

Winds of Change

Solorigate: Winds of change. Underlying causes and implications of the SolarWinds attack.

Charl van der Walt

 [charlvdwalt](#)

MARKETS

[see all](#) →

▼ DOW	30,814.26	-177.26	-0.57%
▼ S&P 500	3,768.25	-27.29	-0.72%
▼ NASDAQ	12,998.50	-114.14	-0.87%

FEATURED



Track the Covid economy

See how drastically everyday life in America has changed since the start of the pandemic.

LATEST

Janet Yellen is heading to Congress. The stakes have never been higher

Goldman Sachs posts impressive earnings thanks to Wall Street's strength

Hundreds of health care facilities were hit by ransomware last year amid pandemic

Massive SolarWinds hack has big businesses on high alert

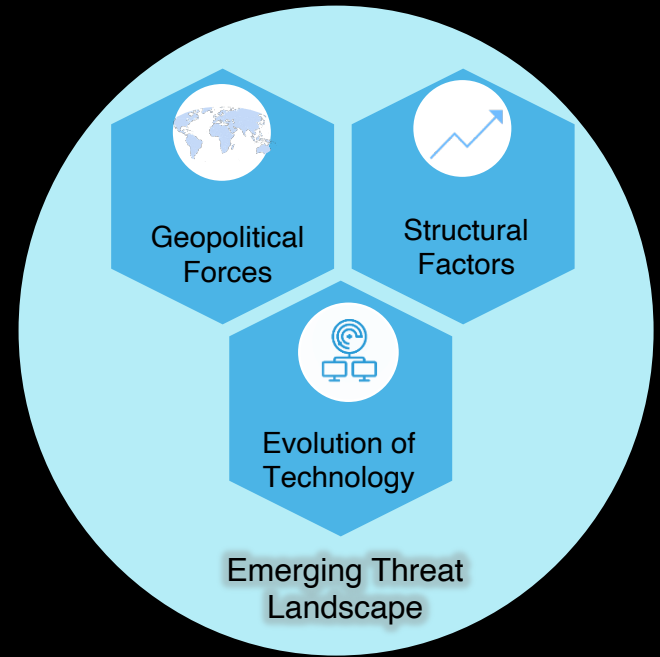


By [Rishi Iyengar](#), [CNN Business](#)

Updated 1514 GMT (2314 HKT) December 19, 2020



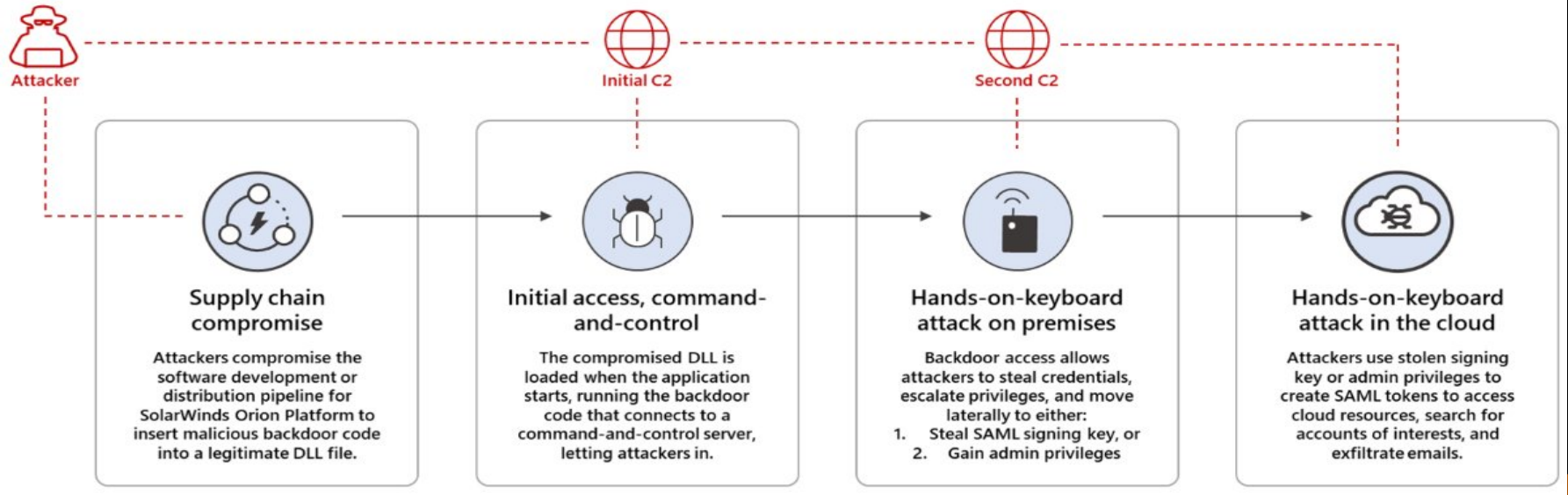
SPRINTER/GETTY IMAGES



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

SOLORIGATE ATTACK

High-level end-to-end attack chain

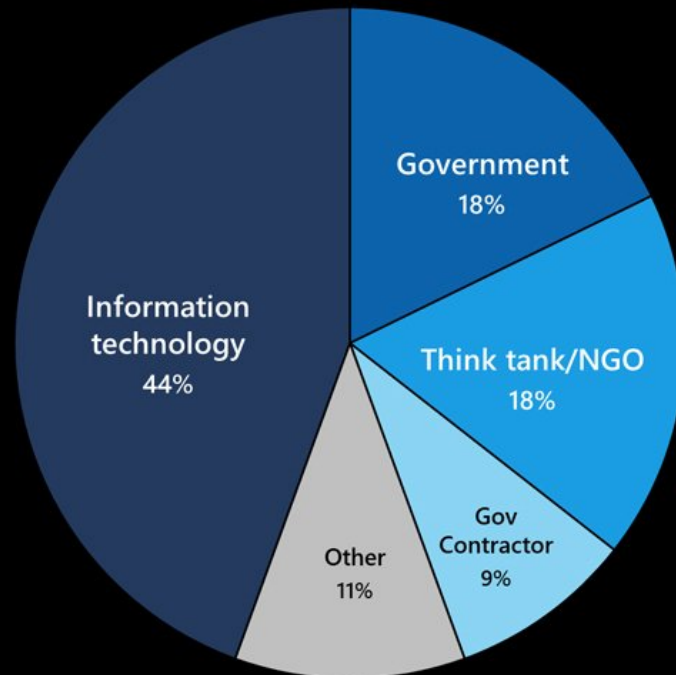




Recent cyberattack victims by sector

44% of targets were in the **information technology** sector, including software firms, IT services and equipment providers.

US government targets are involved in **finance, national security, health, and telecommunications**, while the government contractor victims primarily support **defense and national security** organizations.

