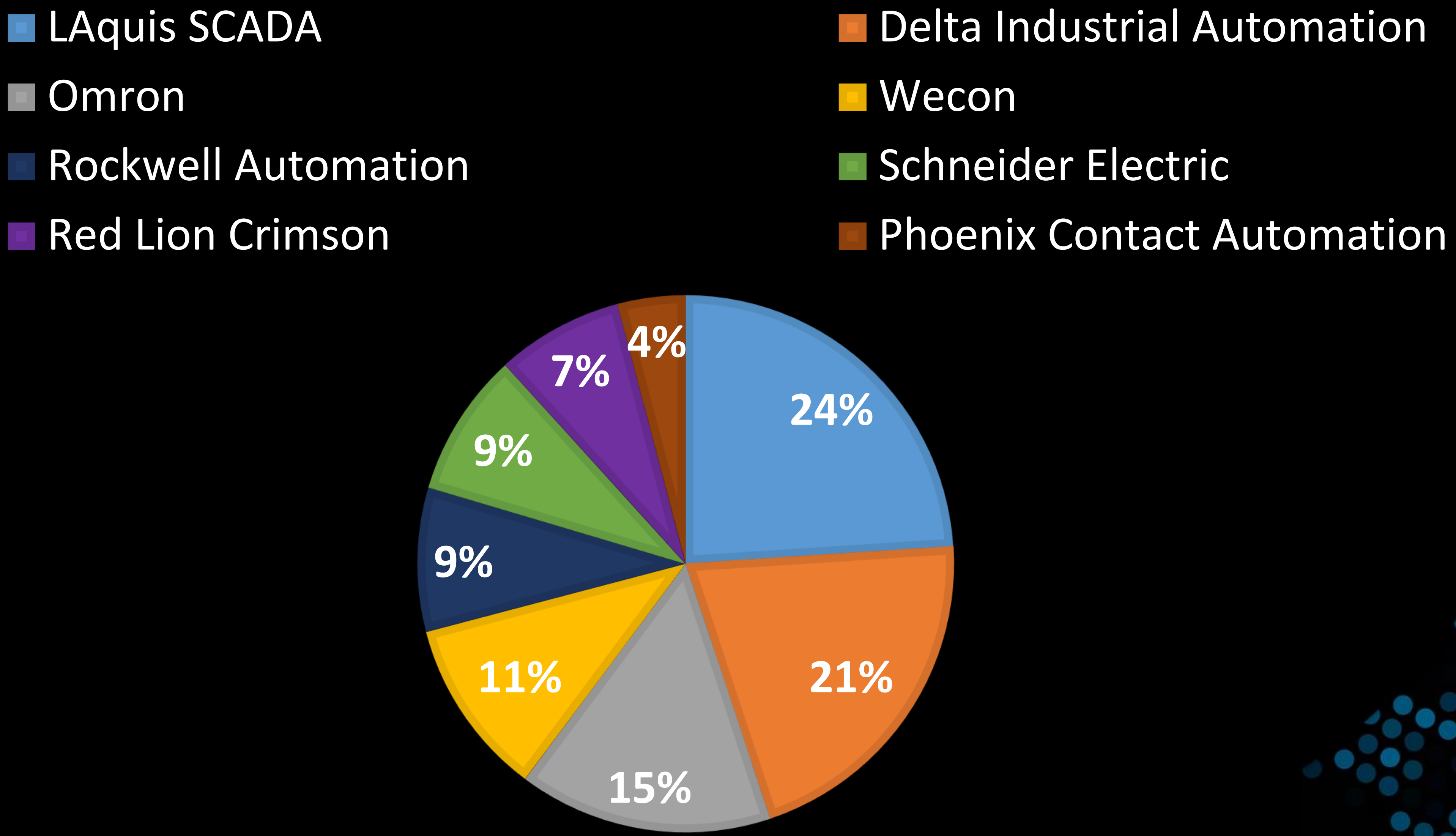
Together with Delta Industrial and Omron, SCADA bugs account for more than 30% of submissions to the program.

