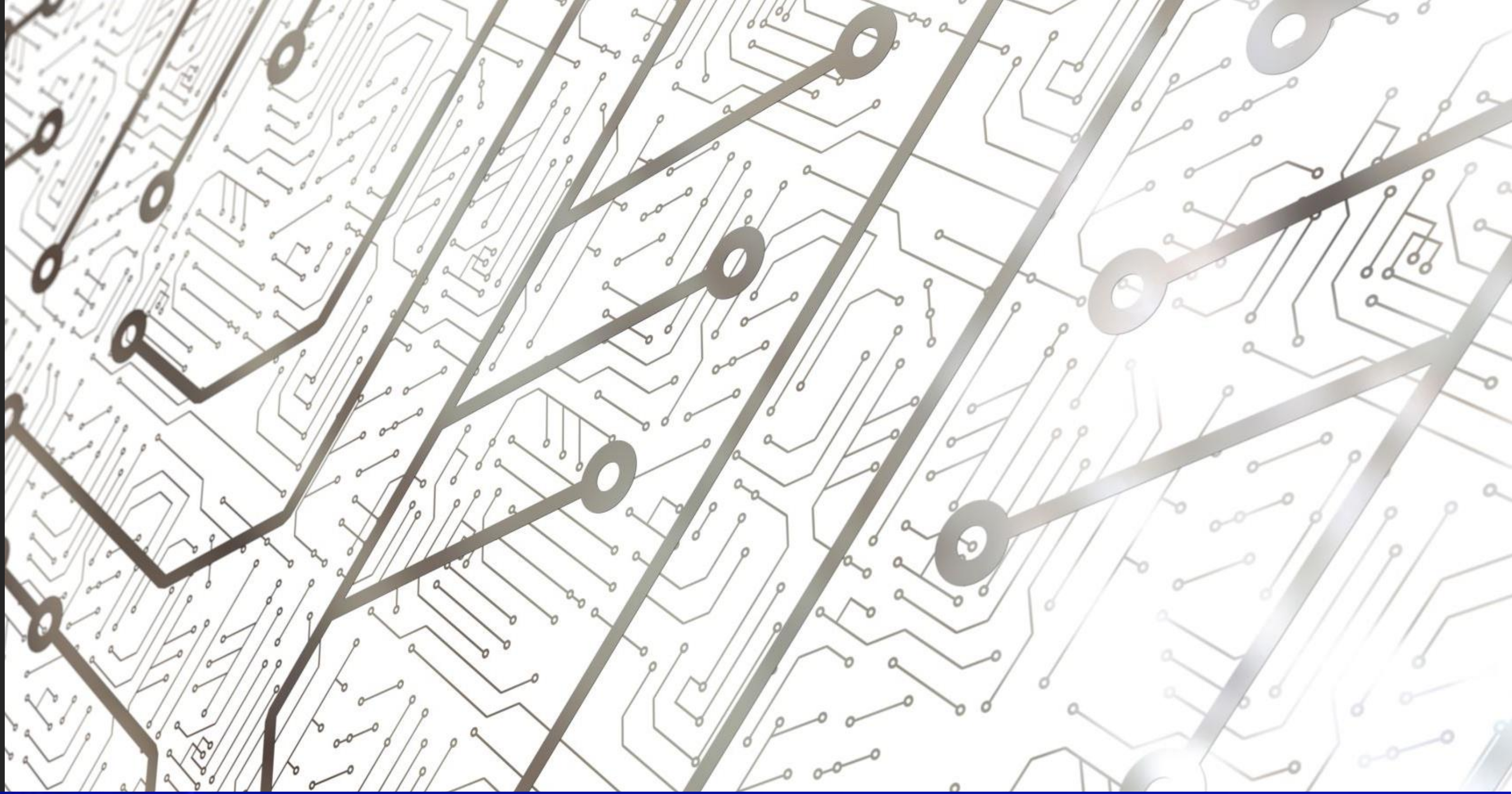
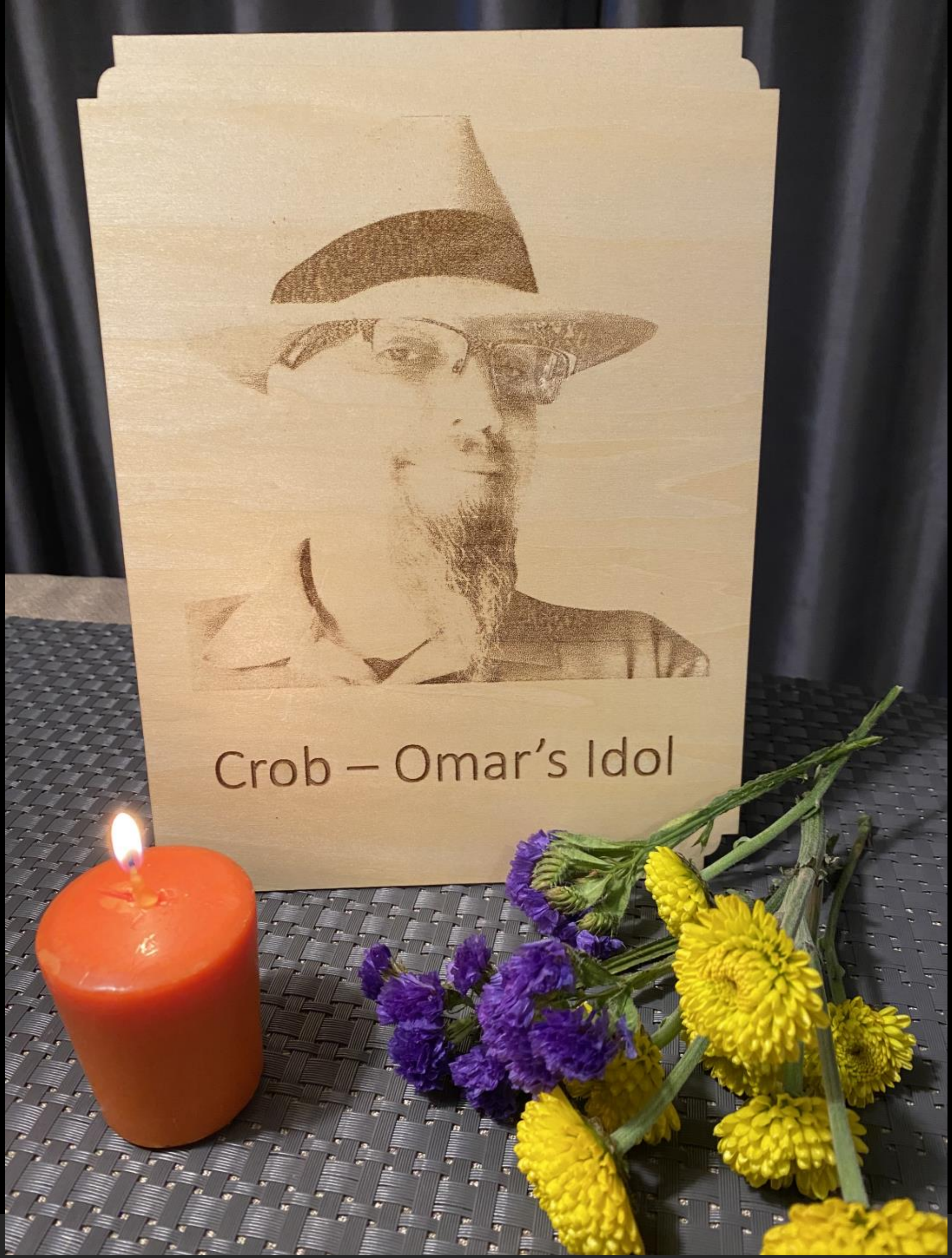
The State of Third-Party Software Security in 2020

