Cloud Security

Jornada TIC UPC 2021 - Memorial Víctor Huerta

A bots i barralls...

Jordi Guijarro Olivares

Cybersecurity Innovation Director - i2CAT
Barcelona cloudadmins.org

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

i2cat
THE INTERNET RESEARCH CENTER

Never stop designing the digital future

i2CAT.net

tecnio catalonia | ACCIÓ Generalitat de Catalunya

Institució CERCA Centres de Recerca de Catalunya

Cloud Computing Vision

"If computers of the kind I have advocated become the computers of the future, then computing may some day be organized as a public utility, just as the telephone system is a public utility ... The computer utility could become the basis of a new and important industry."

-- John McCarthy, MIT Centennial, 1961

Cloud Computing Vision

"If computers of the kind I have advocated become the computers of the future, then computing may some day be organized as a public utility, just as the telephone system is a public utility ... The computer utility could become the basis of a new and important industry."

-- John McCarthy, MIT Centennial, 1961

- computing == fungible utility!
- limitations exist: API lock-in, hardware dependence, latency, privacy, security ...


OVHcloud

https://socprime.com/blog/what-is-bgp-and-how-its-failure-took-facebook-down/

TECH

Amazon Outage Disrupts Lives, Surprising People About Their Cloud Dependency

When Amazon Web Services was interrupted, some vacuum cleaners, light switches and cat-food dispensers stopped working

Big tech firms are investing in data centers as they compete for the $214 billion cloud computing market. WSJ explains what cloud computing is, why big tech is betting big on future contracts. (Video from 11/19/19)

By Sarah E. Needleman

MOST POPULAR NEWS

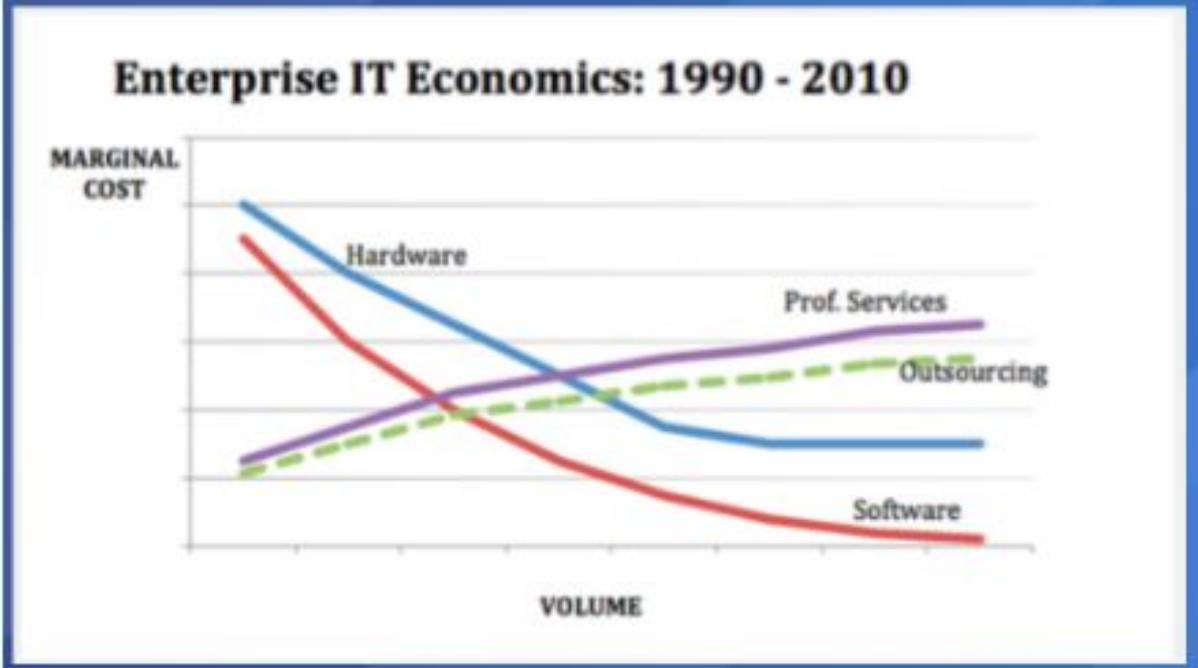
1. Southern California's Container-Ship Backlog Moves Farther Out to Sea
2. Sky-High Vaccination Rates, Zero Taxes Create Boomtown
3. Meet the Kidd Who Goes Toe to Toe With Warren Buffett
4. Rupert Murdoch Buys $200 Million Montana Ranch From the Koch Family
5. U.S. Inflation Hits 39-Year High