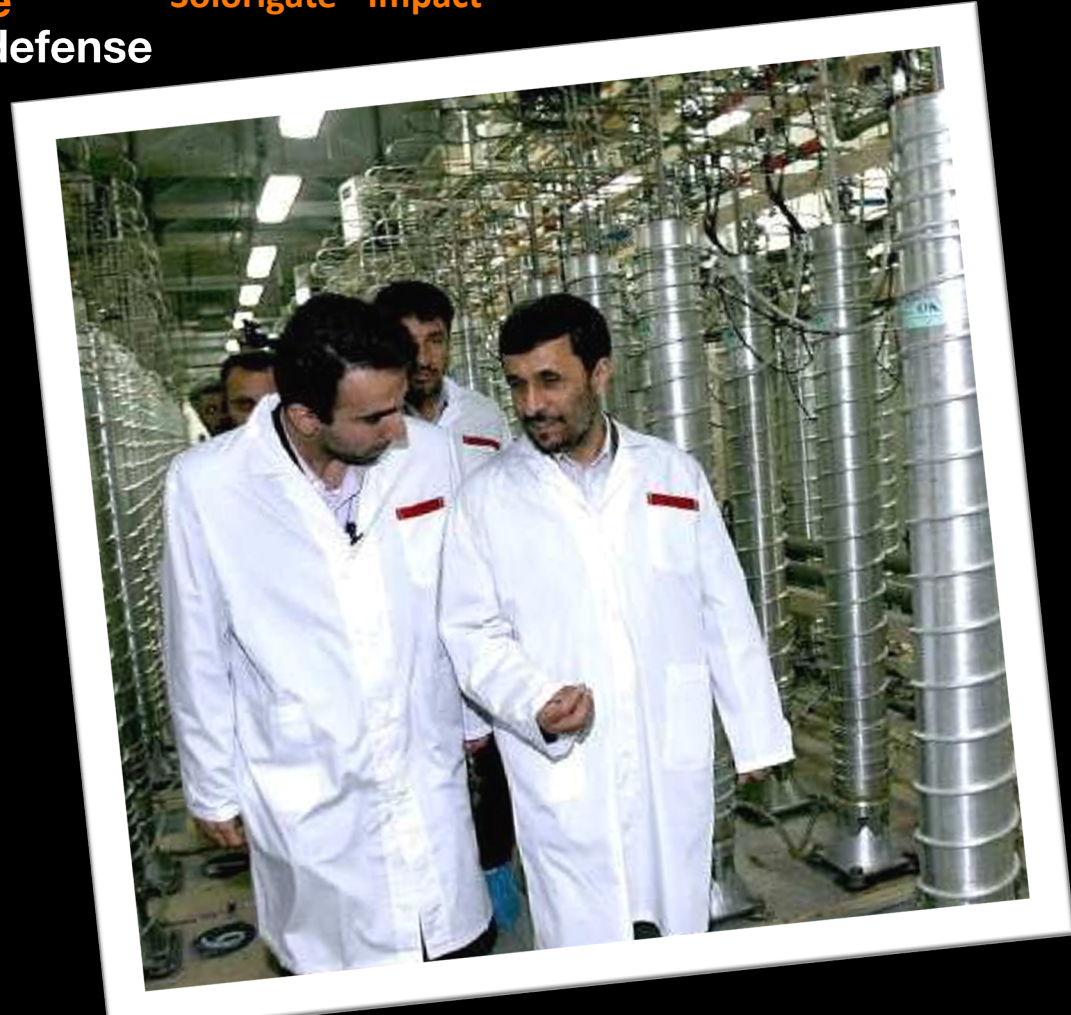


Source: Microsoft data



Orange
Cyberdefense

Solorigate - Impact



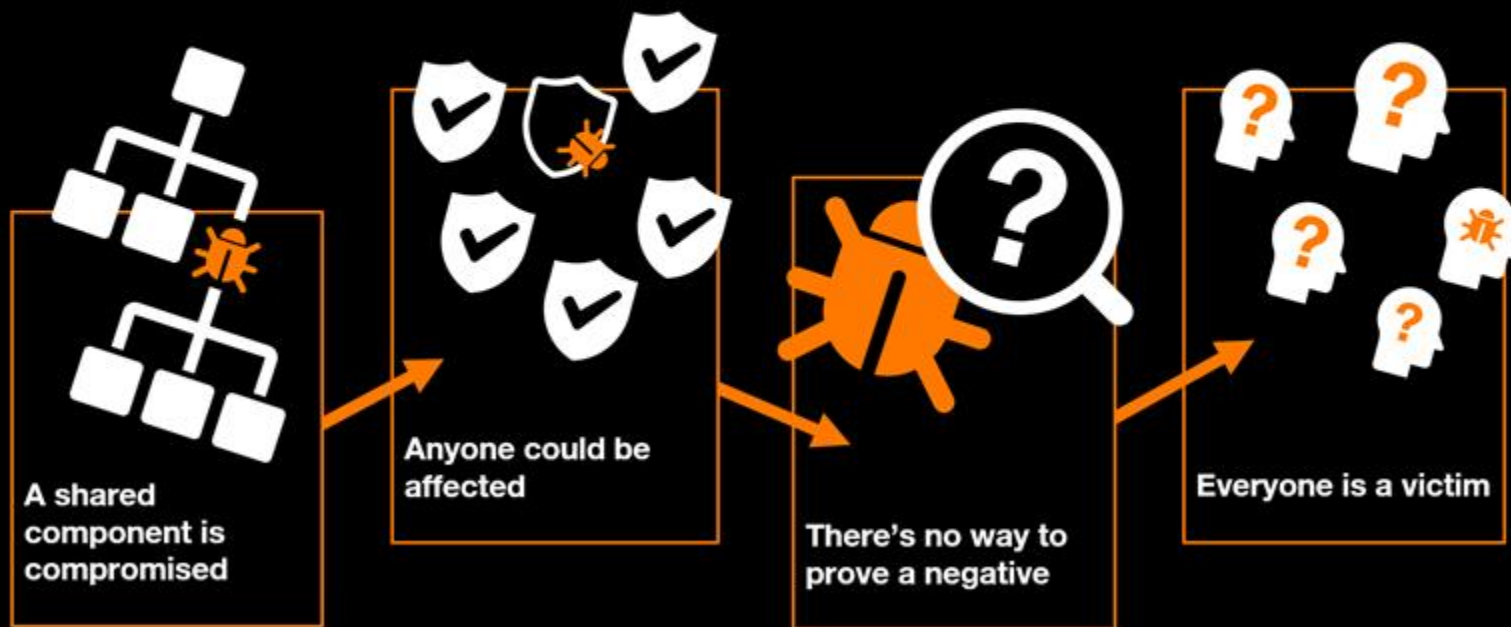


Orange
Cyberdefense

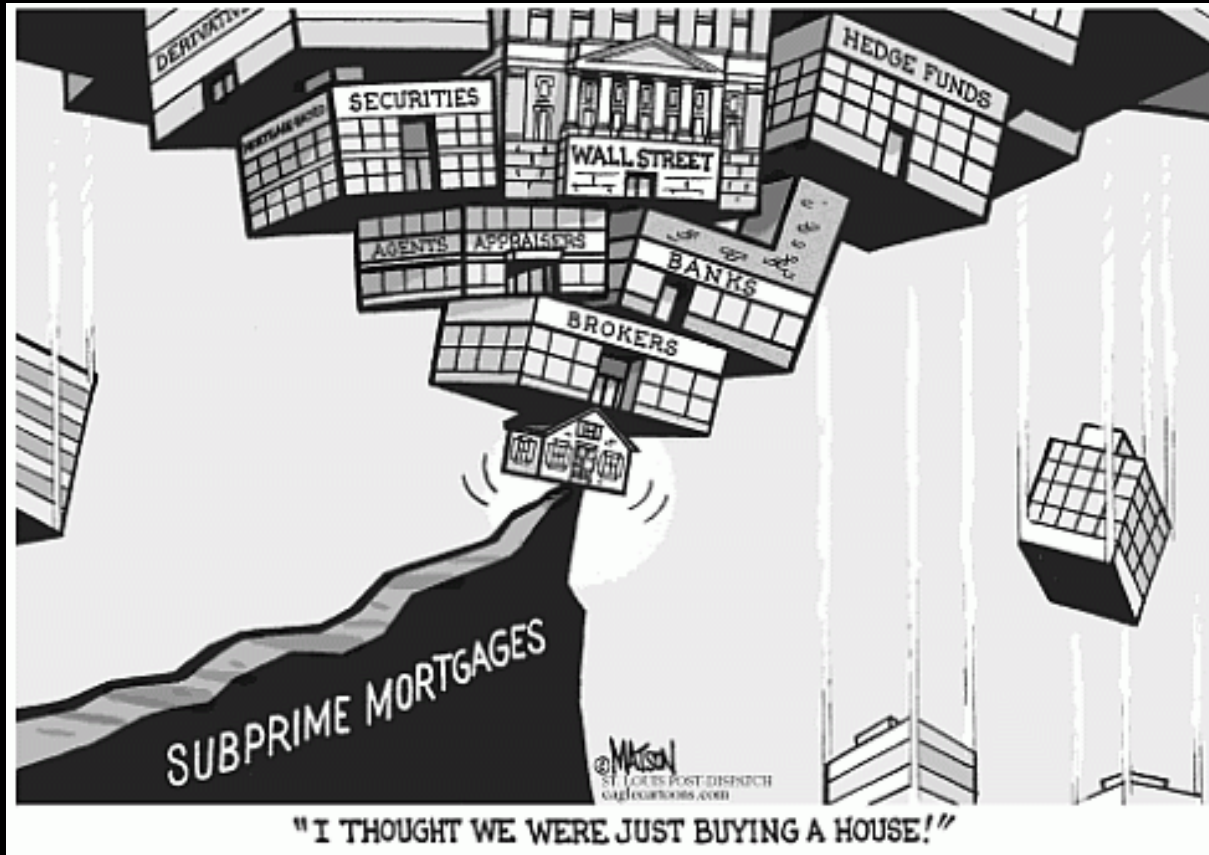
Solorigate - Impact



Compromising integrity & trust, causing “contagious” effect

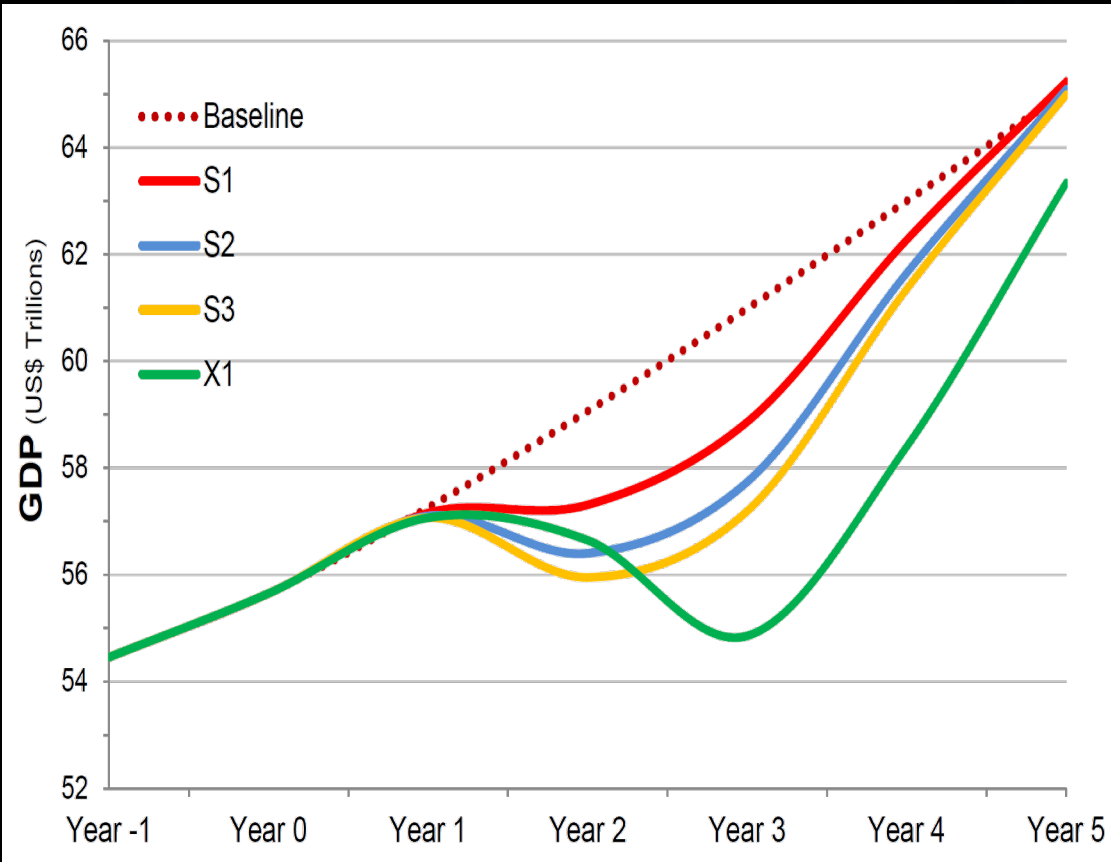


Solorigate - Impact



The 2008 GFC was a contagion event caused by **unmanaged debt** that cost the world economy somewhere in the region of **\$20 trillion**

Solorigate - Impact



The damage caused by the more extreme variants of Sybil Logic Bomb is almost as severe as the Great Financial Crisis of 2007-2012.