Omar Santos
os@cisco.com



This presentation is dedicated to CRob


Crob – Omar’s Idol

CRob

2020

January

Mon	Tue	Wed	Thu	Fri	Sat	Sun
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

February

Mon	Tue	Wed	Thu	Fri	Sat	Sun
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	

March

Mon	Tue	Wed	Thu	Fri	Sat	Sun
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

April

Mon	Tue	Wed	Thu	Fri	Sat	Sun
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

May

Mon	Tue	Wed	Thu	Fri	Sat	Sun
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

June

Mon	Tue	Wed	Thu	Fri	Sat	Sun
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

July

Mon	Tue	Wed	Thu	Fri	Sat	Sun
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

August

Mon	Tue	Wed	Thu	Fri	Sat	Sun
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

September

Mon	Tue	Wed	Thu	Fri	Sat	Sun
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

October

Mon	Tue	Wed	Thu	Fri	Sat	Sun
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

November

Mon	Tue	Wed	Thu	Fri	Sat	Sun
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

December

Mon	Tue	Wed	Thu	Fri	Sat	Sun
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

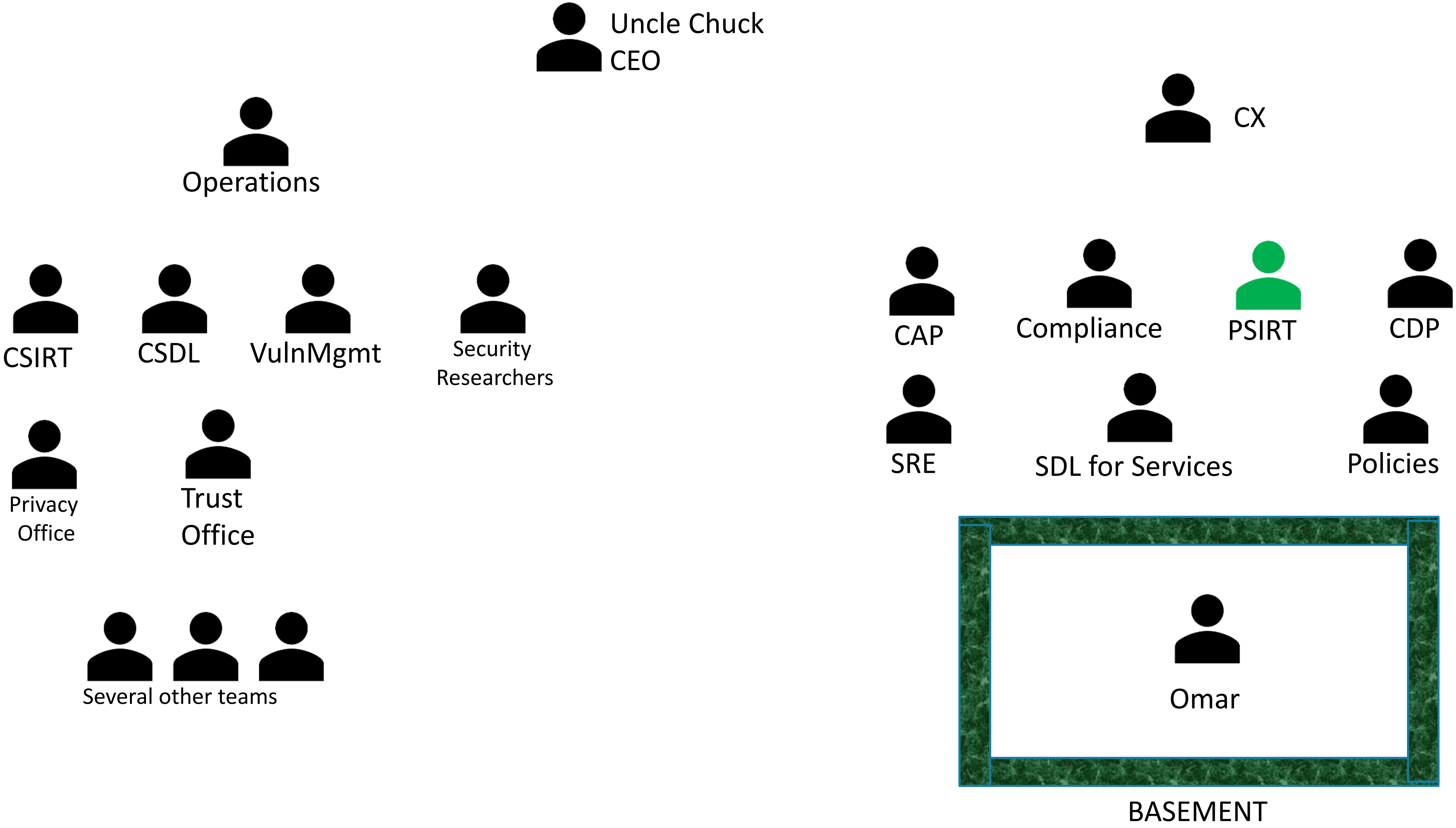
Agenda

- Introduction to third-party software (commercial and open source) security challenges.
- Third-party software (TPS) security tools.
- PSIRT’s role in TPS security.
- Disclosing TPS vulnerabilities.
- TPS security in the cloud.

Are you *#$^& kidding me?

Active Discussion

WHO CAME UP WITH THE TERM “BIRDS OF A FEATHER”?