MOST POPULAR OPINION

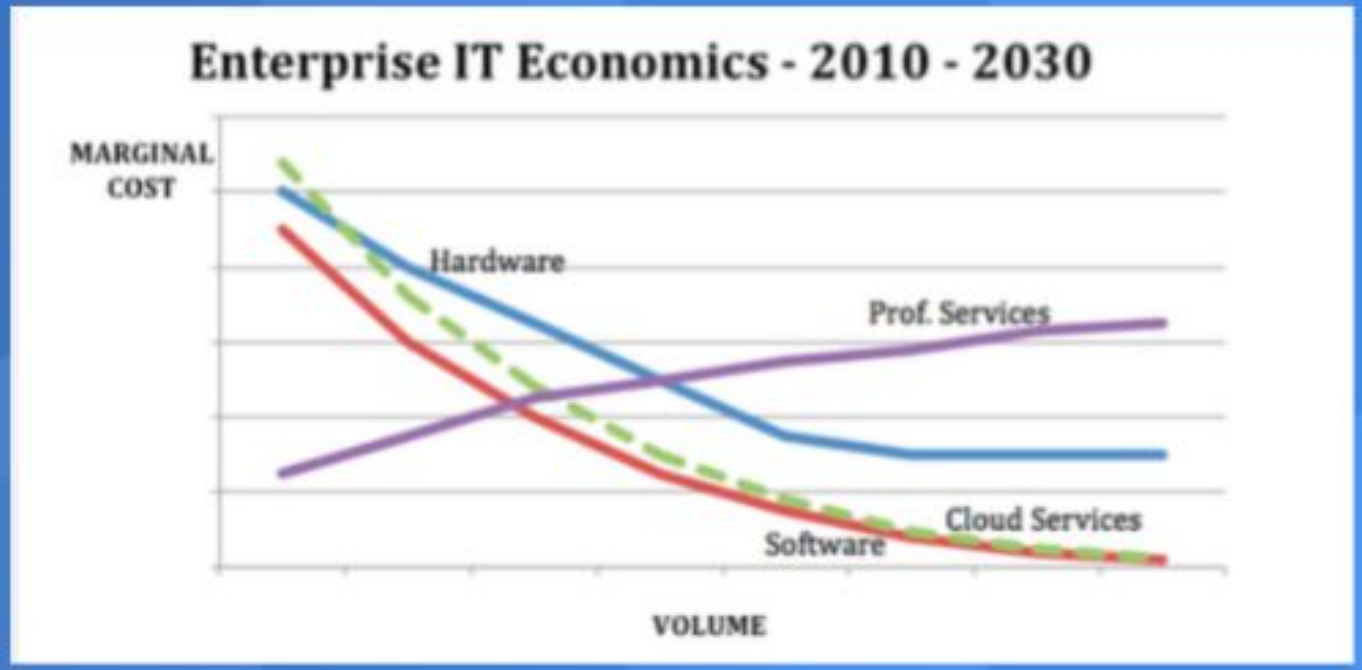
1. Opinion: Kamala Harris Needs to Get

Cloud Economics - Where's the Margin?

