AFRICA CYBER SECURITY CULTURE CONFERENCE

CHARL VAN DER WALT

Highlights of Orange Cyber Defense Research 2020
What Do We Need To Warn Our People About?

Orange
Cyberdefense

@charlvdwalt

"There is too much spending on the wrong things. Security strategies have been driven and sold on fear and compliance issues with spending on perceived rather than genuine threats"
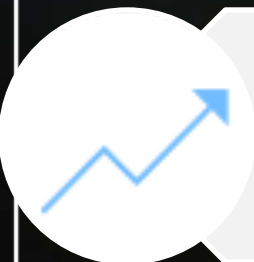
- Art Coviello, RSA Chief Exec

SEISMIC FORCES
The Threat emerges out of an political, economic, social, legal & regulatory context.

OBSERVE & ORIENT
These forces are like the weather – they have an enormous impact but we cannot control them. Our only choice here is to *observe* them and orient ourselves accordingly.

STRUCTURAL FACTORS
Systemic factors that create the enablers and constraints that shape the Threat and our Response.

INFLUENCE
We cannot control these Factors, but is within our means to *influence* them. Influencing the landscape is the most far-reaching way of addressing most Threats over the long run.
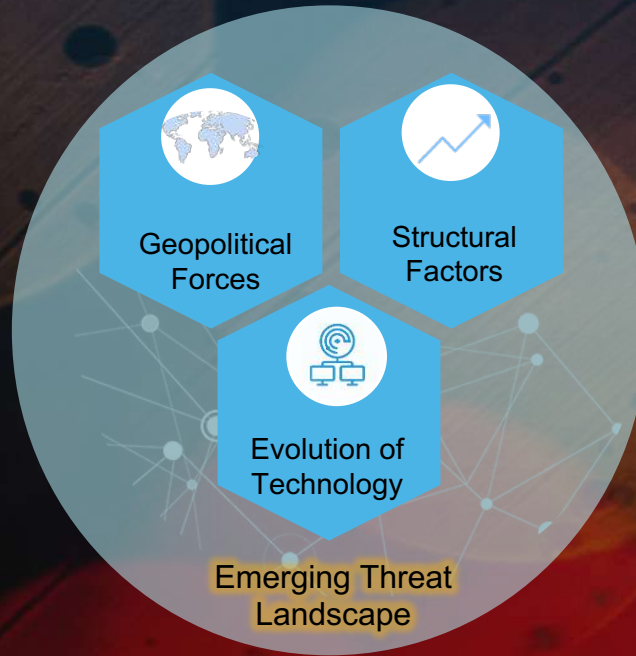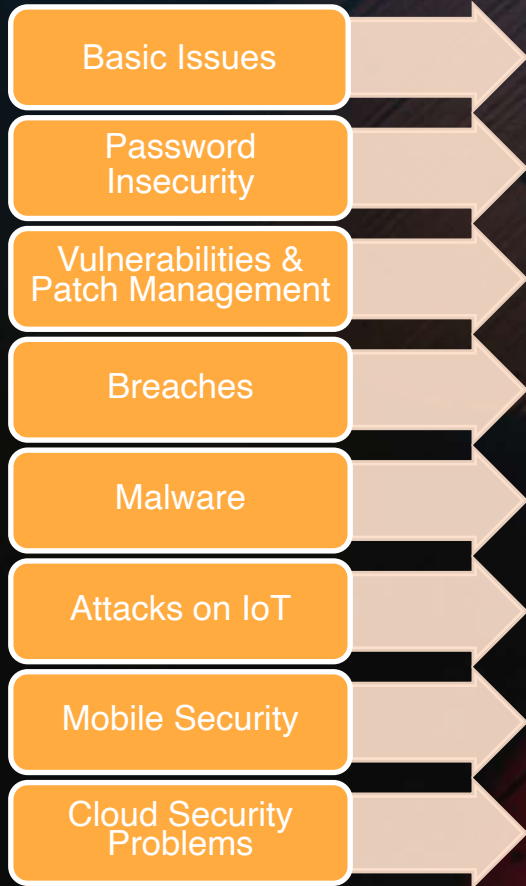
EVOLUTION OF TECHNOLOGY
As technology changes so does the Threat.