---Zero Day Initiative (ZDI), 2018

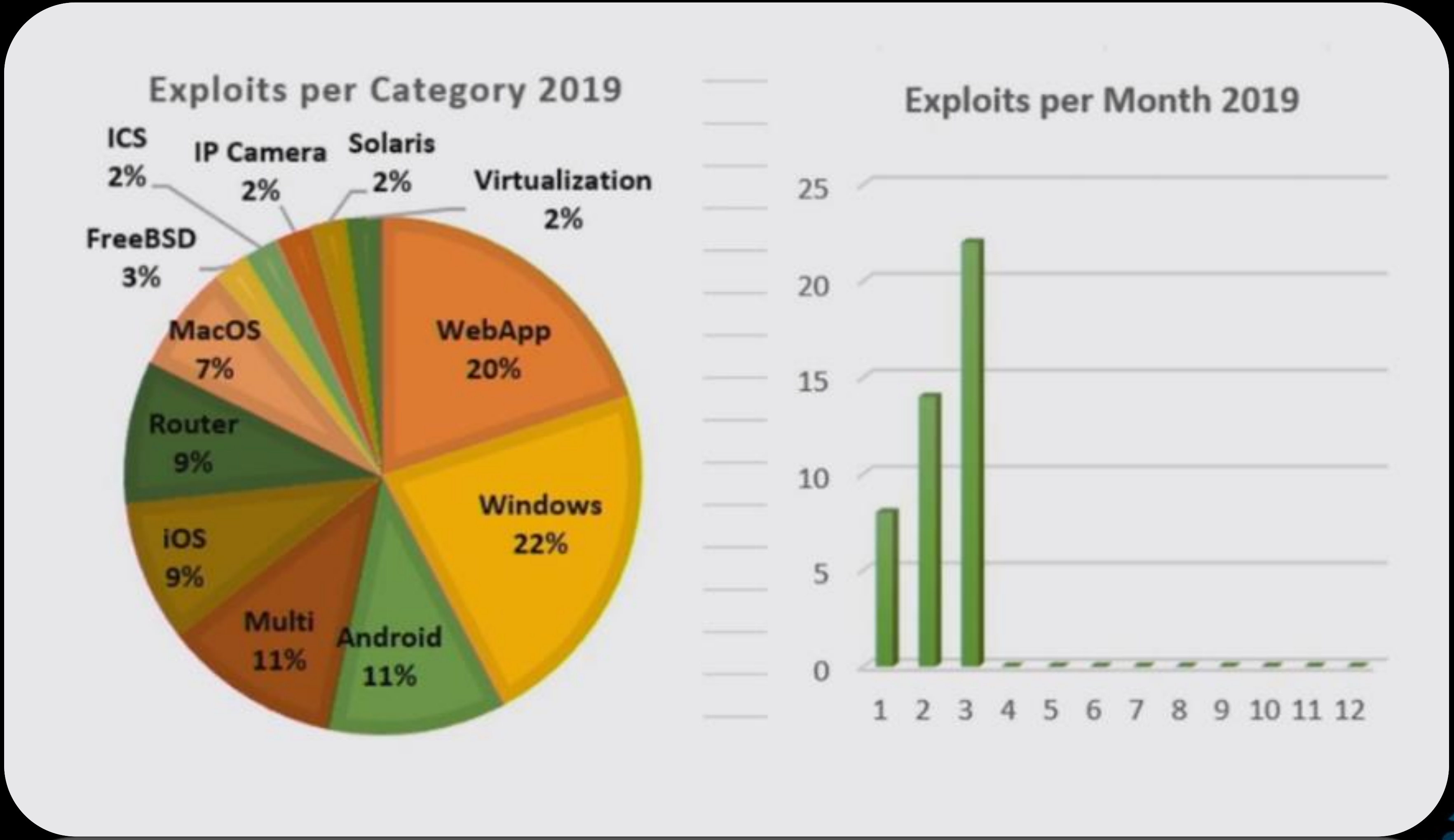


ZDI-19-999	ZDI-CAN-8623	Rockwell Automation	CVE-2019-13510	2019-12-09
Rockwell Automation Arena Simulation DOE File Parsing Use-After-Free Remote Code Execution Vulnerability				
ZDI-19-998	ZDI-CAN-8600	Rockwell Automation	CVE-2019-13510	2019-12-09
Rockwell Automation Arena Simulation DOE File Parsing Use-After-Free Remote Code Execution Vulnerability				
ZDI-19-994	ZDI-CAN-8683	Rockwell Automation	CVE-2019-13510	2019-11-26
Rockwell Automation Arena Simulation DOE File Parsing Use-After-Free Remote Code Execution Vulnerability				
ZDI-19-993	ZDI-CAN-8682	Rockwell Automation	CVE-2019-13527	2019-11-26
Rockwell Automation Arena Simulation DOE File Parsing Uninitialized Pointer Dereference Remote Code Execution Vulnerability				
ZDI-19-802	ZDI-CAN-8175	Rockwell Automation	CVE-2019-13519	2019-09-09
Rockwell Automation Arena Simulation DOE File Parsing Type Confusion Remote Code Execution Vulnerability				
ZDI-19-801	ZDI-CAN-8062	Rockwell Automation	CVE-2019-13510	2019-09-09
Rockwell Automation Arena Simulation DOE File Parsing Use-After-Free Remote Code Execution Vulnerability				
ZDI-19-800	ZDI-CAN-8174	Rockwell Automation	CVE-2019-13510	2019-09-09
Rockwell Automation Arena Simulation DOE File Parsing Use-After-Free Remote Code Execution Vulnerability				
ZDI-19-799	ZDI-CAN-8134	Rockwell Automation	CVE-2019-13521	2019-09-09
ckwell Automation Arena Simulation DOE File Insufficient UI Warning Remote Code Execution Vulnerability				