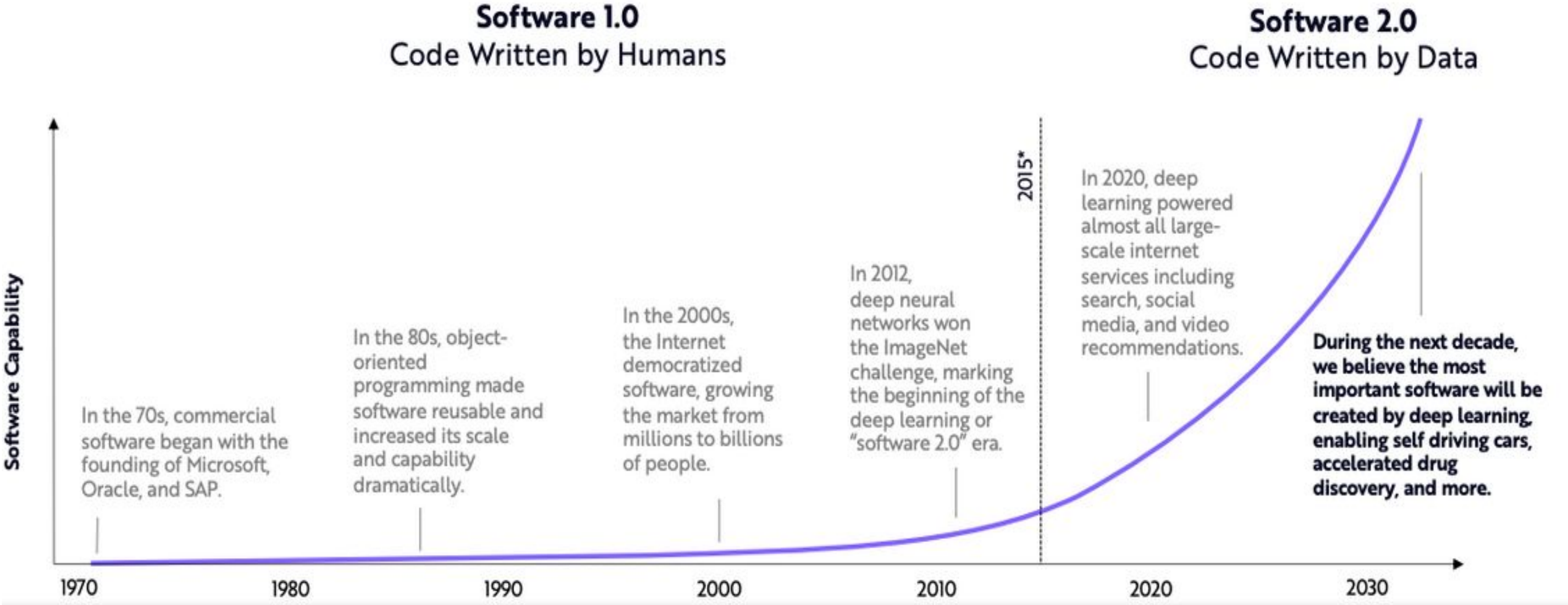
Pre-Cloud Era



Post-Cloud Era

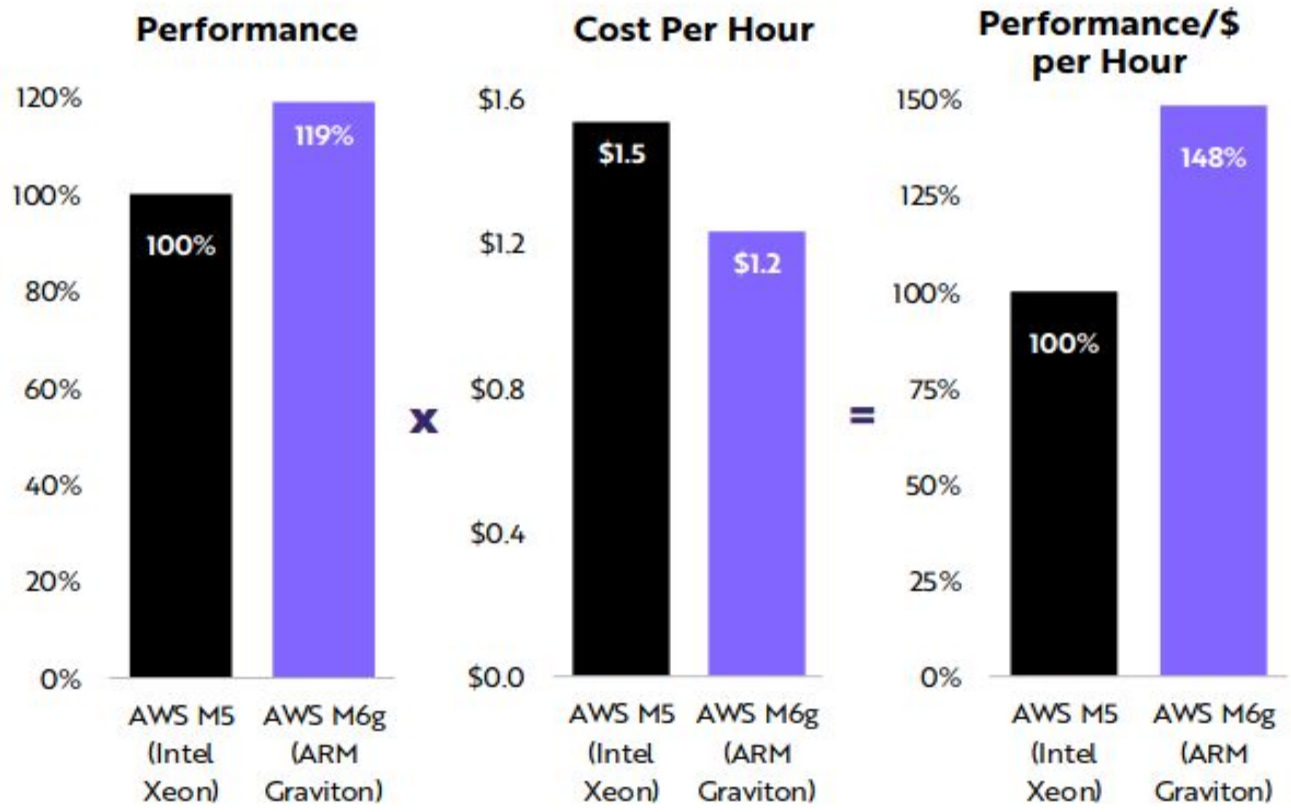


Source: Wikibon


Software 1.0
Code Written by Humans
Software 2.0
Code Written by Data
Software Capability
In the 70s, commercial software began with the founding of Microsoft, Oracle, and SAP.
In the 80s, object-oriented programming made software reusable and increased its scale and capability dramatically.
In the 2000s, the Internet democratized software, growing the market from millions to billions of people.
In 2012, deep neural networks won the ImageNet challenge, marking the beginning of the deep learning or "software 2.0" era.
2015*
In 2020, deep learning powered almost all large-scale internet services including search, social media, and video recommendations.
During the next decade, we believe the most important software will be created by deep learning, enabling self driving cars, accelerated drug discovery, and more.
1970
1980
1990
2000
2010
2020
2030

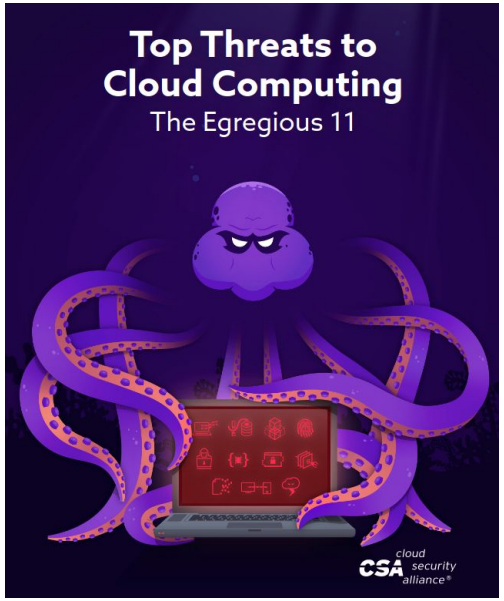
ARM Could Become The New Standard In The Cloud

- The public cloud, the default platform for deploying new applications, generated $140 billion in global revenues in 2020.
- Amazon Web Services (AWS)—the largest public cloud provider in the world—launched the Graviton 2 ARM CPU in 2020, reducing its need to purchase chips from Intel and AMD.
- AWS Graviton 2 is cheaper and faster than Intel CPUs, offering 48% higher performance per dollar.
- In the future, AWS is likely to migrate most of its servers to ARM based processors.



Forecasts are inherently limited and cannot be relied upon. | For informational purposes only and should not be considered investment advice, or a recommendation to buy, sell or hold any particular security. Note for Third Chart: Time is implied. The math is: (119/1.2)/(100/1.5)-1. Source: ARK Investment Management LLC, 2020 based on data sourced from: "Global Cloud Services Market Q2 2020." Canalys, www.canalys.com/newsroom/worldwide-cloud-infrastructure-services-Q2-2020, Michael Larabel. "Benchmarking Amazon's Graviton2 Performance With 64 Neoverse N1 Cores Against Intel Xeon, AMD EPYC." Phoronix, May 2020, www.phoronix.com/scan.php?page=article&item=amazon-graviton2-benchmarks&num=12, Daly, Donald J., and Donald J. Daly. "Economics 2: EC2." Amazon, CGA Canada Publications, 1987, aws.amazon.com/ec2/pricing/.

Top Threats to Cloud Computing



1. Data Breaches (1)
2. Misconfiguration and Inadequate Change Control
3. Lack of Cloud Security Architecture and Strategy
4. Insufficient Identity, Credential, Access and Key Management
5. Account Hijacking (5)
6. Insider Threat (6)
7. Insecure Interfaces and APIs (3)
8. Weak Control Plane
9. Metastructure and Applistructure Failures
10. Limited Cloud Usage Visibility
11. Abuse and Nefarious Use of Cloud Services (10)