CONTROL
We can reduce the size of our attack surface and find and mitigate vulnerabilities, and since these efforts are under our control, it makes perfect sense for us to use best practices and do so.
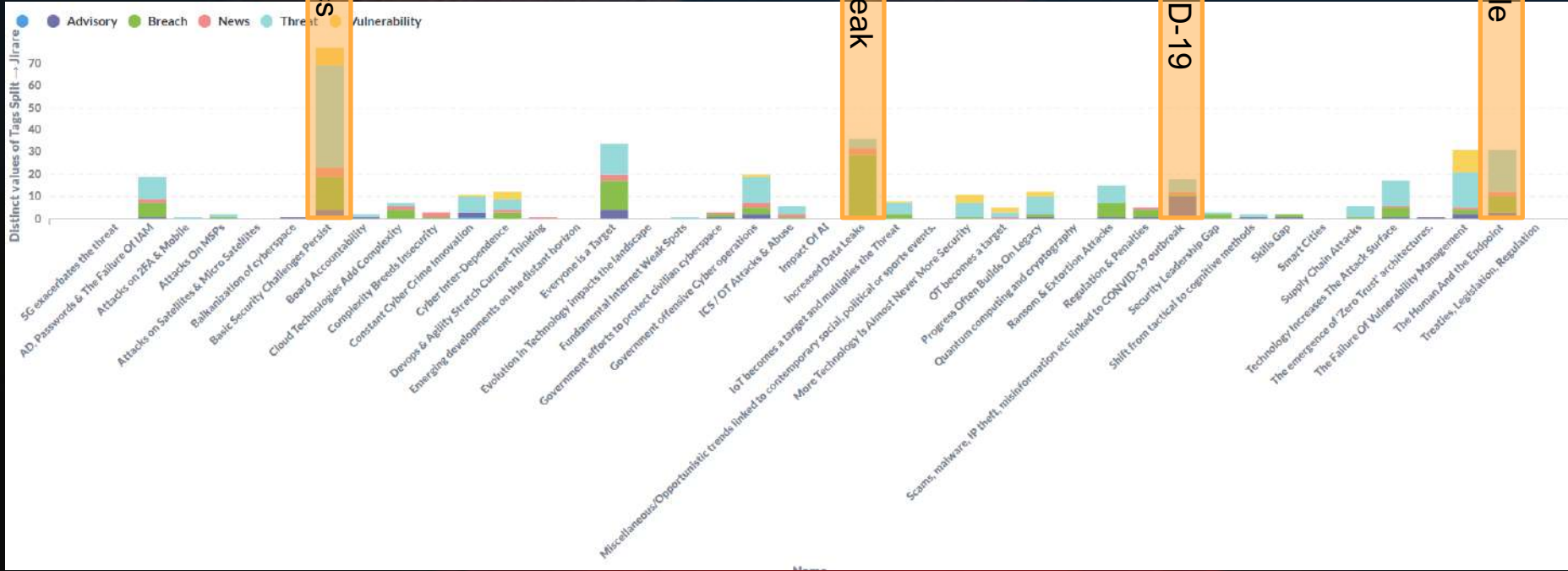
Pandemos