Zero Day Initiative ICS Alerts - 2019

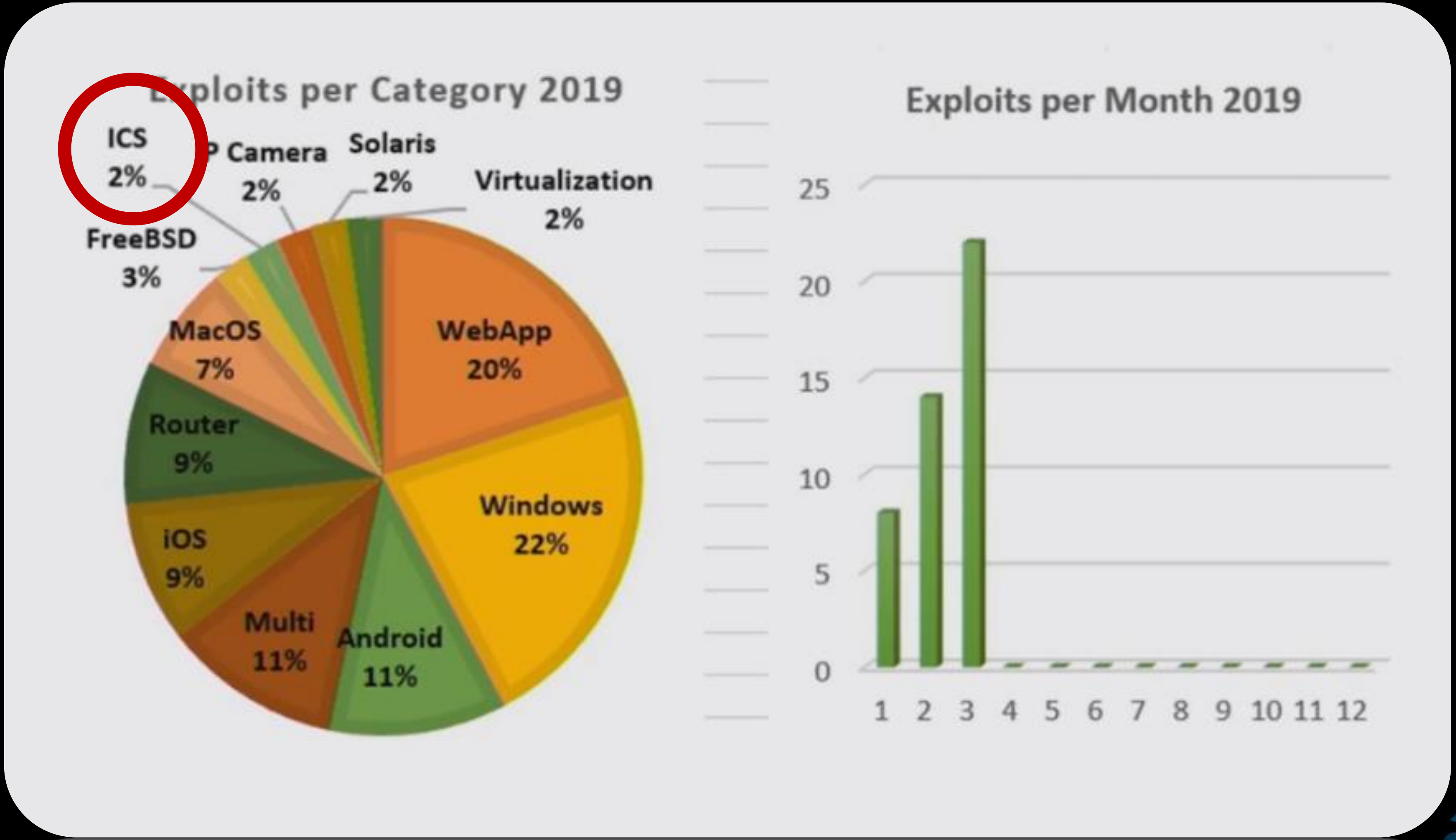


Crowdfense Bug Bounty Payouts Q1 2019



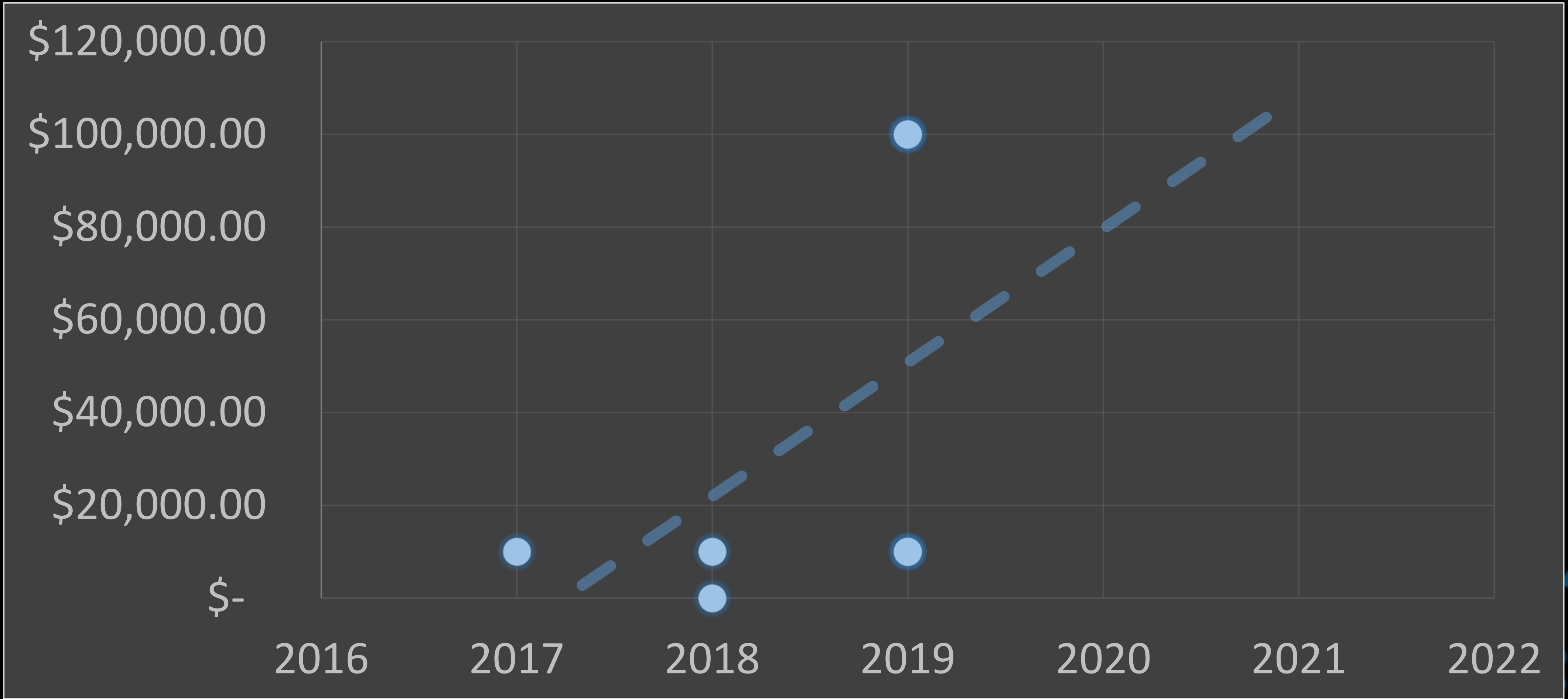
HITBHaxpo; Hacking The 0day Market - Andrea Zapparoli Manzoni, Crowdfense