https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/

Investment in cloud security must match cloud spend

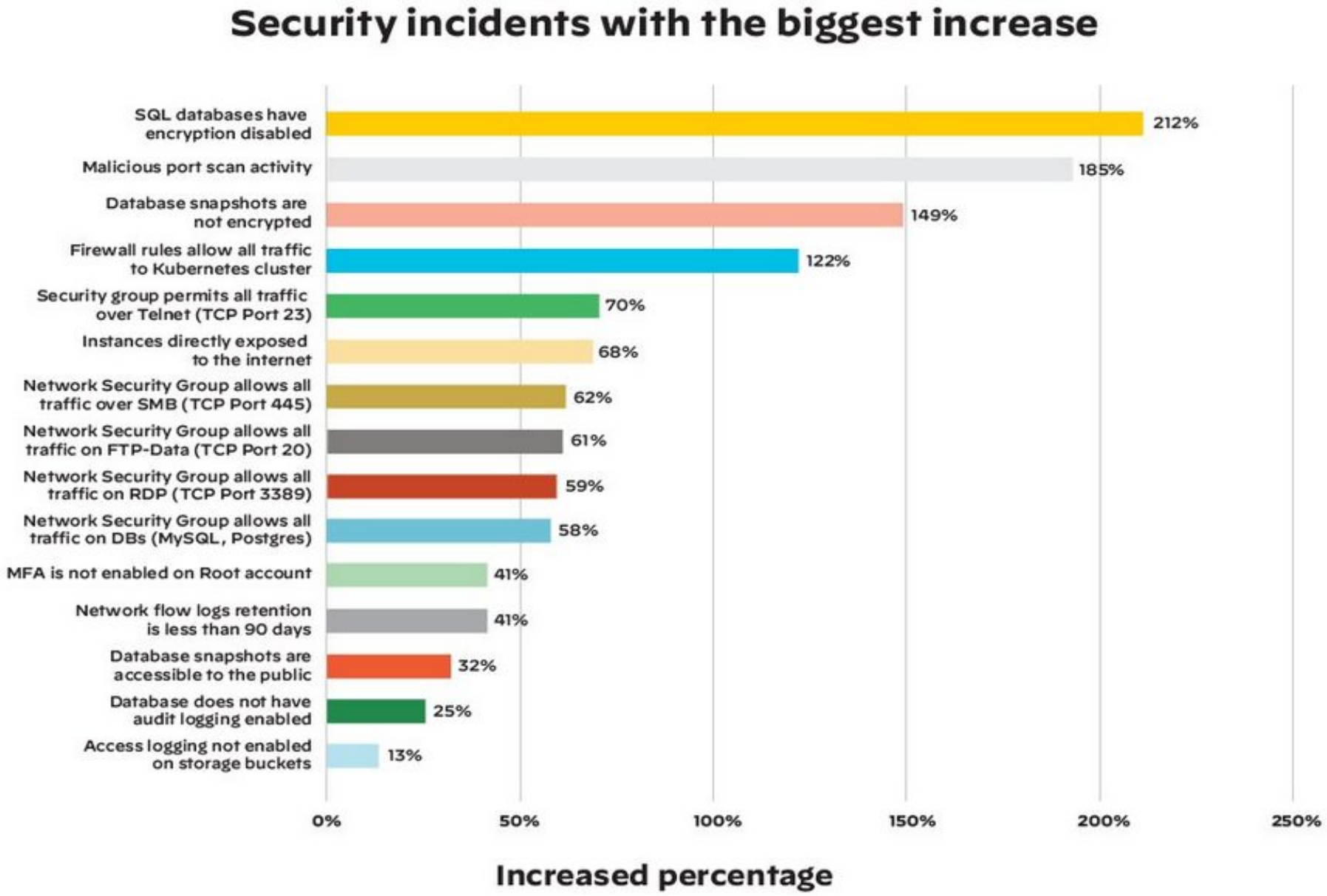
In the early days of the COVID-19 pandemic, there was a rapid uptick in demand for cloud services. Utilizing data pulled from our global array of sensors, our elite cloud threat researchers found a correlation: Organizations globally increased their cloud workloads by more than 20%, leading to an explosion of security incidents. Our research shows that cloud security programs for organizations globally are still in their infancy when it comes to security automation (i.e., DevSecOps and shift left). We concluded that rapid cloud scale and complexity without automated security controls embedded across the entire development pipeline are a toxic combination.

Matthew Chiodi
Chief Security Officer, Public Cloud

https://www.paloaltonetworks.com/prisma/unit42-cloud-threat-research-1h21

Figure 1: Cloud growth and security incidents

https://www.paloaltonetworks.com/prisma/unit42-cloud-threat-research-1h21



https://www.paloaltonetworks.com/prisma/unit42-cloud-threat-research-1h21

COVID-19 and Data Security

Businesses are favoring cloud storage due to its reliability, availability, and scalability. Our research shows that 64% of data in the cloud contains sensitive information (e.g., PII, intellectual property, healthcare and financial data). Within that 64% subset, 69% contains PII, and 34% contains intellectual property (see figure 8).