The most extreme scenario variant, X1, shows a GDP@Risk of \$15 trillion.

By comparison, the Global Financial Crisis of 2007-2008 cost \$20 trillion.

WEAR A MASK

**MY MASK
PROTECTS YOU**



**YOUR MASK
PROTECTS ME**

ONLY TOGETHER CAN WE SAVE LIVES

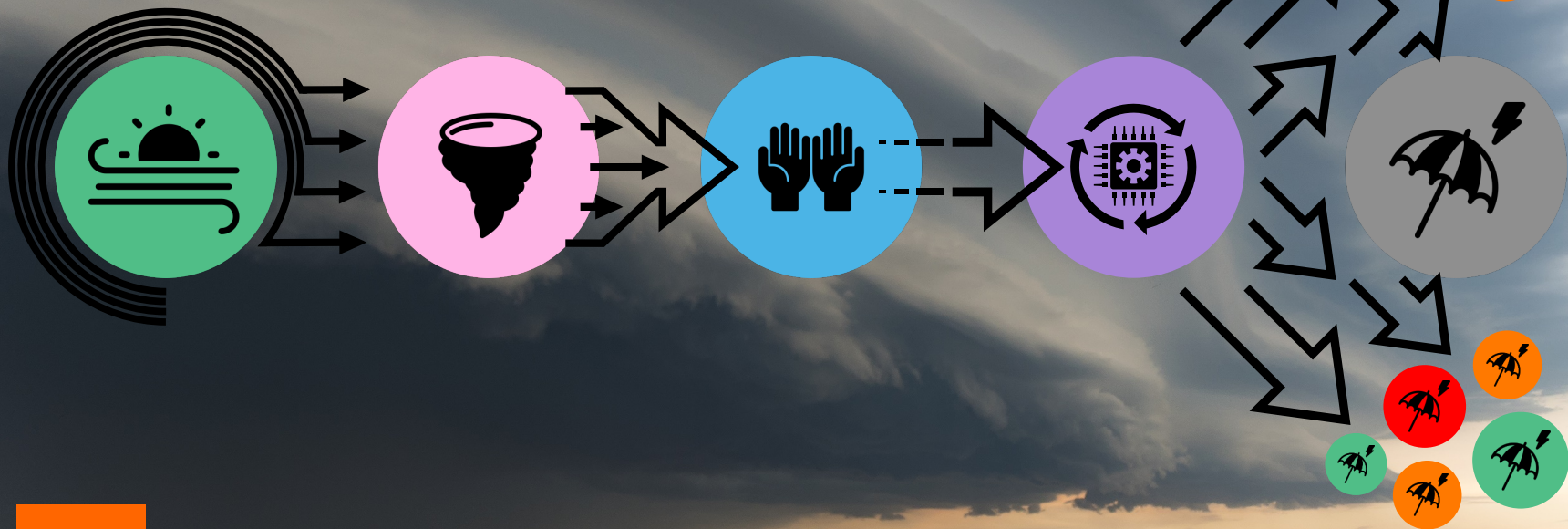
Solorigate - Impact

**Because pandemic
is not just a medical
thing**

Orange Cyberdefense

Solorigate - Causes

1. **Government investments in computer hacking capabilities.**
2. **IT Interdependence.**
3. Accumulated security debt.
4. **Supply Chain Risk.**



GEOPOLITICAL
DRIVERS

STRUCTURAL
FACTORS

LEGACY
FACTORS

EVOLUTION OF
TECHNOLOGY

EMERGING
THREATS



Structural forces

Systemic forces that create the enablers and constraints that shape the threat and our response

Influence

We cannot control these factors, but influence them. Influencing the landscape is the most far-reaching way of addressing threats in the long run.



Inflationary factors

The threat emerges out of a political, economic, social, legal & regulatory context

Observe and orient

These forces are like weather: they have an enormous impact but we cannot control them. Our only choice is to observe and adjust accordingly.



Evolution of technology

As technology changes so does the threat

Control

We can reduce the size of our attack surface, find and mitigate vulnerabilities. These efforts are under our control, so it makes sense to do so.



Government cyber operations

Involves work or investment by governments, state-sponsored or supported hackers, state-developed tools or capabilities, or their associated contractors.



Cyber interdependence

A threat, vulnerability or incident emerging from the inter-dependence businesses have on each other. A simple example of this would be supply chain vulnerabilities and attacks, attacks against MSSPs & attacks against shared (e.g. Open Source) code bases or systems (e.g. DNS or domain registrars). Incidents involving risk, attacks or compromises being spread from one organization to another (e.g. Maersk and notPetya or the Marriott breach) would also fall into this category.



Security debt

Security debt accumulates deep in the architectures, legacy code, 3rd party libraries and dependencies and even the fundamental economic principles that some business models are based on.



Supply Chain Attacks

The notion that the 'supply chain' is a growing new threat vector. 'Supply chain' would include software supply chain (including full applications, Open Source tools or common modules, service providers, contractors and other suppliers).

The hypothesis is that it makes sense for hackers to target the supply chain because it's often the 'weak' link in the chain, but also because a single carefully-selected supply chain compromise (e.g. a commonly used package or system) could allow for a high number of downstream compromises.



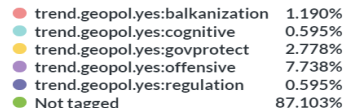
[Story - Trends] Geopolitical Trends

name

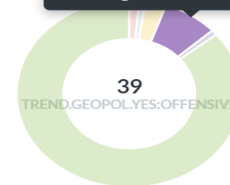
guidance

Government offensive Cyber operations	Use this tag if the Signal involves work or investment by governments, state-sponsored groups, or other entities acting on behalf of a government.
Shift from tactical to cognitive methods	Use this tag if the Signal involves attacks at the 'informational' level, e.g. misinformation, disinformation, or cognitive warfare.
Government efforts to protect civilian cyberspace	Use this tag if the Signal involves national-government cybersecurity interventions, such as blocking access to malicious websites or blocking access to malicious applications.
Treaties, Legislation, Regulation	Use this tag if the Signal discusses internal treaties like the Wassenaar Agreement or international treaties like the Budapest Convention.
Balkanization of cyberspace	Use this tag if the Signal covers issues that increase or decrease the 'splintering' of cyberspace into different, non-interoperable regions.