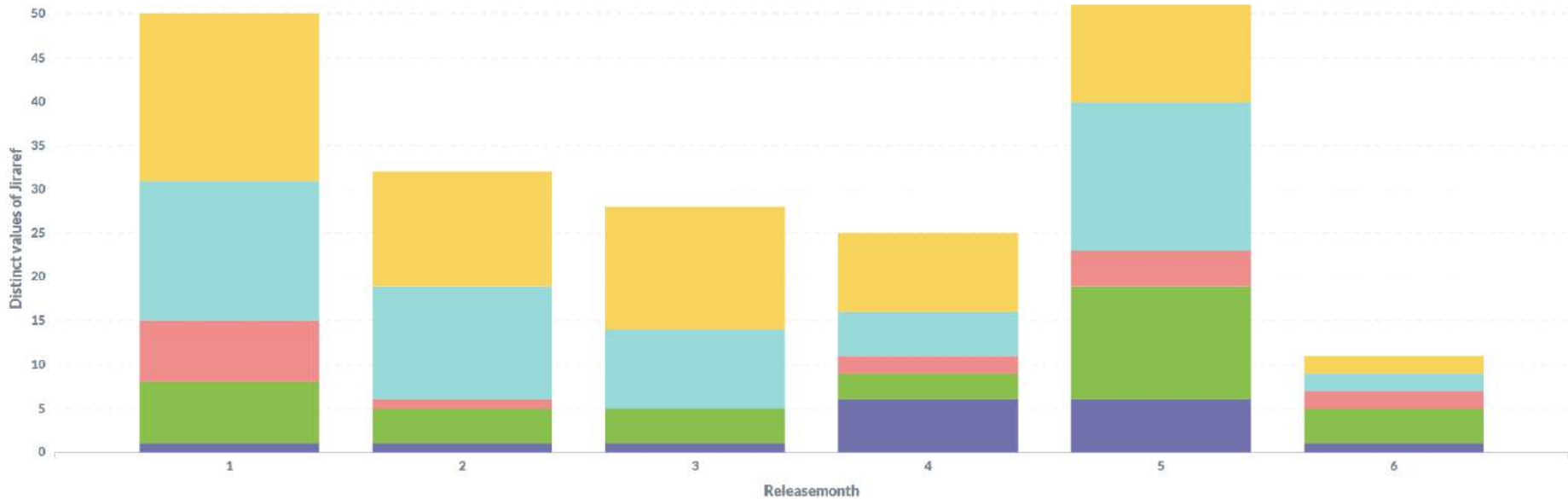**pan·dem·ic | \ pan-ˈde-mik**

○ an outbreak of a disease that occurs over a wide geographic area and affects an exceptionally high proportion of the population : a pandemic outbreak of a disease.

○ occurring over a wide geographic area and affecting an exceptionally high proportion of the population.

An emergency situation that forced us to…

Emerging threat model

Emerging threat model

Your employees are more vulnerable to social engineering and scams than normal.

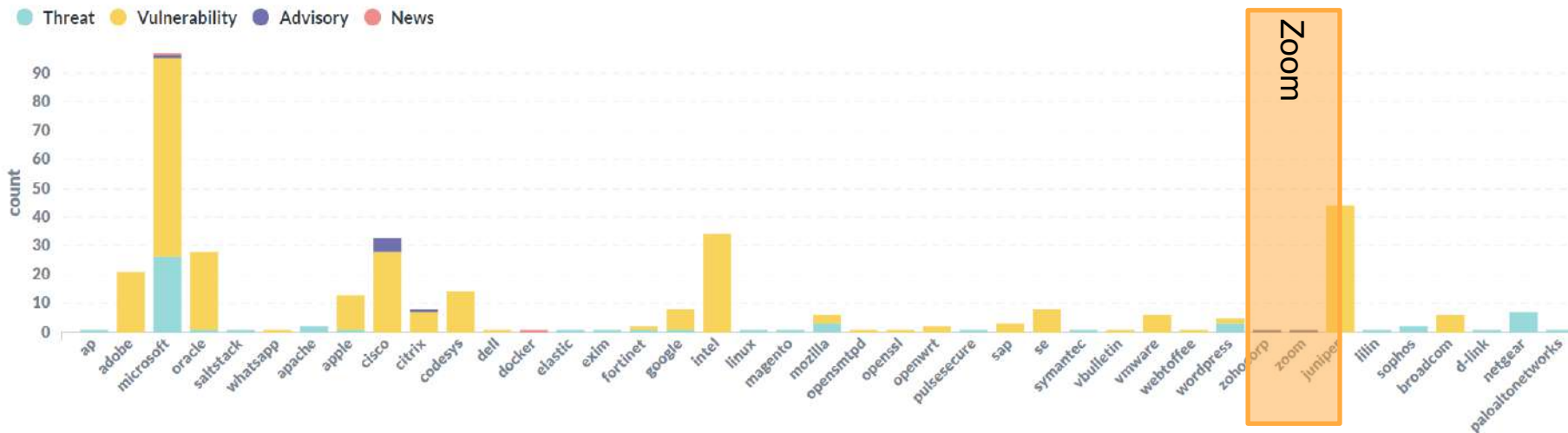You have less control and visibility over the IT systems you protect than you are used to.

Your users may be connecting from systems and environments that are fundamentally insecure or poorly configured.

You may have rushed to implement remote access systems without having the time to plan and execute as well as you would like.

You, your team and your providers may be operating with diminished capacity.