Crowdfense Bug Bounty Payouts Q1 2019

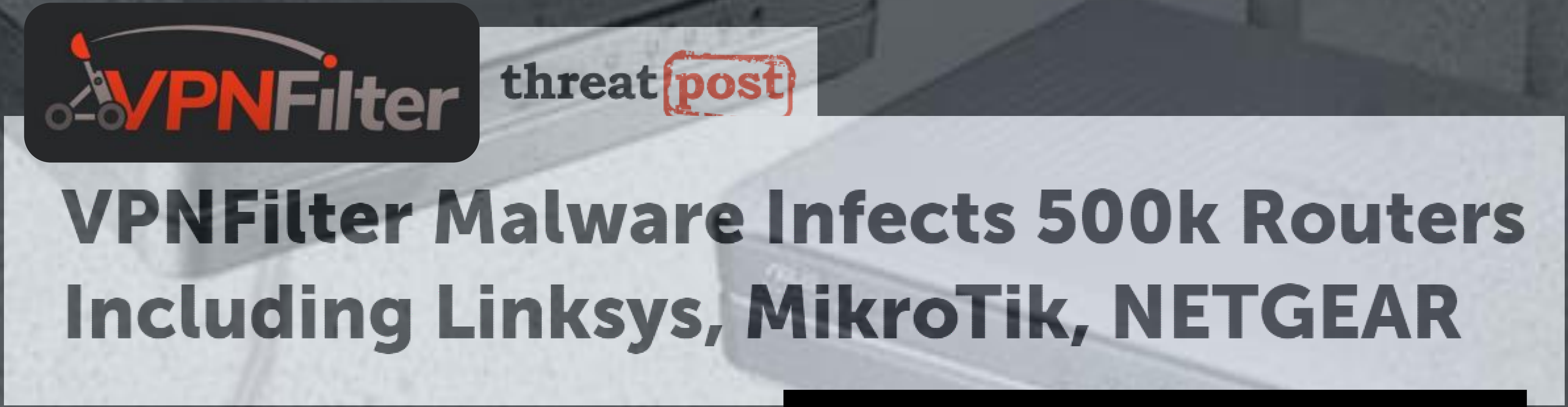


HITBHaxpo; Hacking The 0day Market - Andrea Zapparoli Manzoni, Crowdfense

Continued Targeting of Comms - Routers



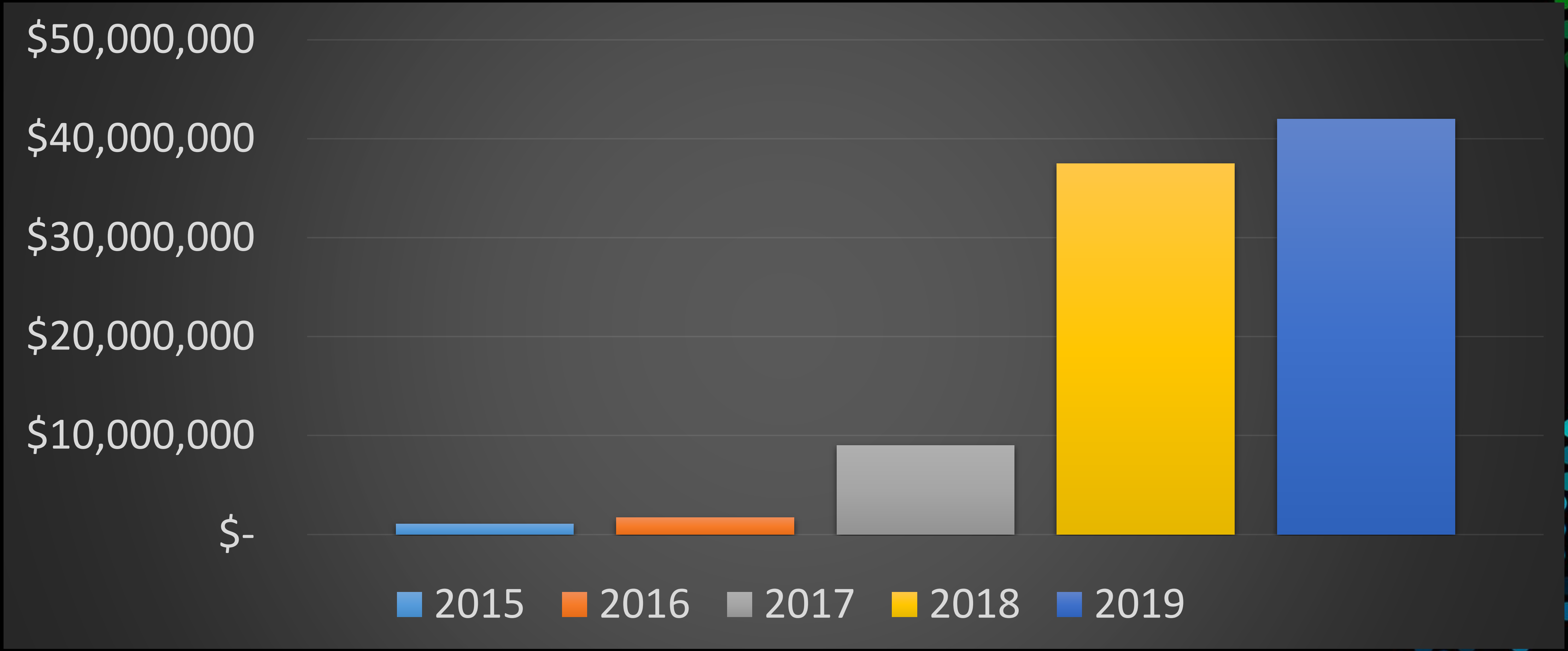
Continued Targeting of Comms - Routers



VPNFilter Malware Infects 500k Routers Including Linksys, MikroTik, NETGEAR

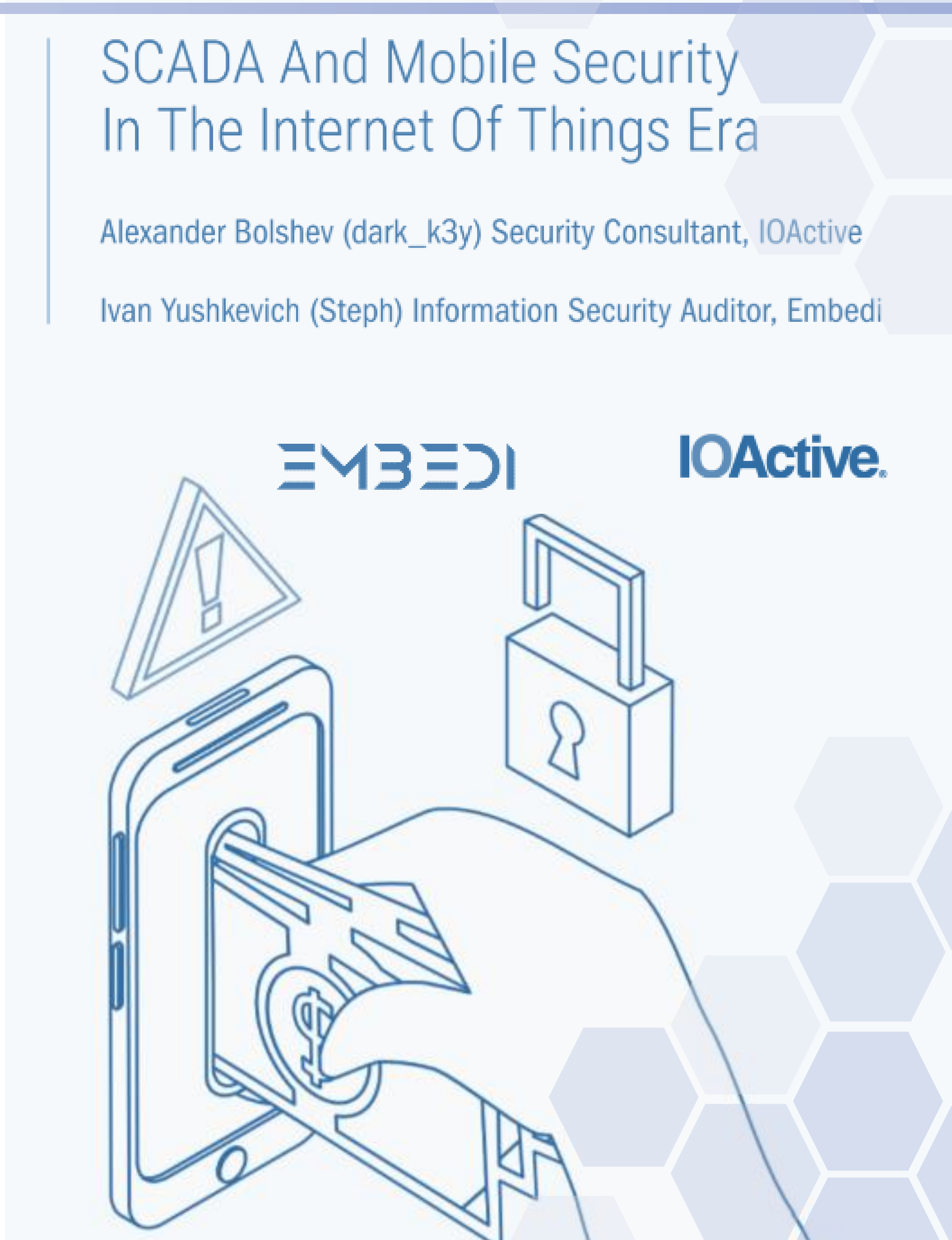
"…the VPNFilter malware allows for theft of website credentials and monitoring of Modbus SCADA protocols."

Bounty Growth for Mobile Targets



Mobile Vulns in OT

- Local (control room) and remote mobile-based devices and applications provide access to OT environment
    - Bolshev and Yushkevich, 2017
    - Emergence of an industrial IOT (IIOT)