Uncle Chuck
CEO

Operations

CSIRT

CSDL

VulnMgmt

Security Researchers

Privacy Office

Trust Office

Several other teams

CX

CAP

Compliance

PSIRT

CDP

SRE

SDL for Services

Policies

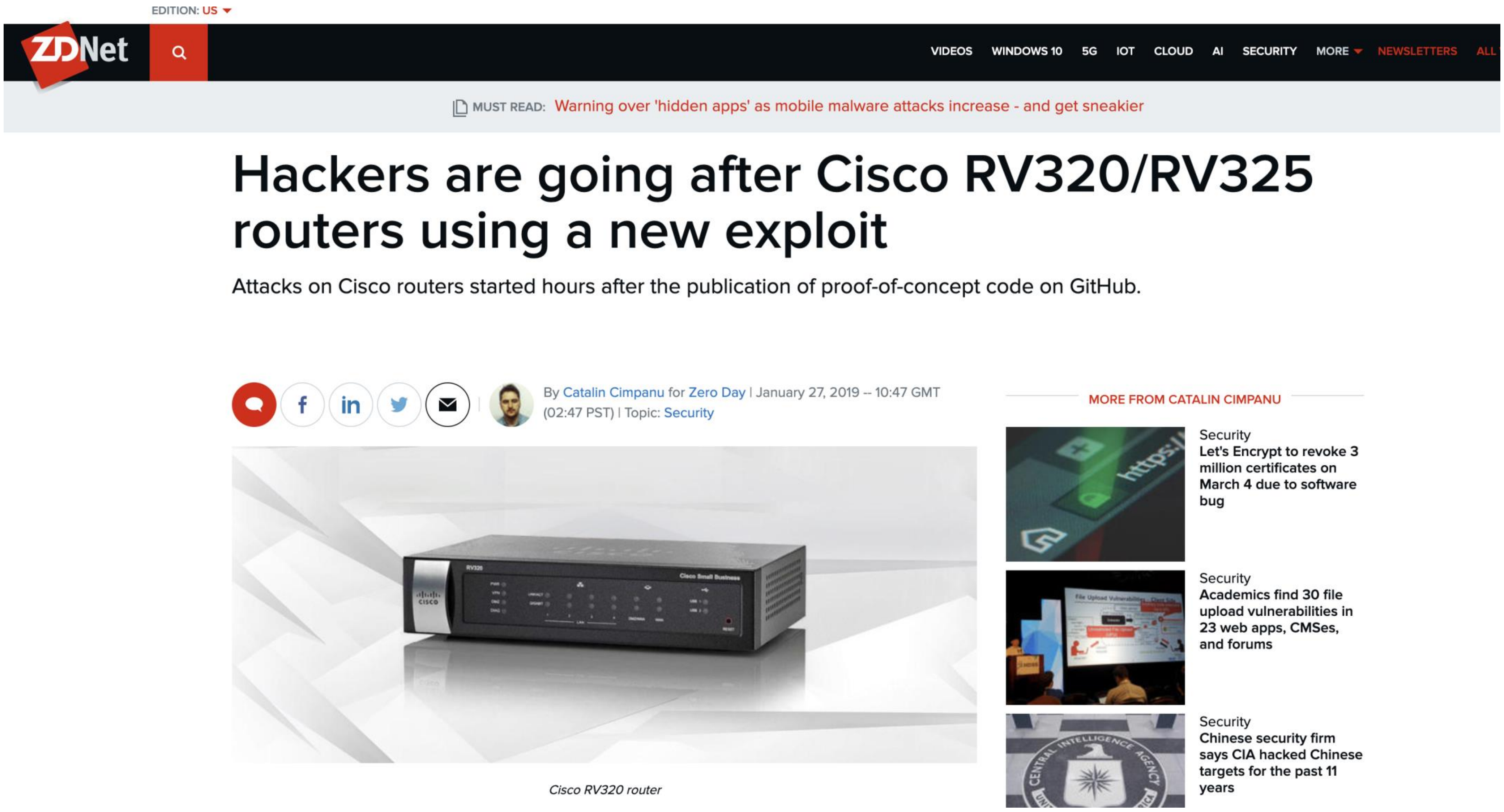
Omar

BASEMENT

TPS Security…
It’s 2020… Are we better than we were 10 years ago?

SLOs/SLAs in Contracts (Customer Contracts and Supplier Contracts)

Fixing Open Source is not one company’s task…



MUST READ: Warning over 'hidden apps' as mobile malware attacks increase - and get sneakier

Hackers are going after Cisco RV320/RV325 routers using a new exploit

Attacks on Cisco routers started hours after the publication of proof-of-concept code on GitHub.

By Catalin Cimpanu for Zero Day | January 27, 2019 -- 10:47 GMT (02:47 PST) | Topic: Security