Guardian

Support The Guardian
Available for everyone, funded by readers

Contribute → | Subscribe →

Lifestyle | More ⌄

Opinion | Sport | Culture

News

Football | Tech | Business | Obituaries

Coronavirus | World | UK | Environment | Science | Global development

🕓 This article is more than **2 months old**

Zoom

'Zoom is malware': why experts worry about the video conferencing platform

The company has seen a 535% rise in daily traffic in the past month, but security researchers say the app is a 'privacy disaster'

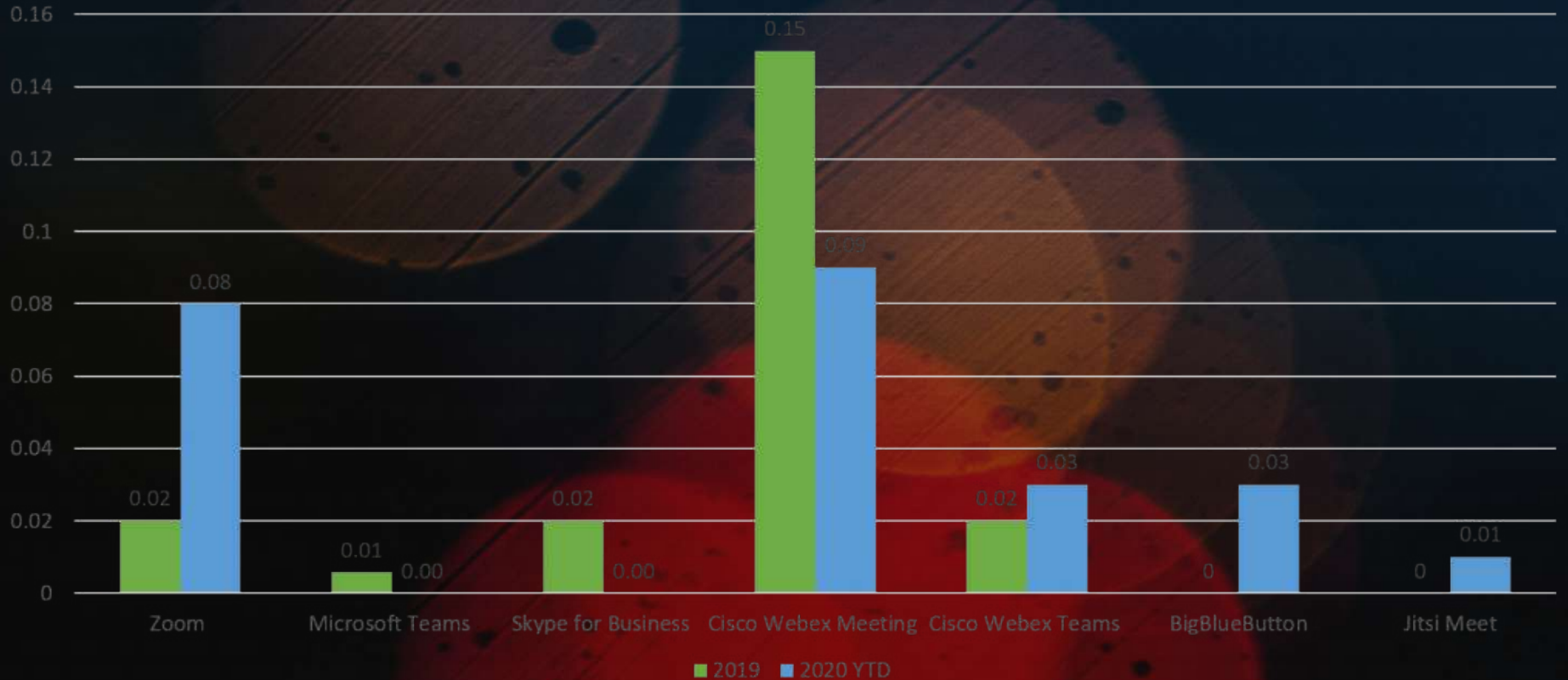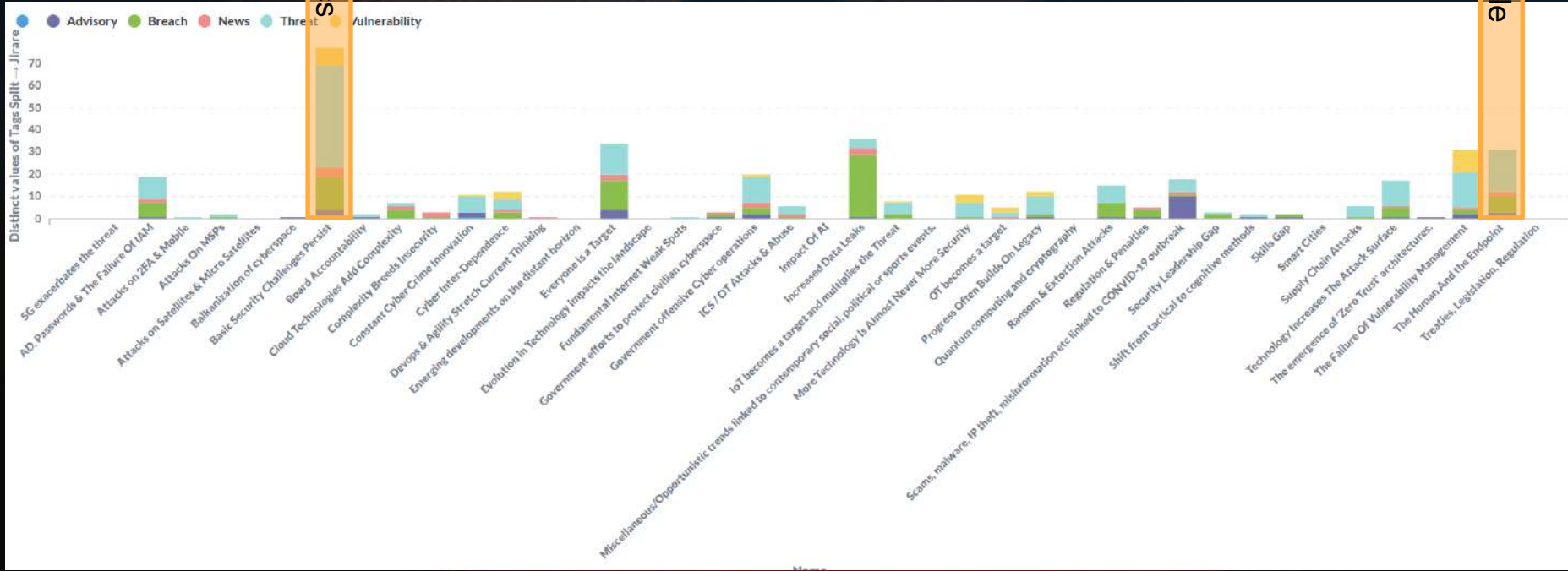**Kari Paul**