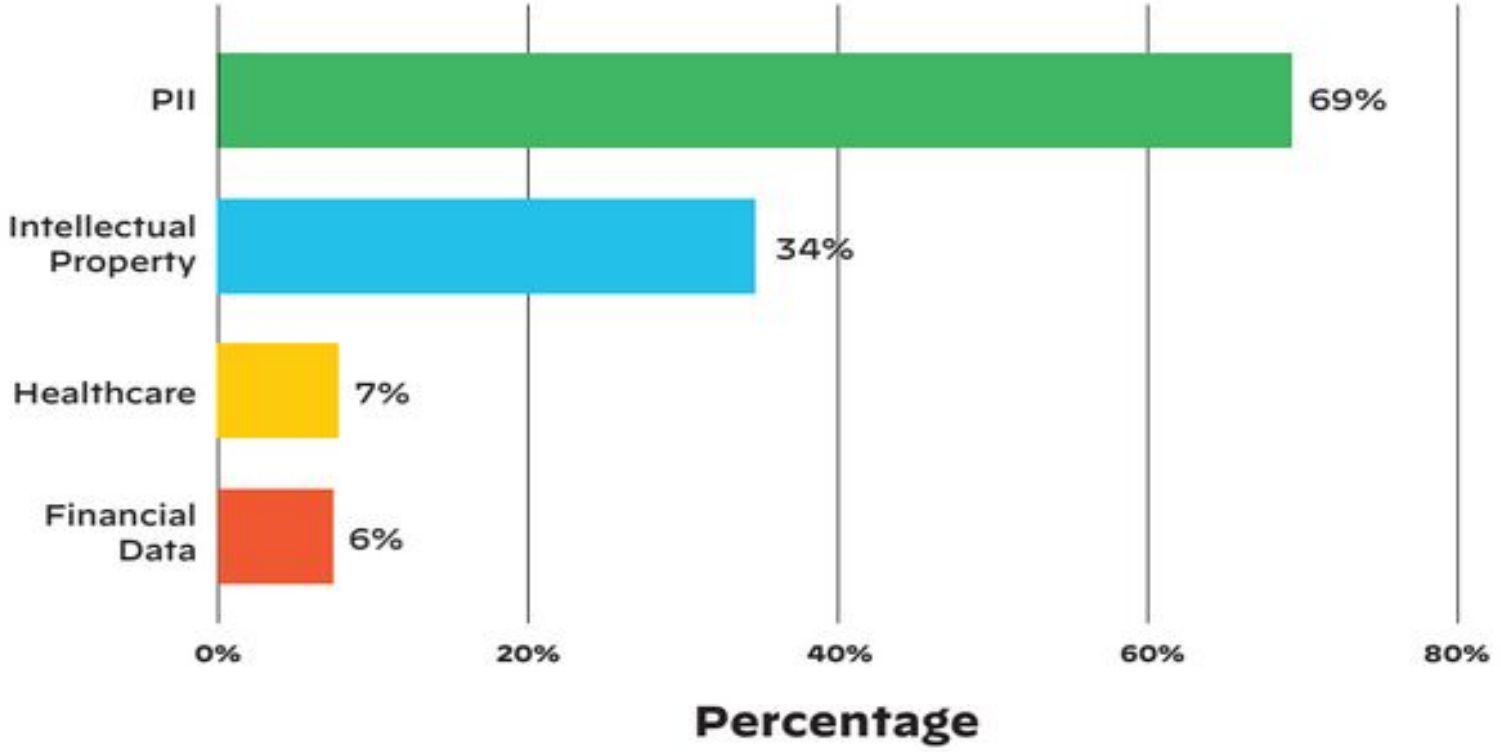


Figure 8: Prevalence of sensitive data types among sensitive data stored in clouds