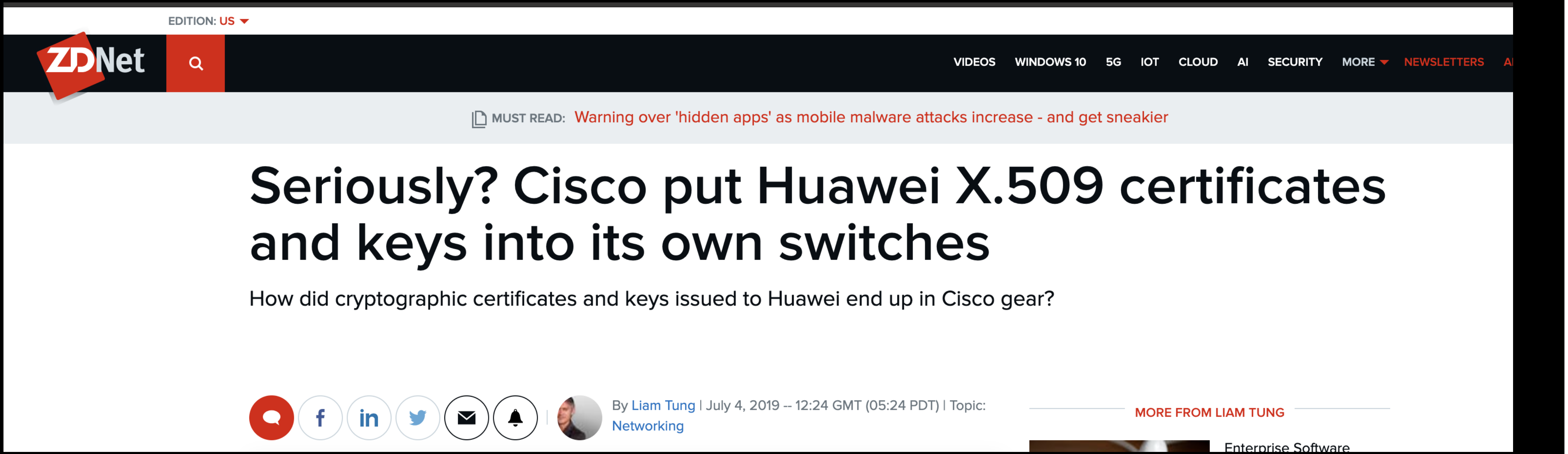
Cisco RV320 router

MORE FROM CATALIN CIMPANU

Security
Let's Encrypt to revoke 3 million certificates on March 4 due to software bug

Security
Academics find 30 file upload vulnerabilities in 23 web apps, CMSes, and forums

Security
Chinese security firm says CIA hacked Chinese targets for the past 11 years



MUST READ: Warning over 'hidden apps' as mobile malware attacks increase - and get sneakier

Seriously? Cisco put Huawei X.509 certificates and keys into its own switches

How did cryptographic certificates and keys issued to Huawei end up in Cisco gear?

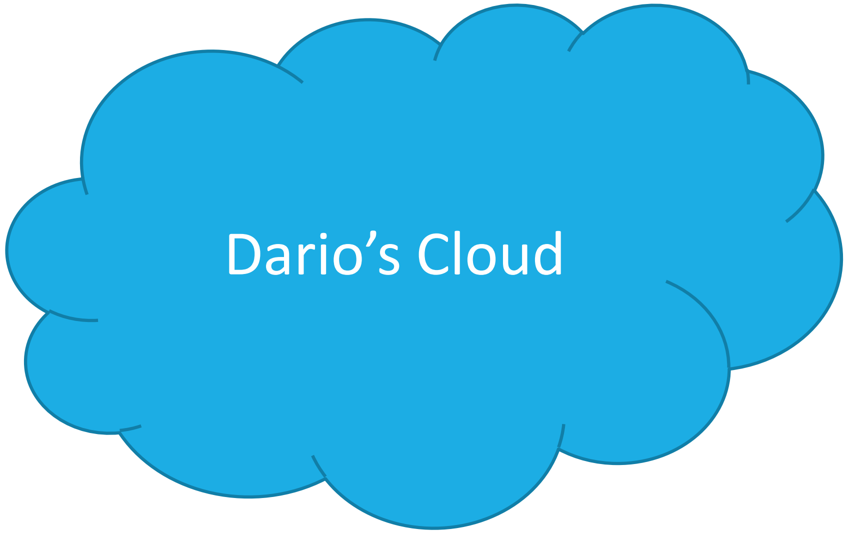
By Liam Tung | July 4, 2019 -- 12:24 GMT (05:24 PDT) | Topic: Networking