Thu 2 Apr 2020 15.23 BST

f 🐦 ✉

< 29,068

▲ Many, including the British prime minister, Boris Johnson, have been using Zoom during the coronavirus crisis.
Photograph: Olivier Douliery/AFP via Getty Images

Emerging threat model

Percentage of the total vulnerabilities reported in the NIST NVD

	Zoom	Microsoft Teams	Skype for Business	Cisco Webex Meeting	Cisco Webex Teams	BigBlueButton	Jitsi Meet
2019	0.02	0.01	0.02	0.15	0.02	0	0
2020 YTD	0.08	0.00	0.00	0.09	0.03	0.03	0.01

■ 2019 ■ 2020 YTD

Endless E2EE

Encryption	Zoom	Teams	Webex Meetings	Webex Teams	Google Meet	BlueJeans	Tixeo	BigBlueButton	Skype for Business	Jitsi Meet
Uses an appropriate encryption algorithm	■	■	■	■	?	■	■	■	■	■
Uses a strong encryption key	■	■	■	■	?	■	■	■	■	■
Data is encrypted in transit under normal use	■	■	■	■	■	■	■	■	■	■
Data stays encrypted in transit on provider servers	▨	?	▨	■	□	?	■	□	?	□
Voice, Video and Text are all encrypted	■	■	■	■	■	■	■	■	■	■
File transfers & session recordings are encrypted	■	■	■	■	■	■	■	▨	■	▨
Vendor technically can't decrypt the data at any point, even under regulatory pressure (full E2EE)	□	▨	▨	▨	□	□	▨	N/A	▨	N/A
Encryption implementation has withstood scrutiny over time	□	■	■	■	■	■	■	■	■	■