- A security review conducted over two years found that an increase in IIOT mobile applications without a corresponding increase in security

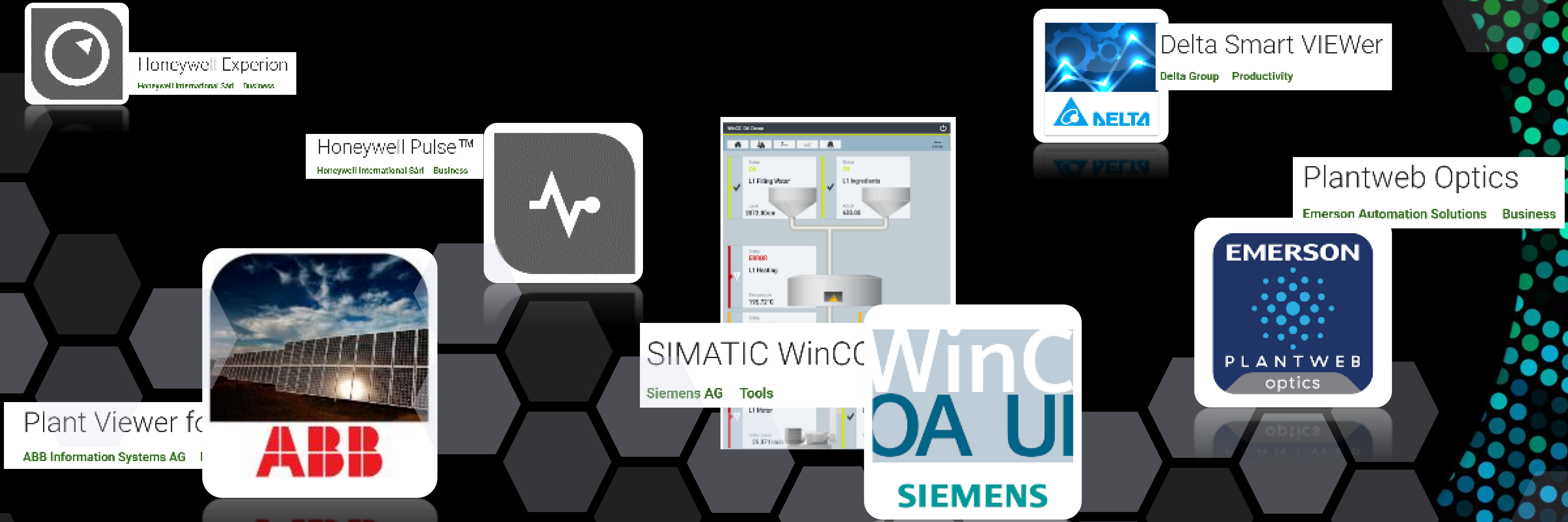


SCADA And Mobile Security
In The Internet Of Things Era

Alexander Bolshev (dark_k3y) Security Consultant, IOActive

Ivan Yushkevich (Steph) Information Security Auditor, Embedi

Propagation of Operational Technology Apps



Honeywell Experion

Honeywell International Sàrl Business

Honeywell Pulse™

Honeywell International Sàrl Business

Plant Viewer fo

ABB Information Systems AG I

SIMATIC WinCC

Siemens AG Tools

Delta Smart VIEWer

Delta Group Productivity

Plantweb Optics

Emerson Automation Solutions Business

Same Security Challenges… Different Platforms

SIMATIC WinCC OA UI

Siemens AG Tools

https://www.us-cert.gov/ics/advisories/ICSA-18-081-01

ICS Advisory (ICSA-18-081-01)