MORE FROM LIAM TUNG

Enterprise Software

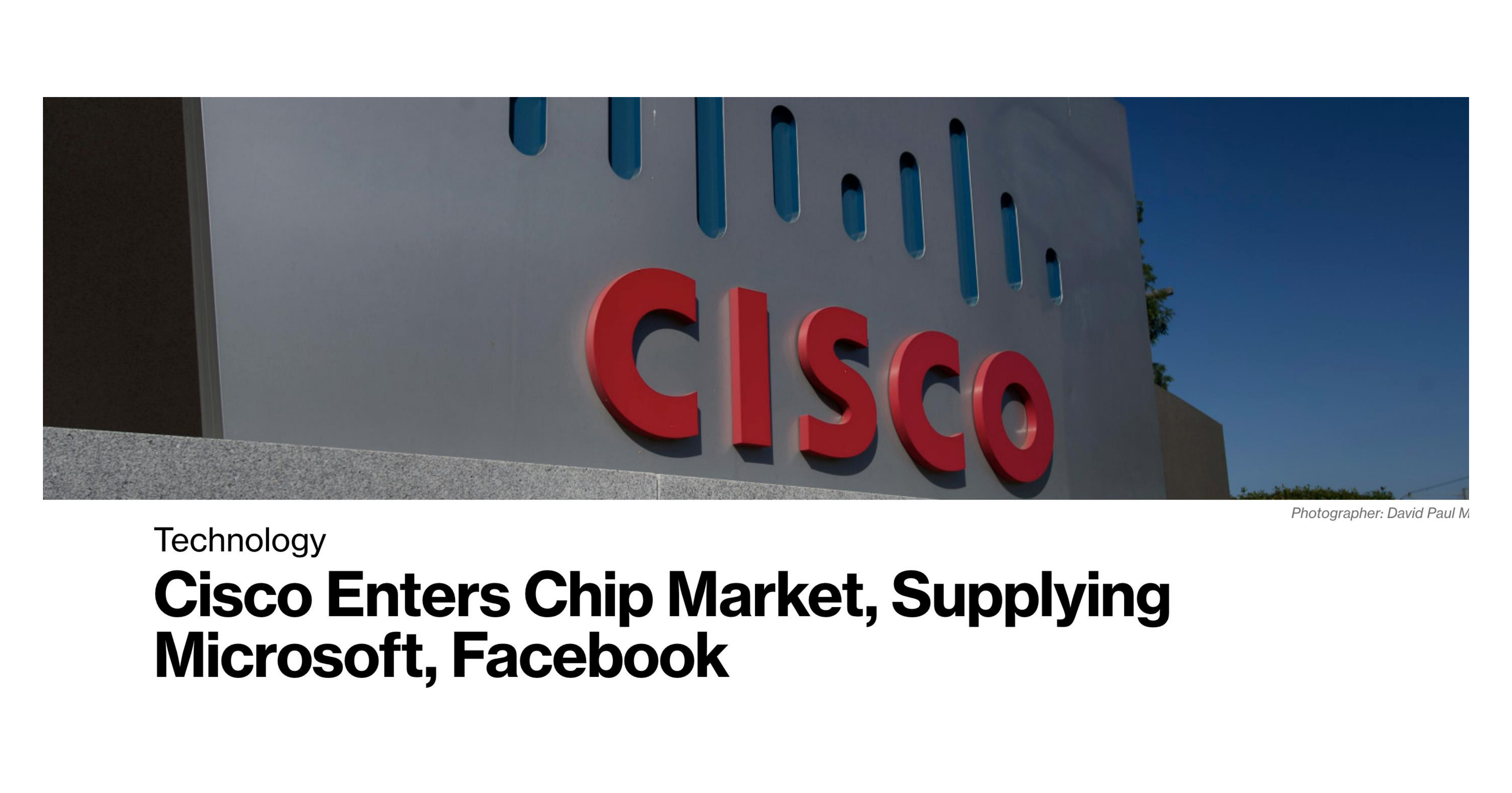
ODMs (Contracts, SLOs/SLAs, Testing, SDLC, etc. etc…)

TPS and the Cloud… What about Disclosures?



Cloud Solutions

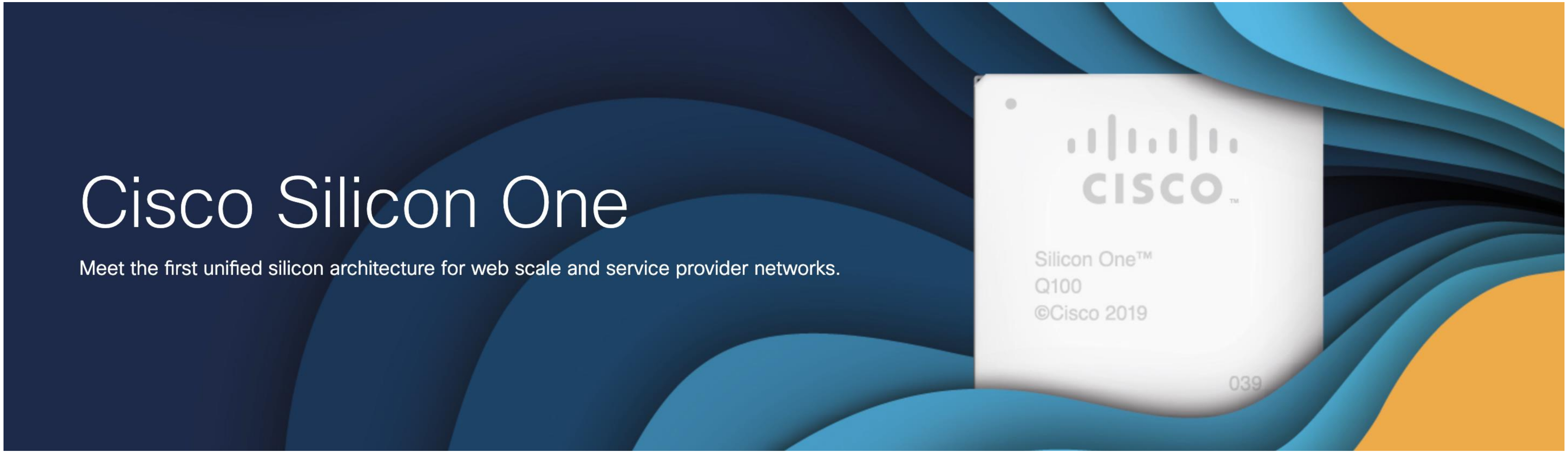
Powering the multicloud world.