CIS Control Group Breakdown - Breach

basic	23.8%
foundational	41.3%
organisational	34.9%

63 TOTAL
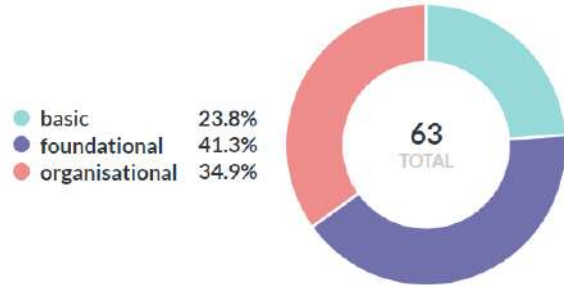
CIS Control Group Breakdown - Vulnerability

basic	84.42%
foundational	9.09%
organisational	6.49%

77 TOTAL
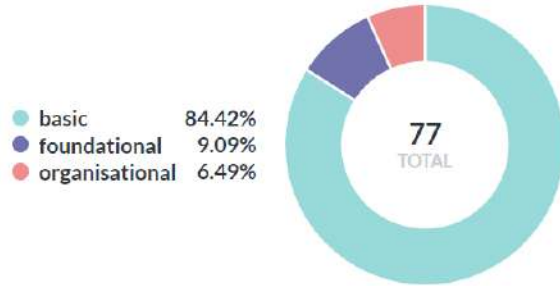
CIS Control Group Breakdown - Threat

basic	38.8%
foundational	33.9%
organisational	27.3%

121 TOTAL

4. Dataleak

summary:	**MGM Grand Leaked Details of 10.6 Million Guests Last Summer**
amount:	**10,600,000**
date:	**2020-2**
control_fail_count:	**1**

2020-1   2020-2   2020-3   2020-4   2020-6
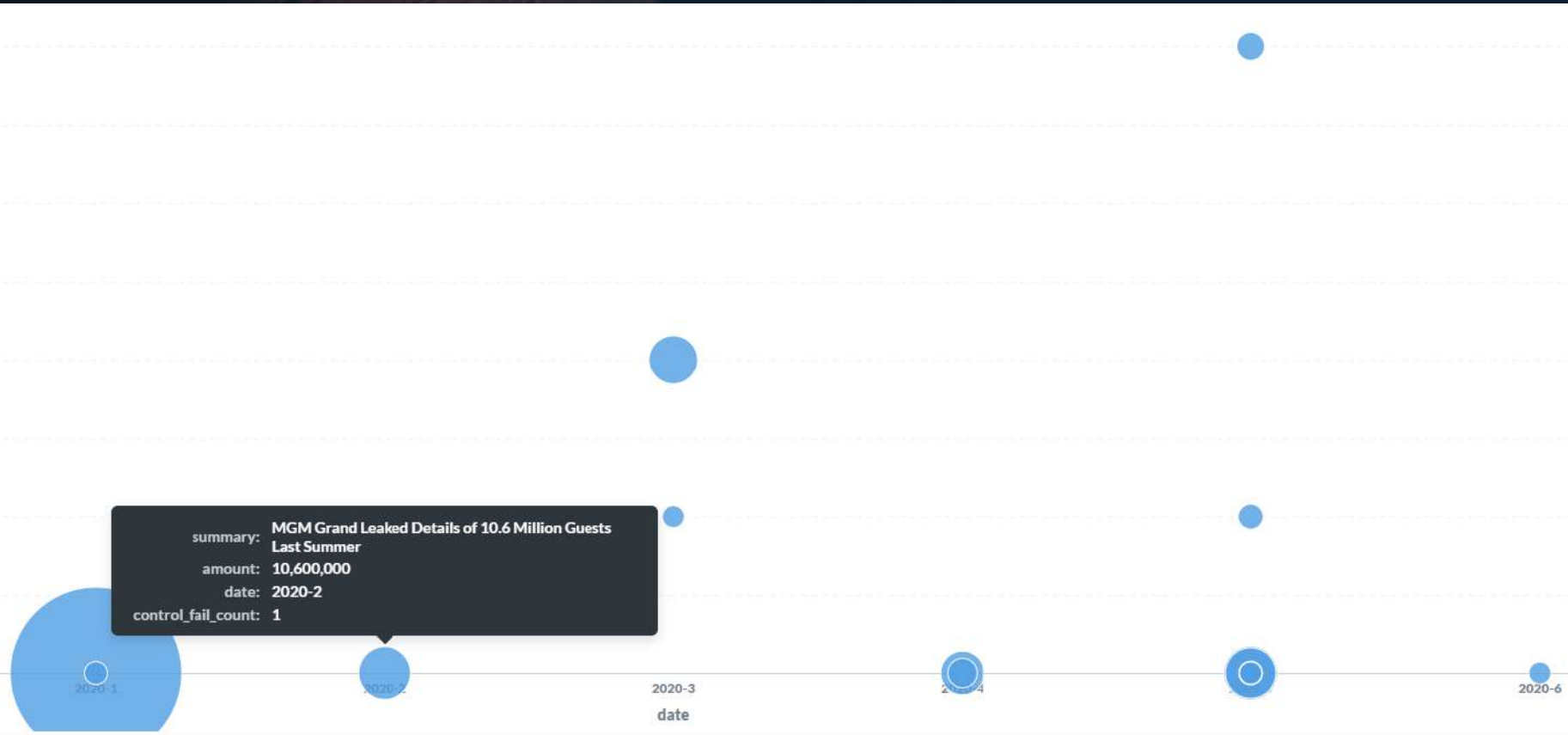
date