[Signal - Trends] Geopolitics - split across all Signals - 2020



value: trend.geopol.yes:offensive
Count: 39
Percentage: 7.738%



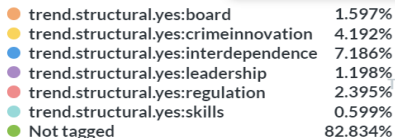
[Story - Trends] Structural Trends

name

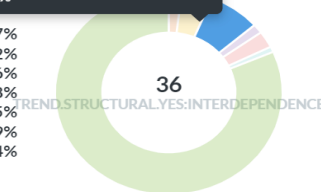
guidance

Regulation & Penalties	Use this tag if the Signal has anything to do with national- or industry-level standards, best practices, or legal requirements.
Board Accountability	Use this tag if the Signal involves something that would directly or indirectly increase the perceived accountability of a company's board of directors.
Cyber Inter-Dependence	Use this tag if the Signal discusses a threat, vulnerability or incident emerging from the interdependence of different systems, services, or organizations.
Skills Gap	Use this tag if the Signal discusses anything that illustrates the skills gap or speaks to major developments in the cybersecurity workforce.
Security Leadership Gap	Use this tag if the Signal discusses an issue that indicates a lack of security leadership, or poor security practices within an organization.
Constant Cyber Crime Innovation	Use this tag for any Signal that demonstrates real 'business' innovation within the criminal ecosystem.

[Signal - Trends] Structural - split across all Signals - 2020



value: trend.structural.yes:interdependence
Count: 36
Percentage: 7.186%



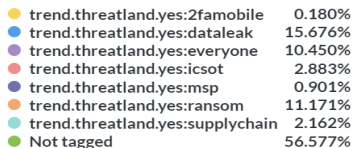
[Story - Trends] Emerging Threat Landscape

name

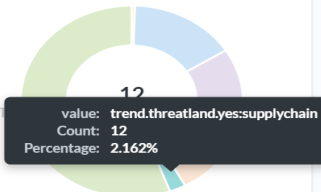
guidance

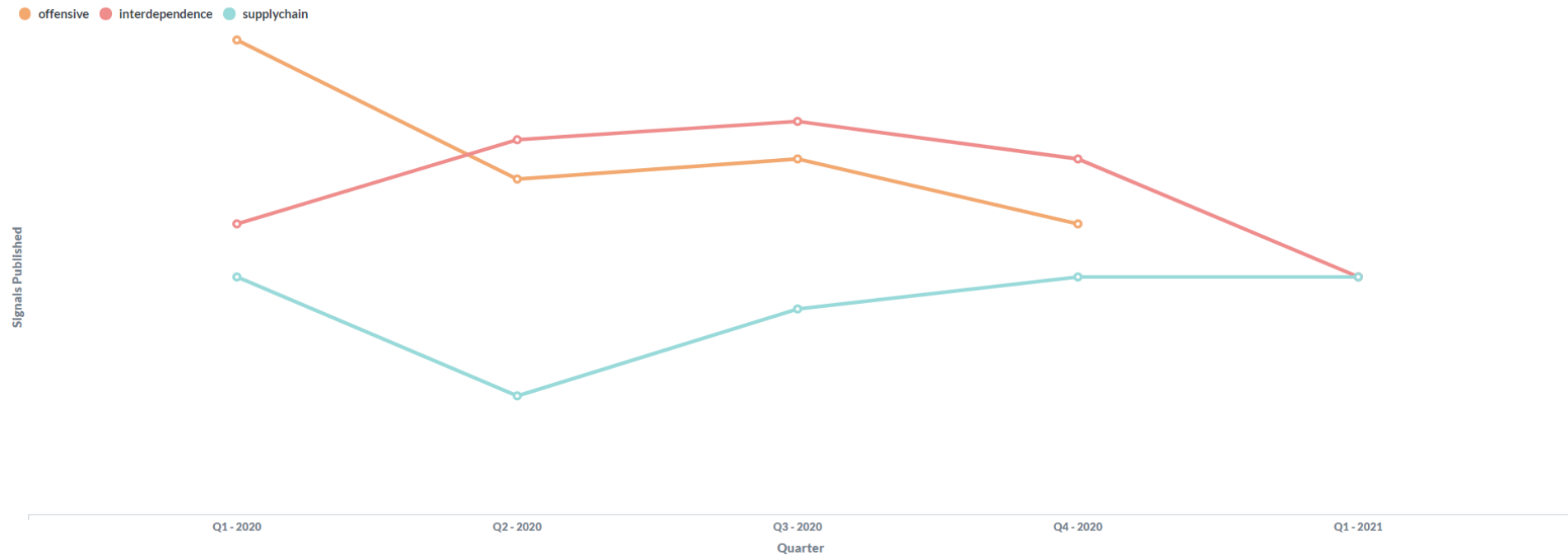
Everyone is a Target	Chose this tag if the Signal proves or disproves the point that no business or person is too big or too small to be targeted.
Supply Chain Attacks	Use this tag if the Signal proves or disproves the notion that the 'supply chain' is a growing new threat vector.
ICS / OT Attacks & Abuse	Use this tag if the Signal covers issues to do with 'Internet of Things' or 'Operational' technologies (e.g. ICS, SCADA, PLCs, etc.).
Attacks On MSPs	Use this tag if the Signal covers something to do with the security of Managed Service Providers or other third-party service providers.
Ransom & Extortion Attacks	Use this tag if the Signal involves ransom or extortion attacks. The hypothesis that we're testing is that ransomware is becoming a more common threat vector.

[Signal - Trends] Threat Landscape - split across all Signals - 2020



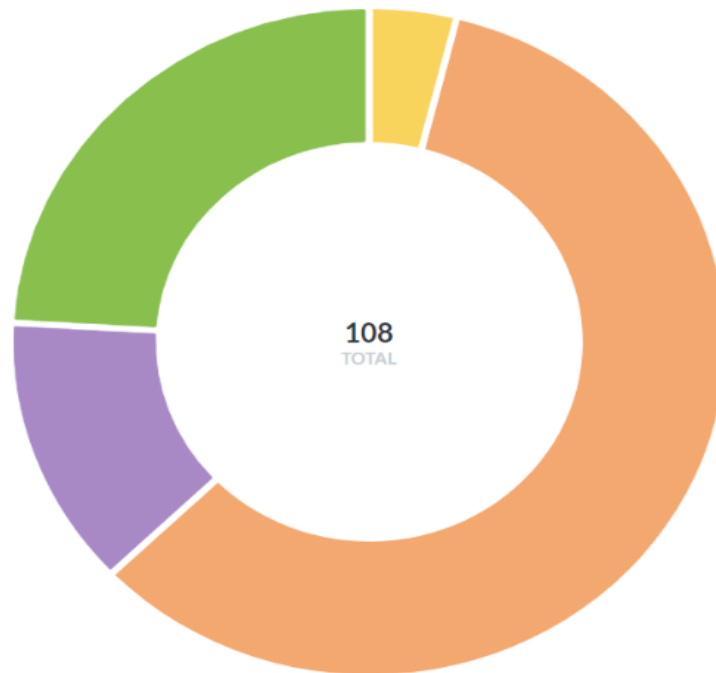
value: trend.threatland.yes:supplychain
Count: 12
Percentage: 2.162%







damaging	3.7%
distracting	59.3%
insignificant	13.0%
painful	24.1%





- SolarWinds will face all kinds of legal, regulatory and civil sanctions
- Fear, Uncertainty and Doubt
- Political fall-out
- Option of retaliation via a 'kinetic' response
- The USA will retaliate in cyberspace, *but that probably won't help*
- The USA will seek to examine and improve its own cyber readiness
- A significant shot in the arm for the security industry... the next SolarWinds



Risk Management

Does Your Cyber Insurance Cover a State-Sponsored Attack?

by Jon Bateman

October 30, 2020



Solorigate - Consequences

Google has suspended business with Huawei that requires the transfer of hardware, software and technical services ...