https://www.paloaltonetworks.com/prisma/unit42-cloud-threat-research-1h21

Mining Trends and Market Events

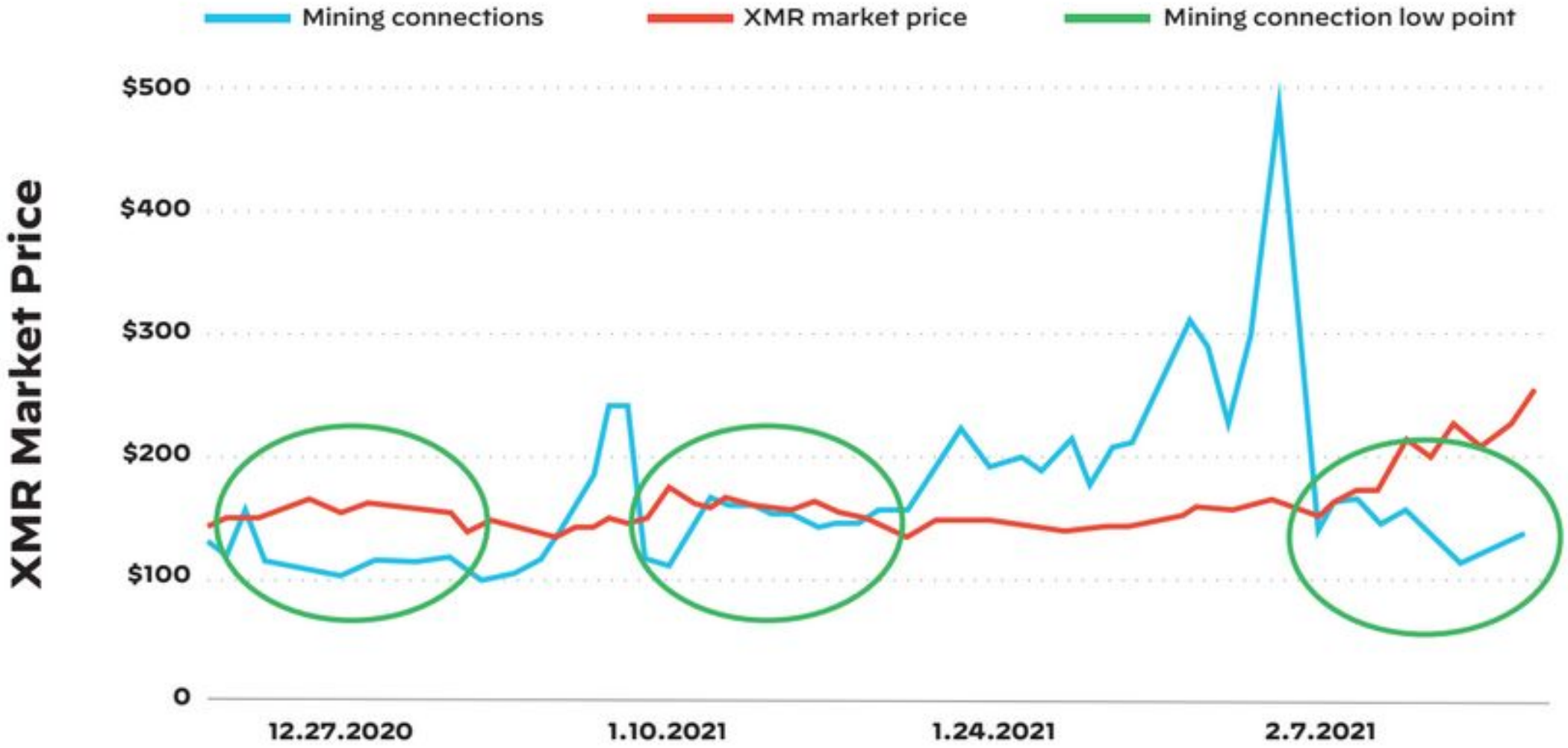


Figure 10: Comparison of cryptomining connections and XMR price

https://www.paloaltonetworks.com/prisma/unit42-cloud-threat-research-1h21

Cloud Governance

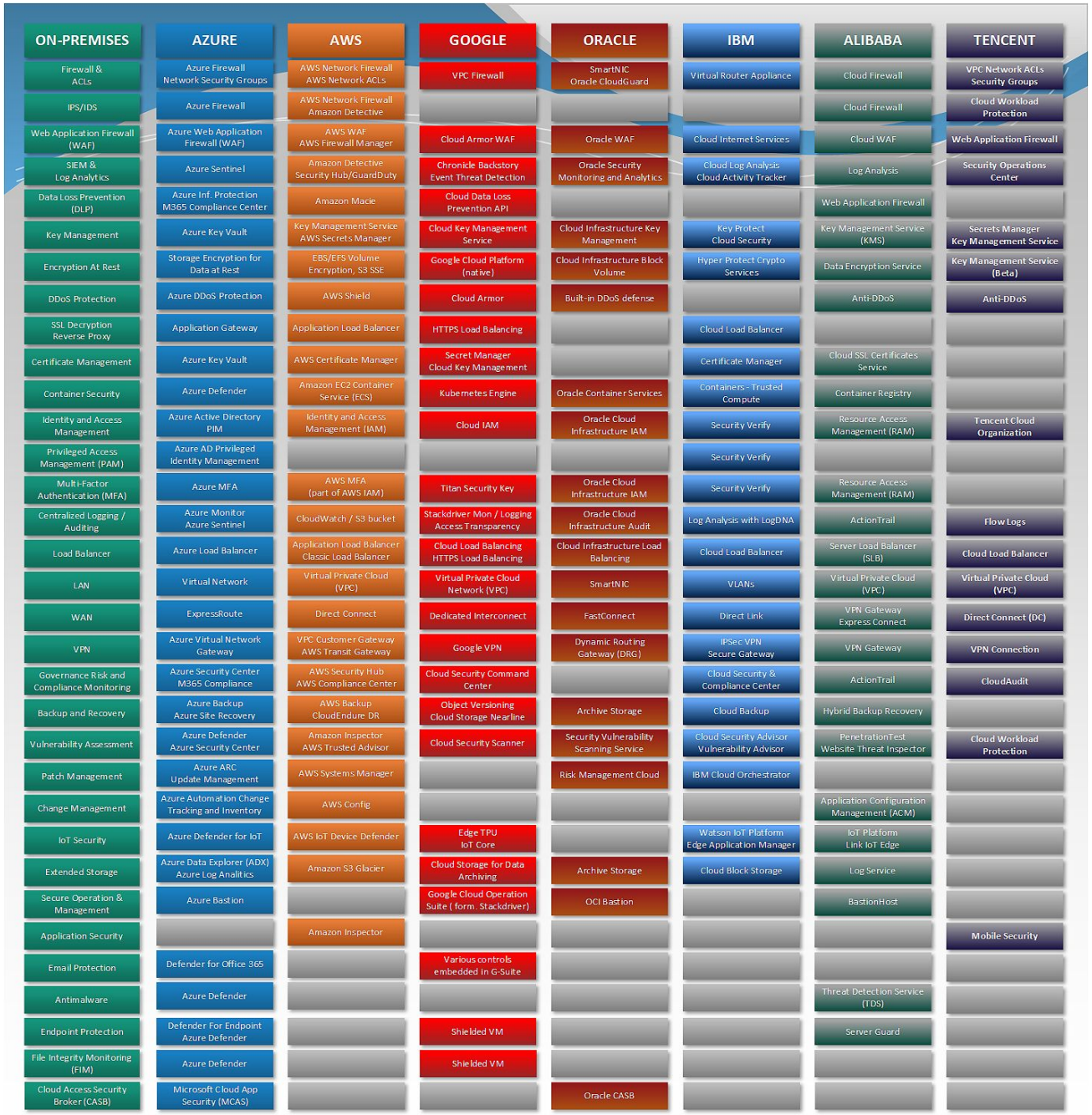
Shared Responsibility Model

Cloud Security Mapping

MANAGED SENTINEL
A BlueVoyant Company

Mapping of On-Premises Security Controls Versus Services Offered by Major Cloud Providers

i2cat



Mapping of On-Premises Security Controls vs Major Cloud Providers Version 5.0 July 2021 © Adrian Grigorof, Marius Mocanu
High Definition available at http://www.managedsentinel.com

https://www.managedsentinel.com/mapping-of-on-premises-security-controls-versus-services-offered-by-major-cloud-providers/

Shared Responsibility Model

CIS Center for Internet Security®
Creating Confidence in the Connected World.

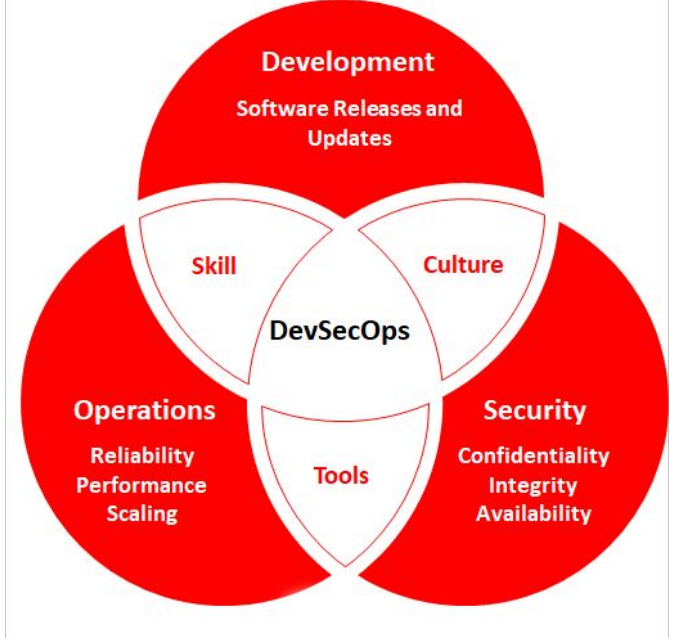
CIS Benchmarks™

With our global community of cybersecurity experts, we've developed CIS Benchmarks: more than 100 configuration guidelines across 25+ vendor product families to safeguard systems against today's evolving cyber threats.