Siemens SIMATIC WinCC OA UI Mobile App

CVSS v3 5.1
ATTENTION: Exploitable from an adjacent network.
Vendor: Siemens
Equipment: SIMATIC WinCC OA UI mobile app
Vulnerability: Improper Access Control

AFFECTED PRODUCTS

Siemens reports that this vulnerability affects the following products:
SIMATIC WinCC OA UI for Android: All versions prior to V3.15.10, and
SIMATIC WinCC OA UI for IOS: All versions prior to V3.15.10

IMPACT

This vulnerability could be exploited by an attacker who tricks an app user to connect to a malicious WinCC OA server. Successful exploitation of this vulnerability could allow an attacker to read and write data from and to the app's project cache folder.

Same Security Challenges… Different Platforms

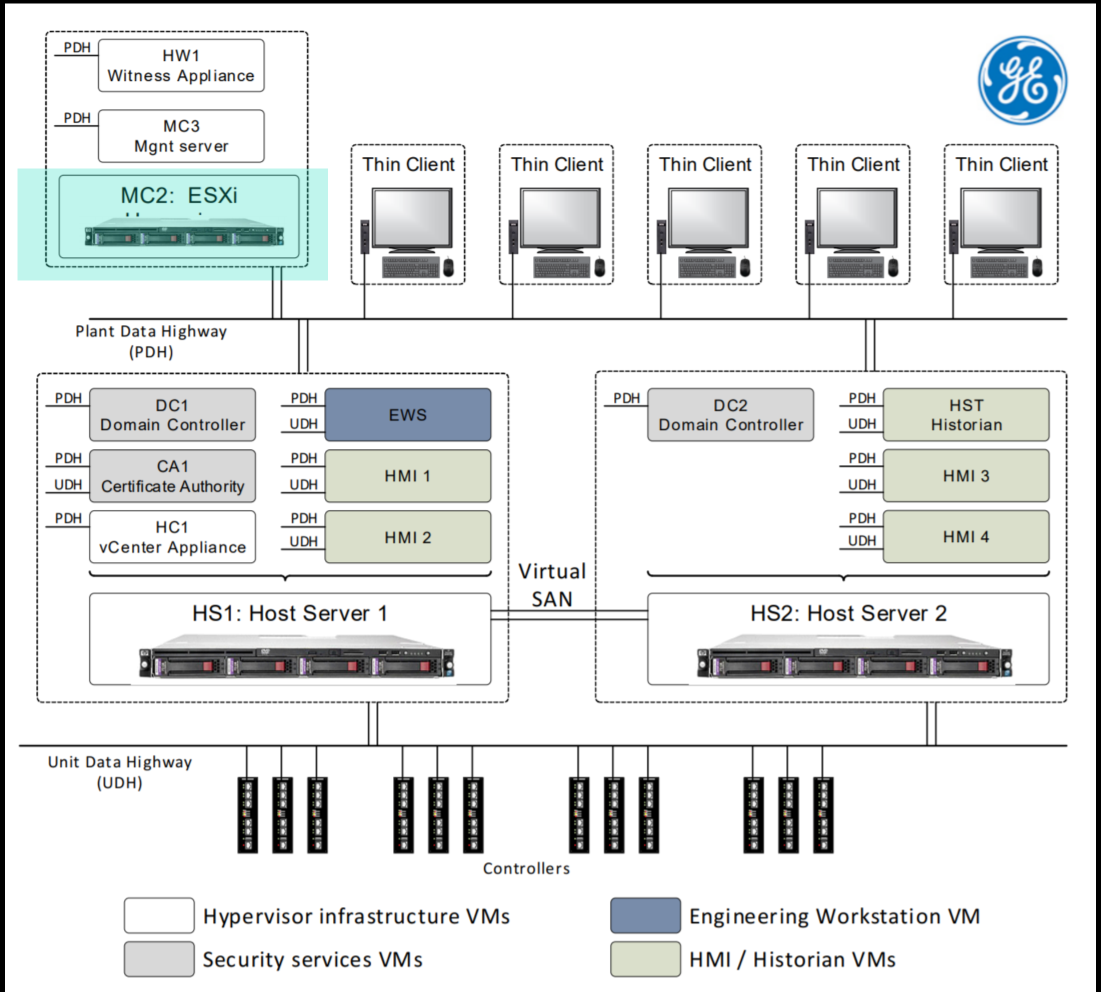
https://www.us-cert.gov/ics/advisories/ICSA-18-046-03

ICS Advisory (ICSA-18-046-03)