Photographer: David Paul M

Technology

Cisco Enters Chip Market, Supplying Microsoft, Facebook



Cisco Silicon One

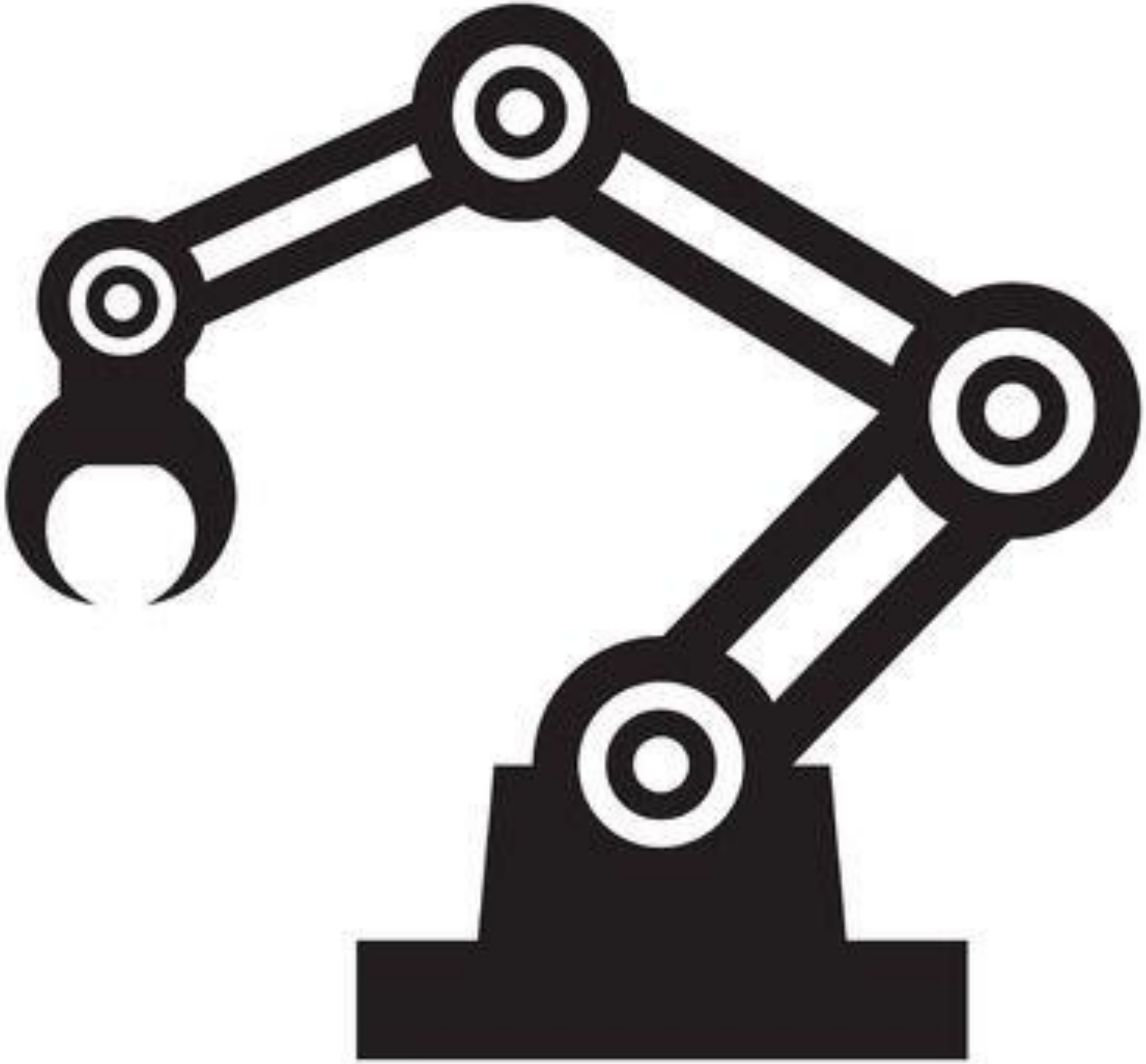
Meet the first unified silicon architecture for web scale and service provider networks.