Join a Community

https://www.cisecurity.org/cis-benchmarks/

DevSecOps is a MUST!



vulnerability in Apache Log4j which affects many major internet-facing services. Log4j is a Java logging package that’s used in many popular services and utilities. With a CVSS score of 10, this vulnerability (CVE-2021-44228) impacts Apache Log4j versions 2.0-beta9 to 2.14.1 according to Apache.

Log4Shell

Critical Log4j Vulnerability

net Players

Google Cloud

IDENTITY & SECURITY

Google Cloud Armor WAF rule to help mitigate CVE-2021-44228 Apache Log4j vulnerability

README.md

Logout4Shell

cybereason

Description

However, enabling these system property requires access to the vulnerable servers as well as a restart. The Cybereason research team has developed the following code that *exploits* the same vulnerability and the payload therein forces the logger to reconfigure itself with the vulnerable setting disabled - this effectively blocks any further attempt to exploit Log4Shell on this server.

This Proof of Concept is based on @tangxiaofeng7's tangxiaofeng7/apache-log4j-poc

i2cat

CLOUDFLARE The Cloudflare Blog

Thanks for being here

Email Addres

Product News | Speed & Reliability | Security | Serverless | Zero Trust | Developers | Deep Dive

Inside the Log4j2 vulnerability (CVE-2021-44228)

10/12/2021

SOFT LAW & CLOUD PROVIDERS

International standards (ISOs) would be part of the Soft Law that, although not mandatory, establishes the principles of quality in the provision of cloud services by the companies that comply with them.

The most relevant ISO in the provision of cloud services would be:

ISO 27001: For information security management systems. It focuses on risk assessment and the application of essential controls for their mitigation and elimination.

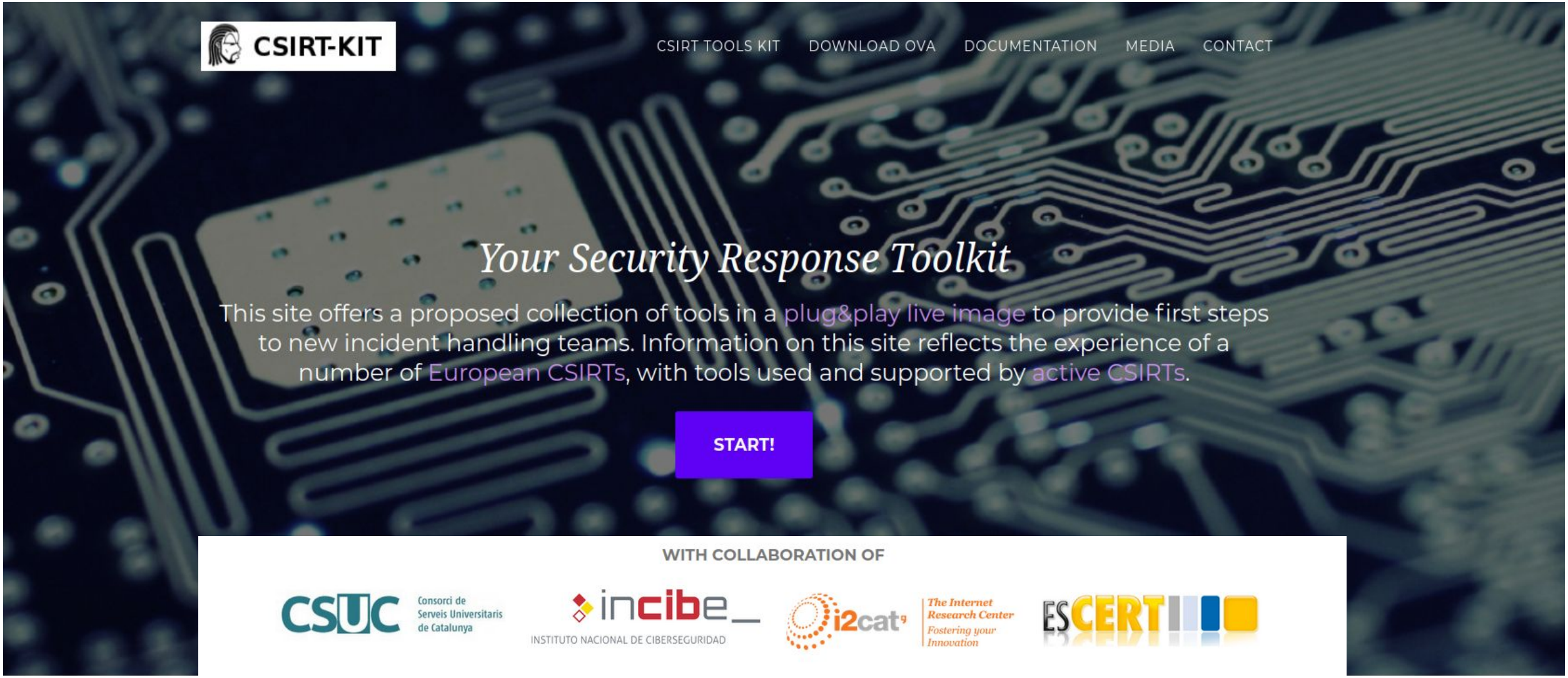
ISO 27002: Good practice guide that describes the control objectives and recommended controls in relation to information security.

ISO / IEC 27017: Security controls for cloud services. It focuses on aspects of responsibility, elimination and return of assets at the end of the contract, operations and administrative procedures, ...

ISO / IEC 27018: For the control of data protection in Cloud services.