... could hobble Huawei's smartphone business outside China...

Trump administration officially added the telecoms manufacturer to a trade blacklist on Thursday, declaring a **national economic emergency** to ban the technology and services of "foreign adversaries"

... follows a report last week calling for Huawei to be prevented from supplying 5G mobile networks in the UK, because its operations are "subject to influence by the Chinese state"...

The British government has been pressured by partner intelligence agencies in the US and Australia to reconsider [HUAWEI] participate in the UK's 5G network.

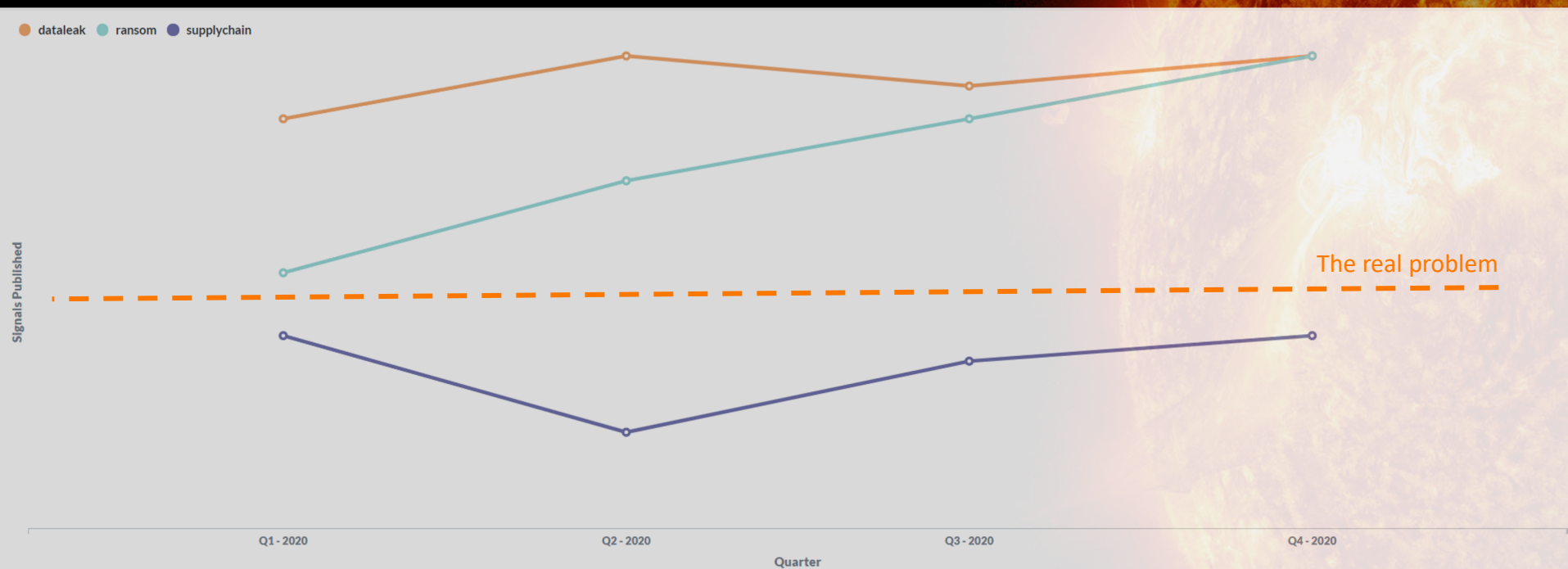




Orange
Cyberdefense

Solorigate - Response



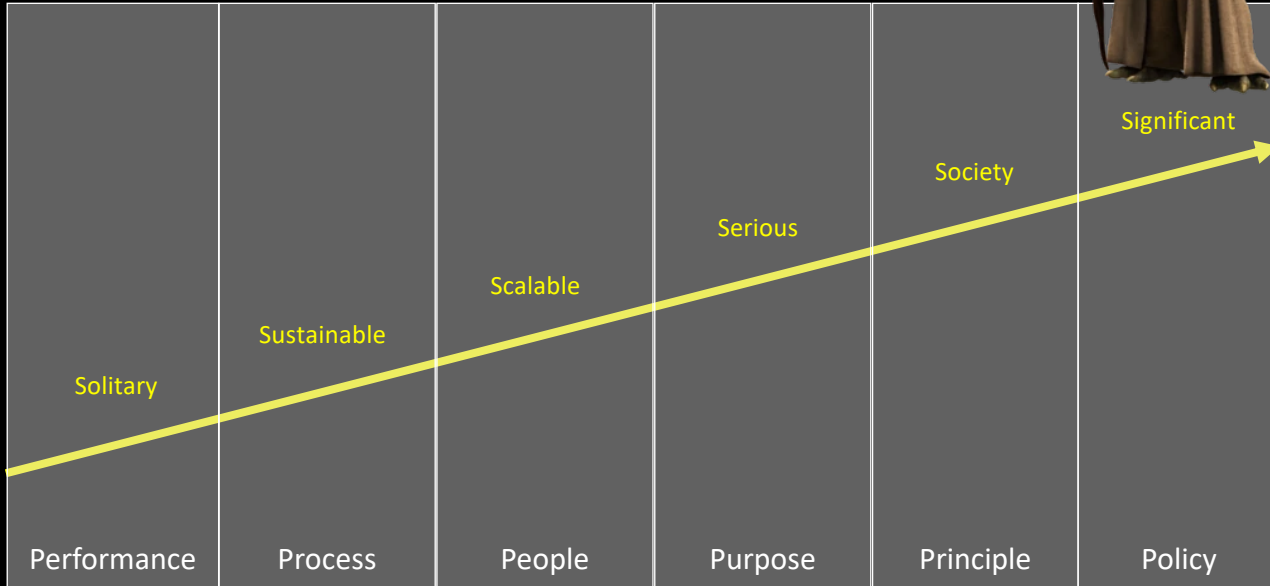




teachers,
philosophers,
scientists,
engineers
physicians,
diplomats
...and warriors.

who value knowledge
and wisdom above nationality.