Geopolitical Forces

Structural Factors

Evolution of Technology

Emerging Threat Landscape
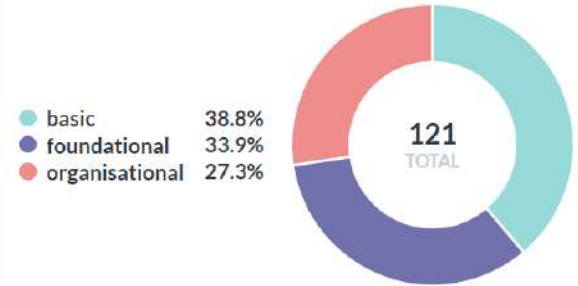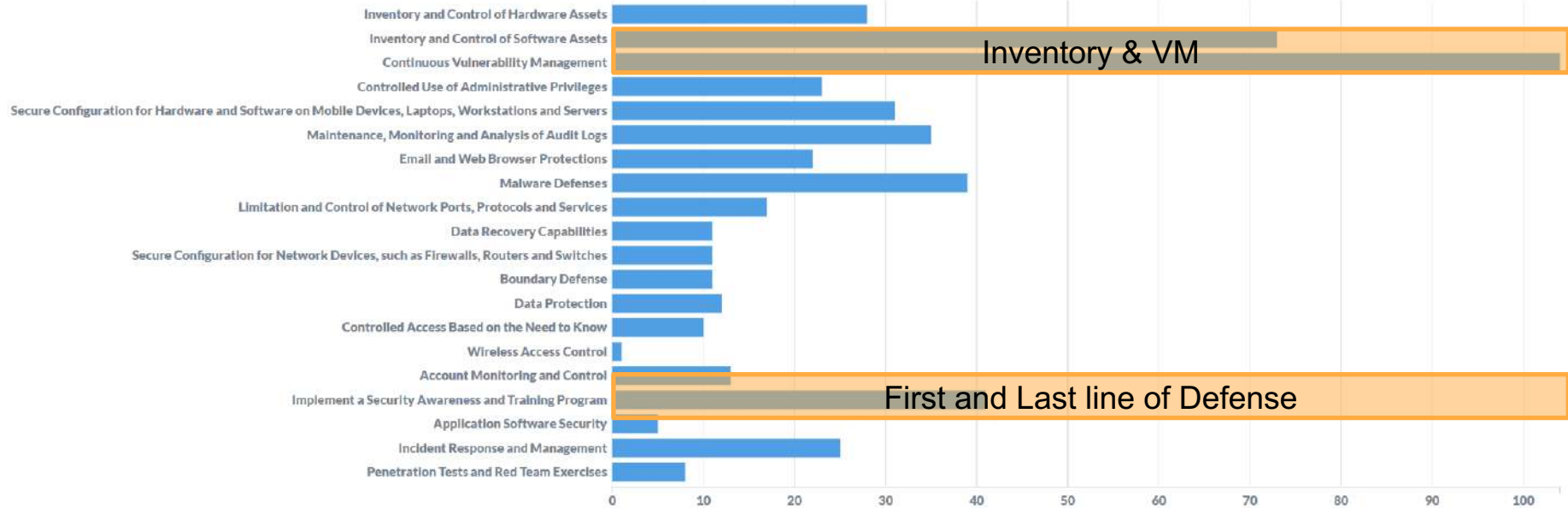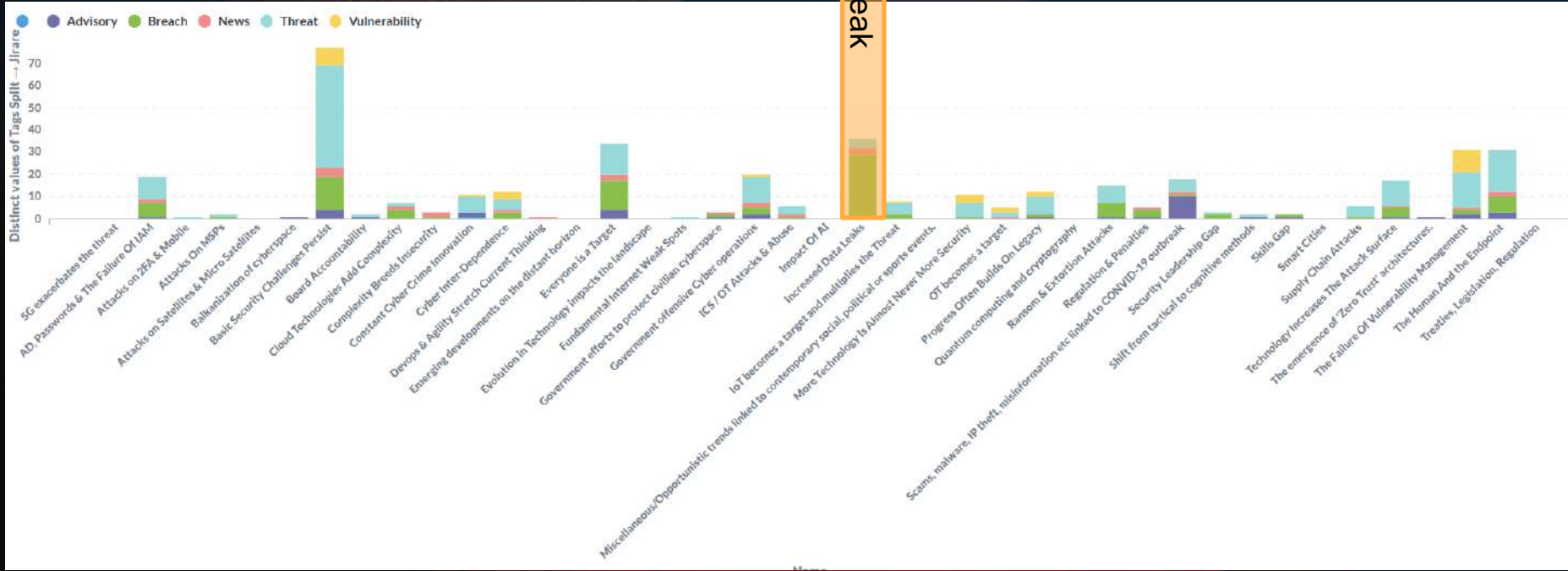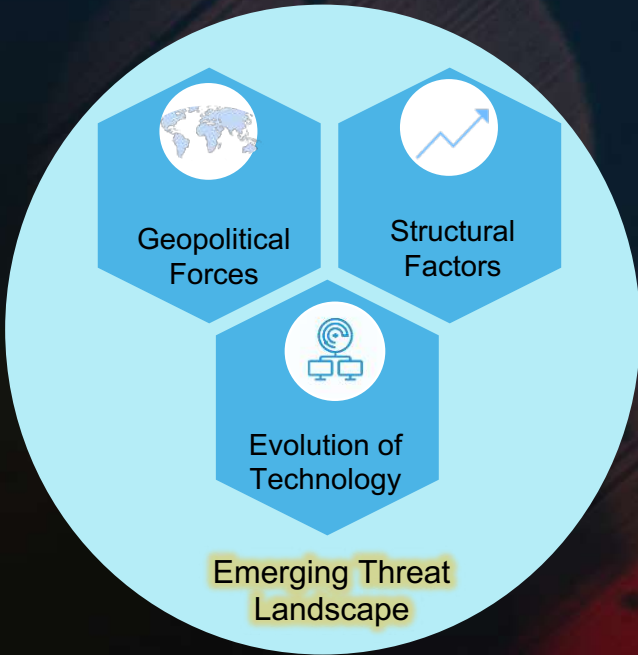
You can outrun some of the bulls some of the time, but you can't outrun all of the bulls all of the time.

We live and work in an inter-connected, inter-dependent world.

We must think beyond the single-dimensional risk we are addressing for our business and consider the impact of the secondary and tertiary effects on the broader economy when breaches and compromises happen.

Recognize that what's bad for society generally, is bad for us as businesses too.

Thanks!

Any questions?

You can find me at @charlvdwalt & charl@ocd.link