It is also important to highlight the National Institute of Standards and Technology Framework (NIST) and the Cloud Security Alliance (CSA) which is a voluntary tool intended to help organizations identify and manage the risk of privacy to build innovative products and services, protecting the privacy of people.

https://csirt-kit.org



AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Trending TOPIC: Sovereign Clouds

Gartner Says Four Trends Are Shaping the Future of Public Cloud

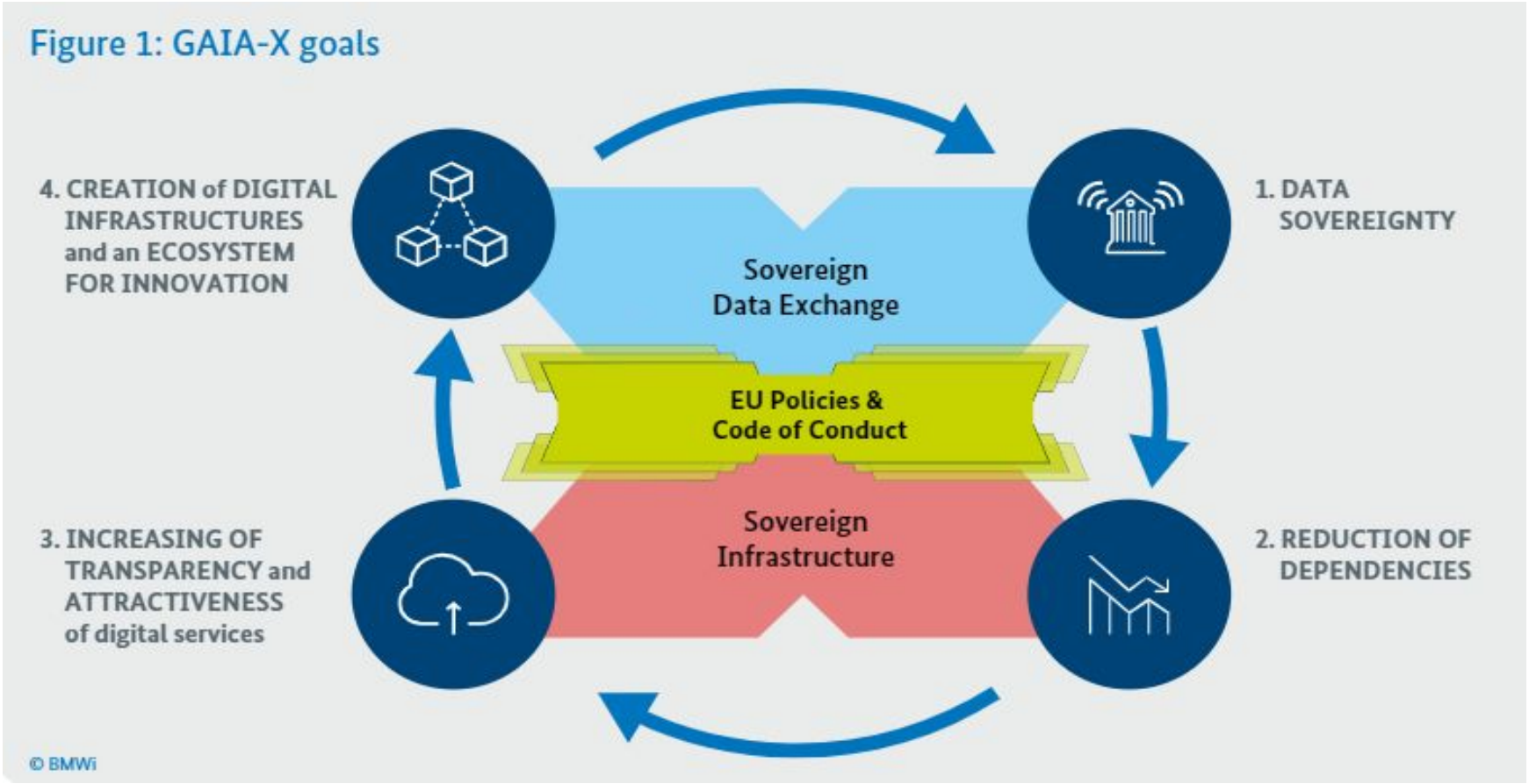
Regional Cloud Ecosystems

Growing geopolitical regulatory fragmentation, protectionism and industry compliance are driving the creation of new regional and vertical cloud ecosystems and data services. Companies in the financial and public sectors are looking to reduce critical lock-in and single points of failure with their cloud providers outside of their country.

Regions not able to create or sustain their own platform ecosystems will have no choice but to leverage the platforms created in other regions and resort to legislation and regulation to maintain some level of control and sovereignty. Concerns among politicians, academia and tech providers in these regions are increasing, leading to initiatives such as GAIA-X in European countries.

Sovereign Data Driven Clouds: Gaia-X initiative

https://gaia-x.eu/



https://scs.community/


i2cat
THE INTERNET
RESEARCH CENTER

Thanks! Q&A

@jordiguijarro

i2CAT.net

Never stop designing the digital future

Generalitat de Catalunya
Government of Catalonia

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Ajuntament de Barcelona

UNIVERSITAT RAMON LLULL

upf. Universitat Pompeu Fabra Barcelona

UNIVERSITAT ROVIRA I VIRGILI

tecnio catalonia

ACCIÓ Generalitat de Catalunya

orange

cellnex driving telecom connectivity

JUNIPER NETWORKS

cisco

vodafone

FUJITSU

MEDIAPRO

parlem telecom

Institució CERCA Centres de Recerca de Catalunya

BONUS SLIDE

Cloud Admins Barcelona

Barcelona, España
300 miembros · Grupo público
Organizado por **George S.** y otras 4 personas

Compartir:

CloudAdmins.org Inicio Equipo Eventos Telegram Libro Cybercantera Sponsors

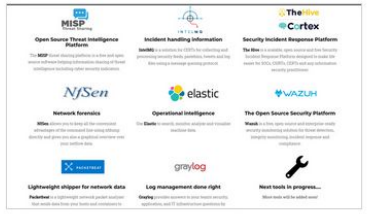
Newsletter | Subscríbete y recibe GRATIS el primer capítulo del libro Devops y Seguridad Cloud. Recibe los últimos artículos y eventos, directamente en tu buzón

Suscríbete →

Recording 🚀🚀 Cyberops e-TechDay Barcelona 24/11/21 16h CEST

The Cloudadmins TechDays (now turned virtual due to the COVID-19 pandemic) are educational and networking events organized by...

Jordi Guijarro
1 Dic. 2021 · 1 min de lectura



🚀🚀 Cyberops e-TechDay

Recording 🚀🚀 Workflow

🚀e-TechDay OpenNebula