give of themselves through acts of
charity, citizenship, and volunteerism





- **Performance**: Master the theory and practice of information security.
- **Process**: Capture the practice in the form of clear and repeatable processes that can be delegated to others.
- **People**: Focus on enabling others through education and mentoring to also master security fundamentals and practice.
- **Purpose**: Understand the why of cyber security - the fundamental goals it has of enabling business, government and healthy life in the modern world.
- **Principle**: Understand and explain how security can and should contribute to the fundamental goals of society.
- **Policy**: Interact with regulators, executives and other leaders in society to create and influence the policies that will ultimately shape the world we live in for many years to come

Our approach to stay ahead of the bad weather

- The risks are real, and the stakes are high
- The system is complex and fundamentally predisposed to fail
- The victim of failure is trust
- Trust is a runnable asset
- The difference between compromise and crisis... is early detection and effective response



- Attack is inevitable
- Compromise is probable
- Engagement is essential

Detect and Respond – Intelligence-led security

**“ Everybody
complains about
the weather, but
nobody does
anything about it.”**

Charles Dudley Warner (1829 – 1900)



Intelligence led security is the collection, validation, aggregation, correlation and analysis of both **internal and external data...**

to understand risks, identify threat actors, discover attacks underway, and **understand the motivations, methods and actions of likely adversaries...**

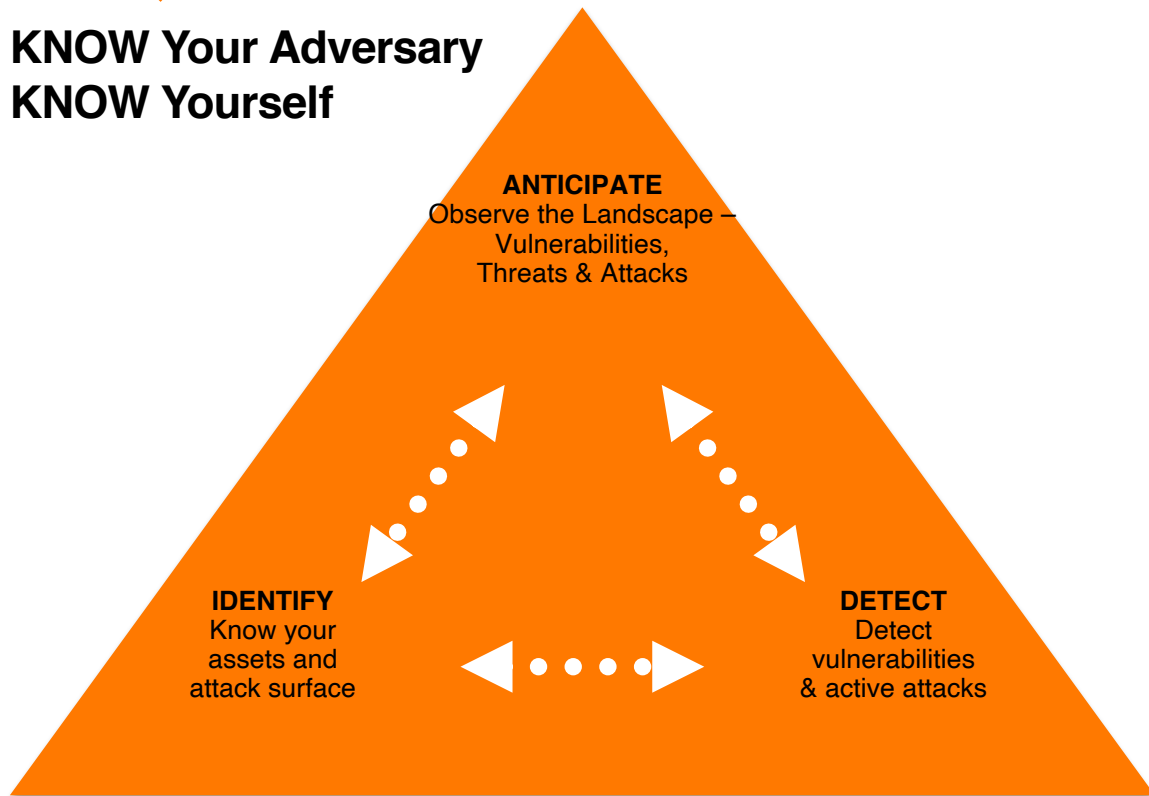
so that limited security resources can be invested where they will **have the most impact.**



INTELLIGENCE LED SECURITY REQUIRES 2 PERSPECTIVES

KNOW Your Adversary

KNOW Yourself



**KNOW THY SELF,
KNOW THY ENEMY.
A THOUSAND BATTLES,
A THOUSAND VICTORIES.**
SUN TZU

OCD.360 - EXTERNAL Intelligence at different levels



Strategic

Concerned with long term trends and systemic changes.
Used to drive high-level organisational strategy