Software Composition Analysis (SCA) Tools

- Policy creation and enforcement
- Some require IDE support
- Build infrastructure
- Reporting
- Language support
- Container Decomposition
- Performance

BMC/ILOs & Connected Power Supplies

Automated Vulnerability Disclosures



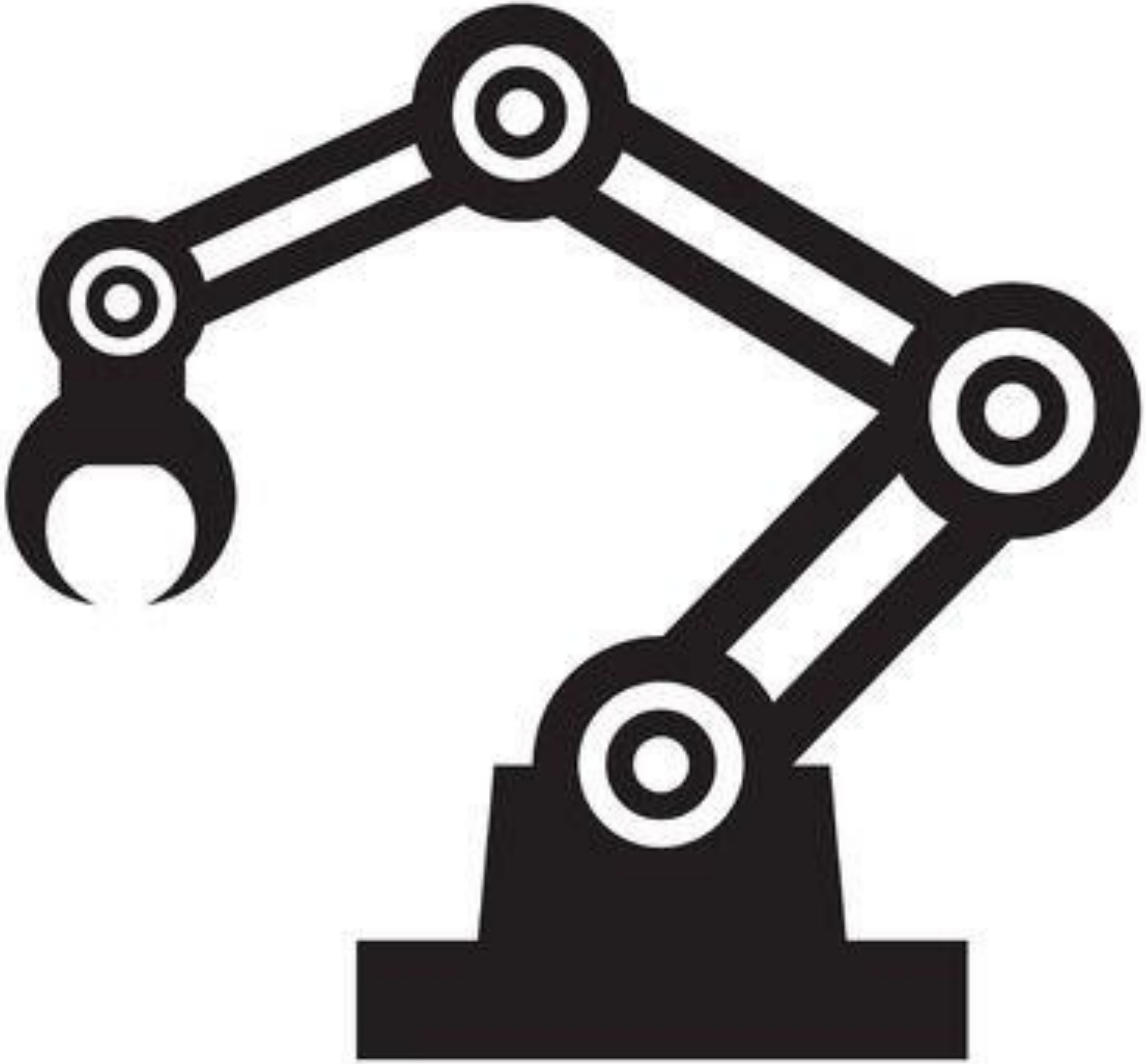
5000 CVEs per year

x 700 products (we have thousands of registered “projects” (a project can be a new major release or a new product)).

If 10% of them affect a product…
500 x 700 = 350,000 notifications / bugs

That’s 958 potential disclosures per day.
Even if you consolidate, there could be over 1,000 per week!

So… Automated Vulnerability Disclosures…



Triage?
CVSS from NVD?
Does it work for automation?

What if you develop Open Source? How do you disclose?

SNORT®

Contiv

Thank you!