Schneider Electric IGSS Mobile

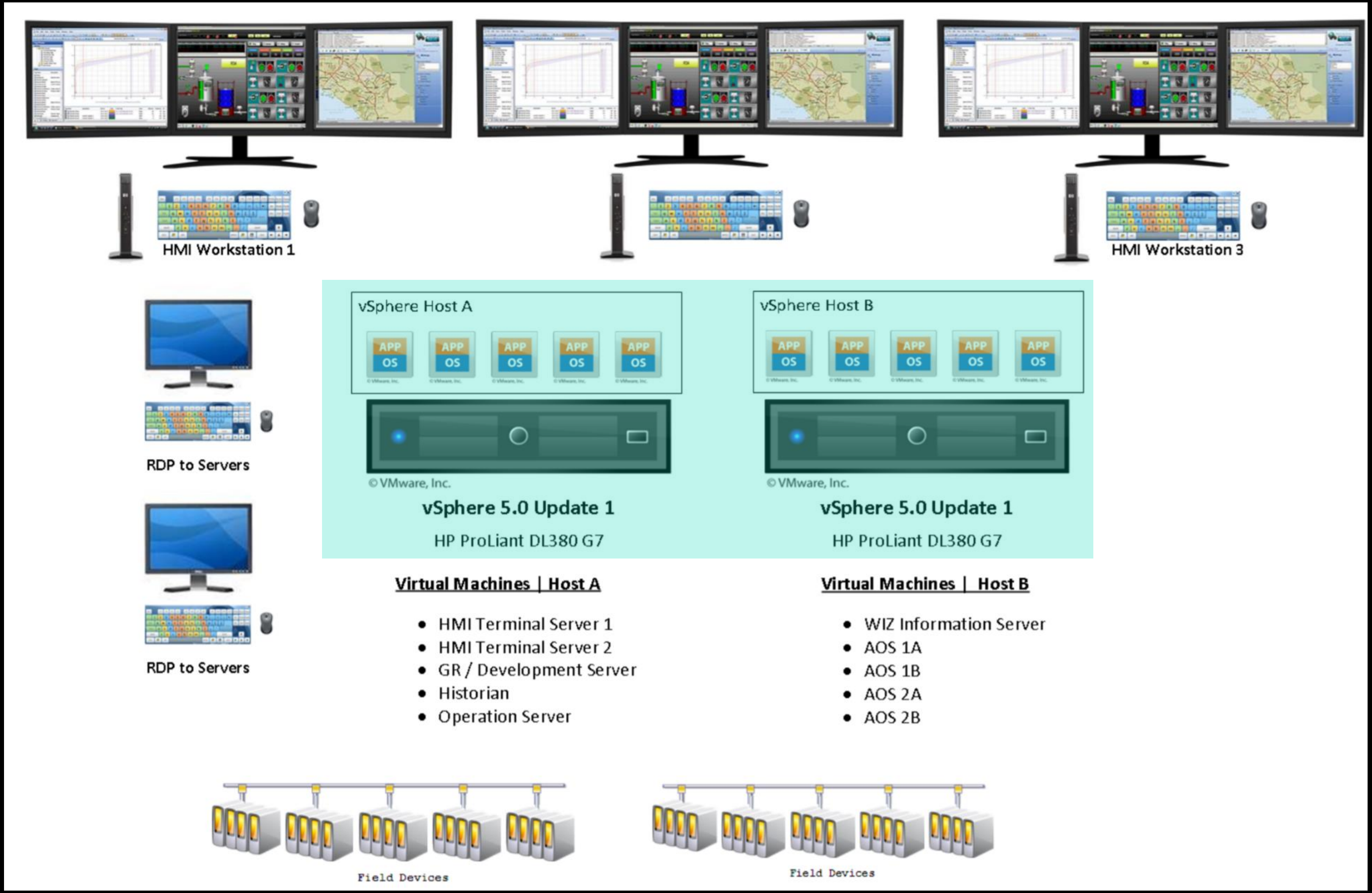
CVSS v3 6.4
ATTENTION: Locally exploitable/low skill level to exploit.
Vendor: Schneider Electric
Equipment: IGSS Mobile
Vulnerabilities: Improper Certificate Validation, Plaintext Storage of a Password
AFFECTED PRODUCTS
Schneider Electric reports that the vulnerabilities affect the following IGSS Mobile products:
IGSS Mobile for Android, version 3.01 and all versions prior, and
IGSS Mobile for iOS, version 3.01 and all versions prior.
IMPACT
Successful exploitation of these vulnerabilities could allow an attacker to execute a man-in-the-middle attack. In addition, passwords can be accessed by unauthorized users.

Virtual Machine Vulnerabilities



- Virtual machine exploitation & escape
  - Consistently requested vulnerabilities with bounties appearing every year (2015-2019)
  - Maximum payout ranges - $50K to $500K