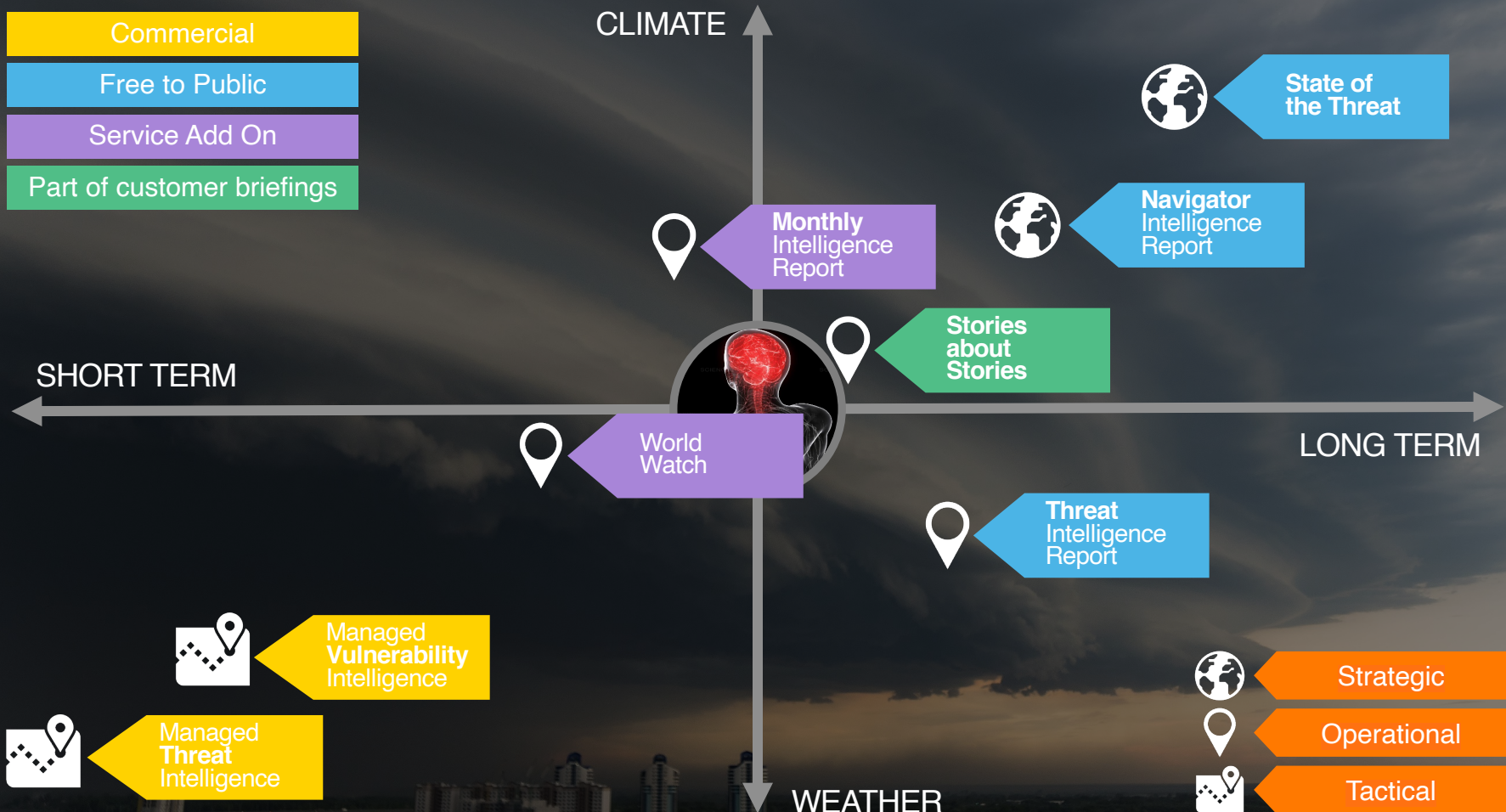
Operational

Insight that allows us to direct our resources in the most effective manner to counter contemporary threats, mitigate vulnerabilities or respond to relevant changes in the broader environment

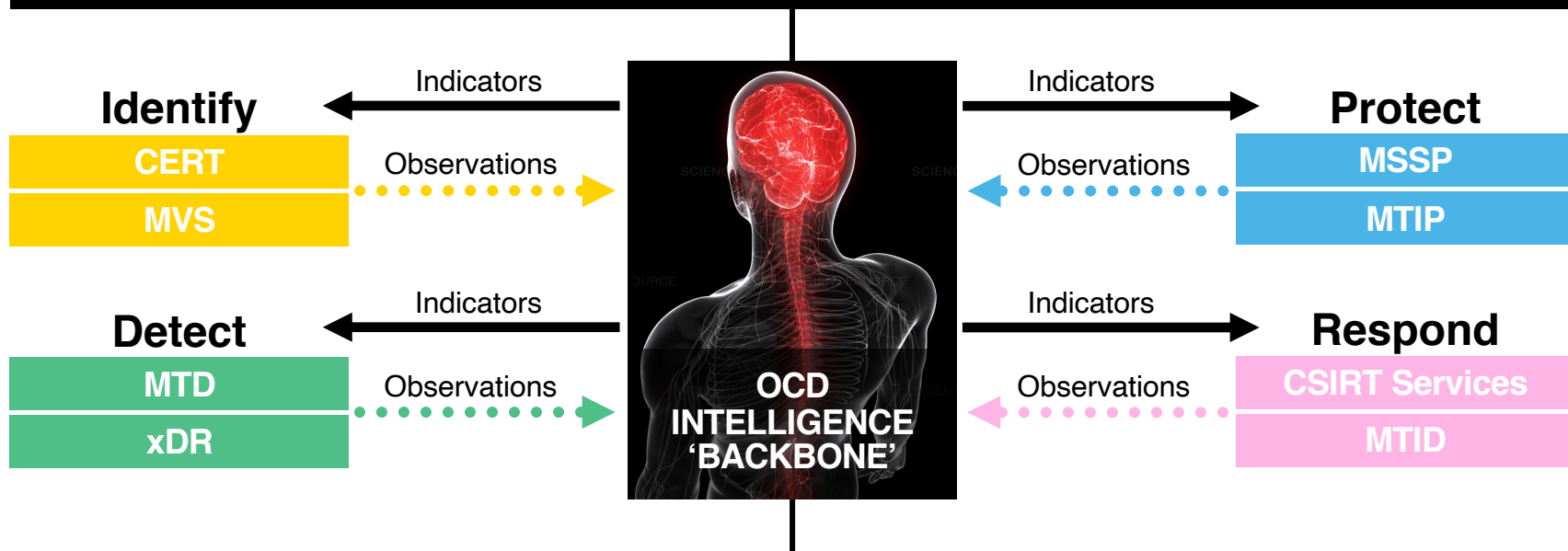


Tactical

Near Real time Technical intelligence with a short TTL. Includes Indicators of Vulnerability, Compromise & Attack such as IP addresses, file names, or hashes, which can be used to assist in the identification of threats and vulnerabilities.



Threat feeds, vulnerability feeds, OSInt, Pulse, OCD / OBS / OCD CERT





Anticipate	Cyber threat intelligence	Vulnerability intelligence
Strategic	Monthly Briefings, State of the Threat, Security Navigator, Stories	
Operational	Epidemiology Labs I Threat Intelligence Report	
	World Watch Advisory Service	
Tactical	Managed Threat Intelligence	Managed Vulnerability Intelligence



Fin. Baie dankie!

<https://orange cyberdefense.com/global/white-papers/solorigate-winds-of-change/>

Timeline

- 25-09** Threat actors started targeting one of our customer
- 14-10** We noticed that lot of malwares are trying to be delivered using google docs
- 15-10** Proactive hunting and research on Bazarloader / Bazarbackdoor
- 16-10** Start threat actor's infrastructure tracking
-  **20-10** Sopra-Steria hit by global ransomware attack (Ryuk)
- 21-10** Sopra-Steria communicated about the attack and share some IOCs
-  **22-10** Orange Cyberdefense CyberSOC started a MTC
- 28-10** End of Orange Cyberdefense MTC
- 29-10** CISA warns of disruptive ransomware attacks on US hospitals
- 29-10** Many companies share high-value TTPs and IOCs and we start diffing and hunting on them.

sopra  steria

Ransomware Ryuk : la piste d'une attaque éclair contre Sopra Steria

Septembre 2020, les équipes de sécurité de Sopra Steria ont été alertées par un client d'une attaque par ransomware. Les équipes de sécurité ont immédiatement lancé une enquête et ont découvert que l'attaque était liée à un ransomware connu sous le nom de Ryuk.



Le 29 octobre 2020, les équipes de sécurité de Sopra Steria ont été alertées par un client d'une attaque par ransomware. Les équipes de sécurité ont immédiatement lancé une enquête et ont découvert que l'attaque était liée à un ransomware connu sous le nom de Ryuk.