Virtual Machine Vulnerabilities



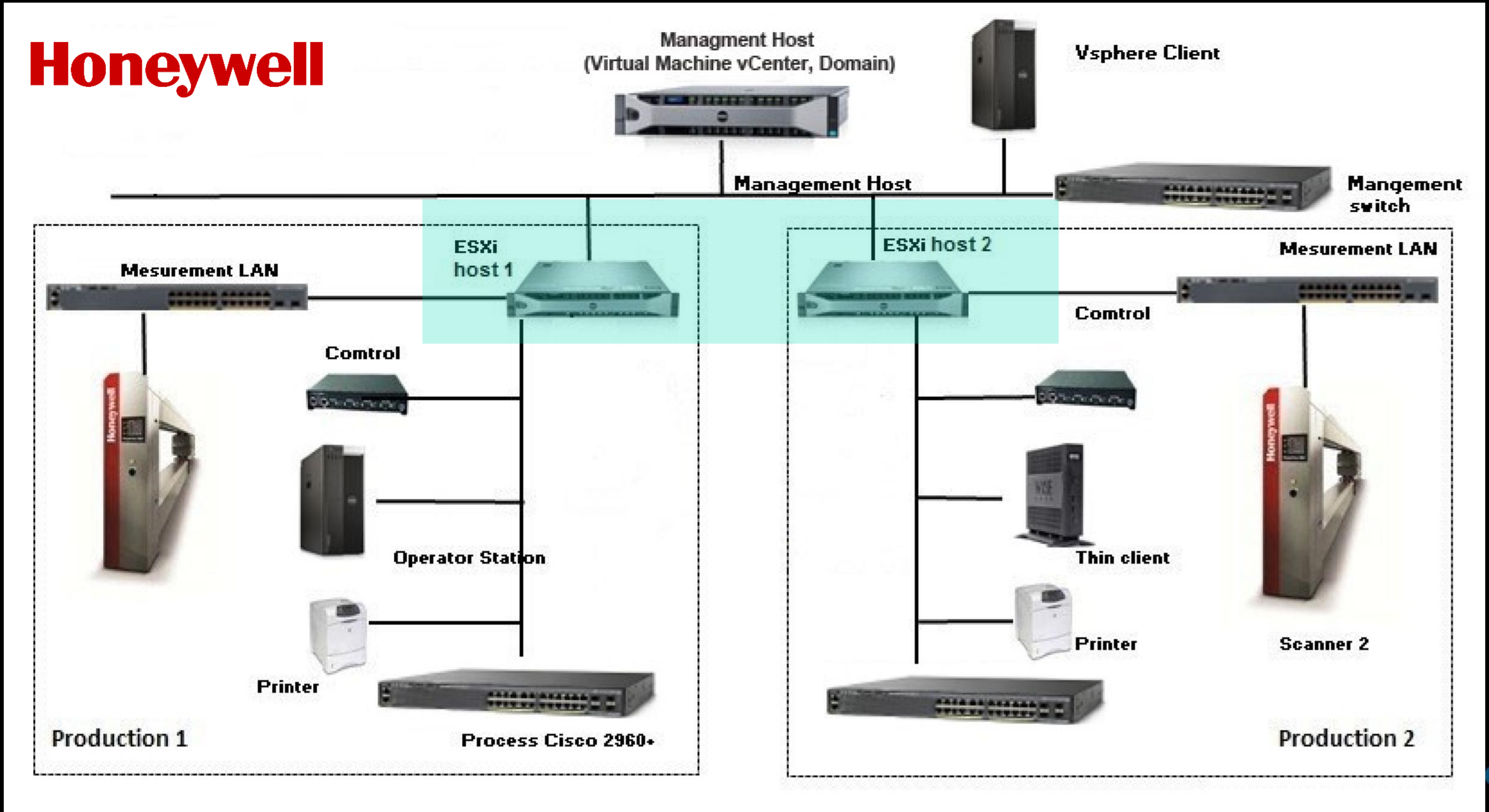
Virtual Machines | Host A

- HMI Terminal Server 1
- HMI Terminal Server 2
- GR / Development Server
- Historian
- Operation Server

Virtual Machines | Host B

- WIZ Information Server
- AOS 1A
- AOS 1B
- AOS 2A
- AOS 2B

Virtual Machine Vulnerabilities



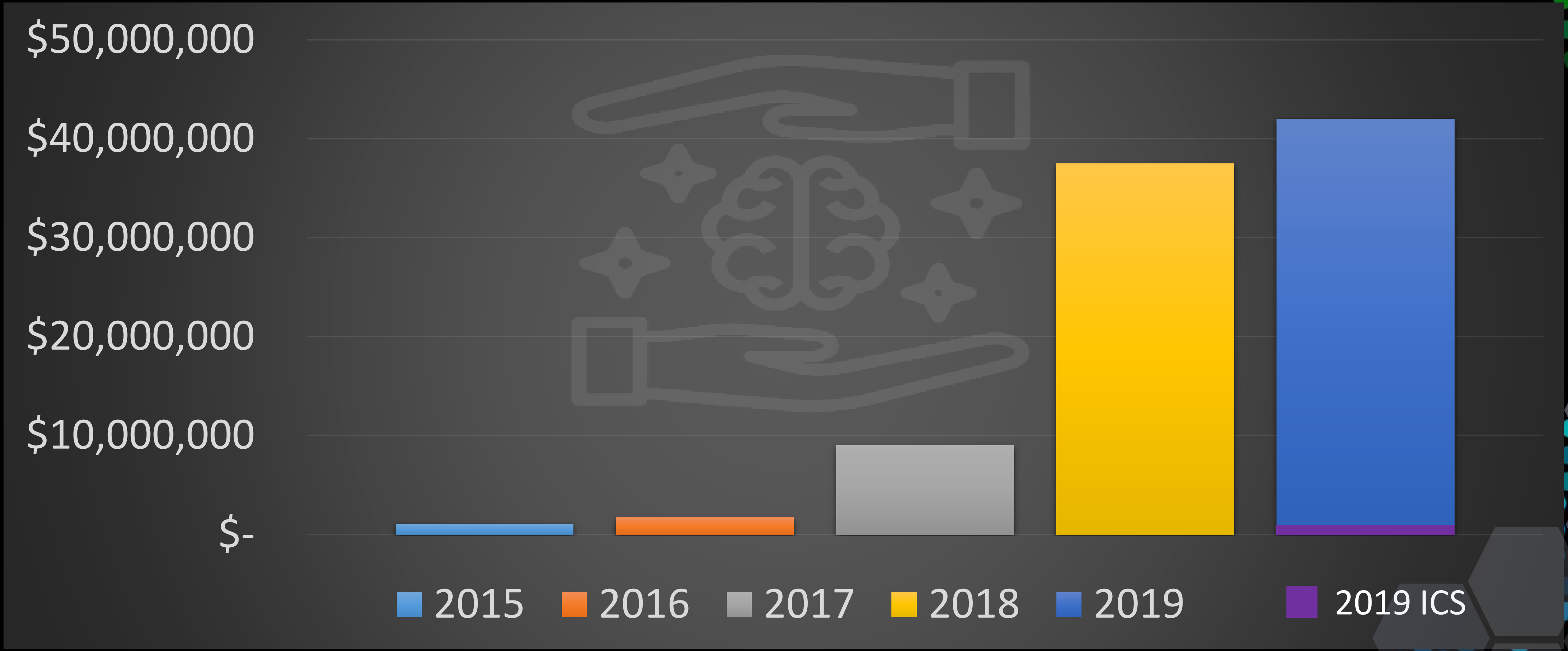
So What?

- The ICS/OT formal 0day market is relatively new
  - Growth will likely mirror the expansion of the collective market
  - Vender/service-based bounties remain overshadowed by the vulnerability brokers
- Identification and categorization of ICS/OT bounties will remain challenging as IT technologies and architectures continue to be integrated within OT
  - Many ICS/OT bounties will likely be collected under different technology bounty pools

So What?

- Threat intelligence is based on the foundational concept that cyber weapon development progresses in a logical and definable path
  - Growth can be predicted allowing for the adjustment of risk models
  - Faulty Assumption: capabilities are developed in a secure and segmented vacuum
- Unfortunate Reality – Cyber capabilities and competencies can be bought and growth can be augmented
  - Risk assessments must be prepared for these potential **jumps** in growth

Future Growth ???



Contact Info

Sarah Freeman
Idaho National Laboratory
Cybercore Integration Center
Sarah.Freeman@inl.gov