

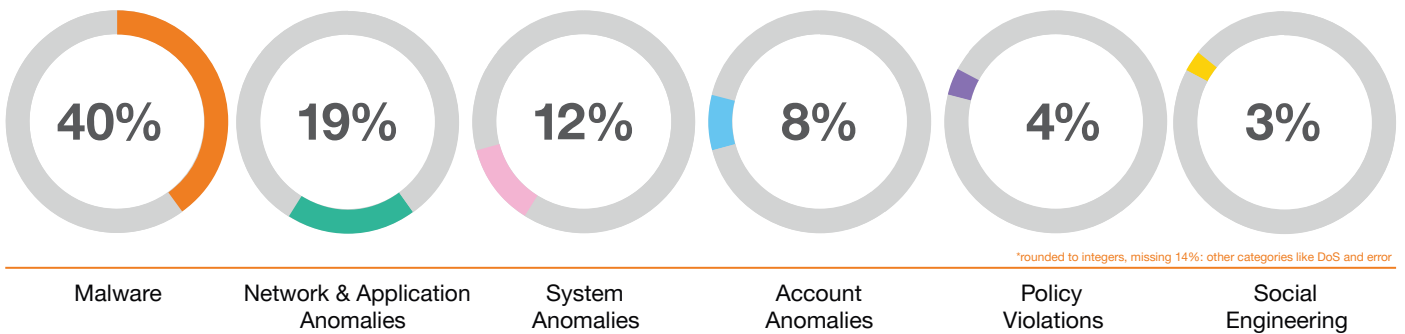
# Security Navigator 2023

Research-driven insights  
to build a safer digital society



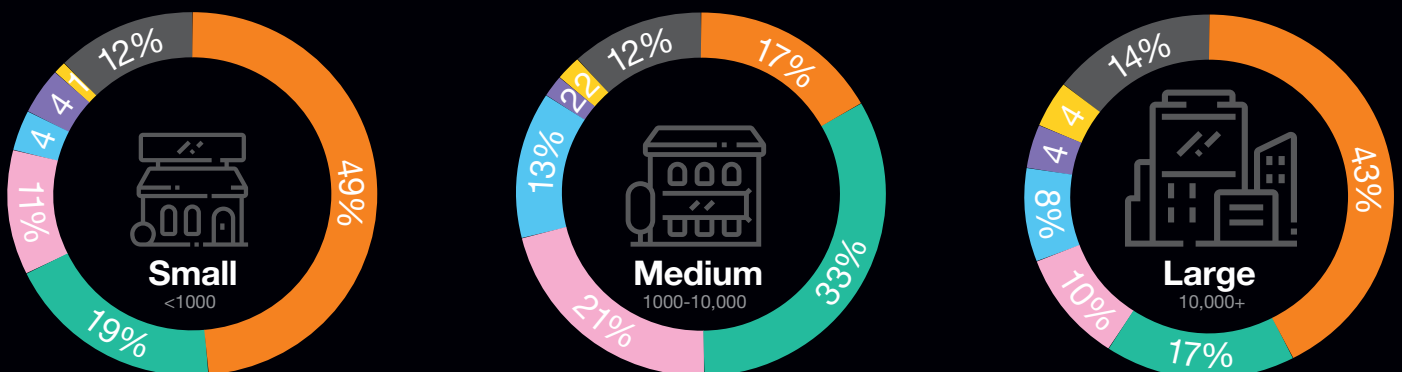
- Get the 'big picture' of cybersecurity
- 100% first-hand information from Orange Cyberdefense's the 17 global SOCs & 13 CyberSOCs , CERT, Epidemiology Labs, World Watch, Ethical Hacking and Vulnerability Management operations
- Gain invaluable insights into the threat landscape
- Expert reports and technology reviews on topics like Ransomware/Cyber Extortion, Mobile Security and the impact of the war in Ukraine
- Check attack patterns and statistics for your business size and vertical
- Learn what the most disrupting events in 2022 were and how that projects into the future
- Get the full 120-page report [here!](#)

## Funnel: 99,506 incidents ► 29,291 confirmed security incidents



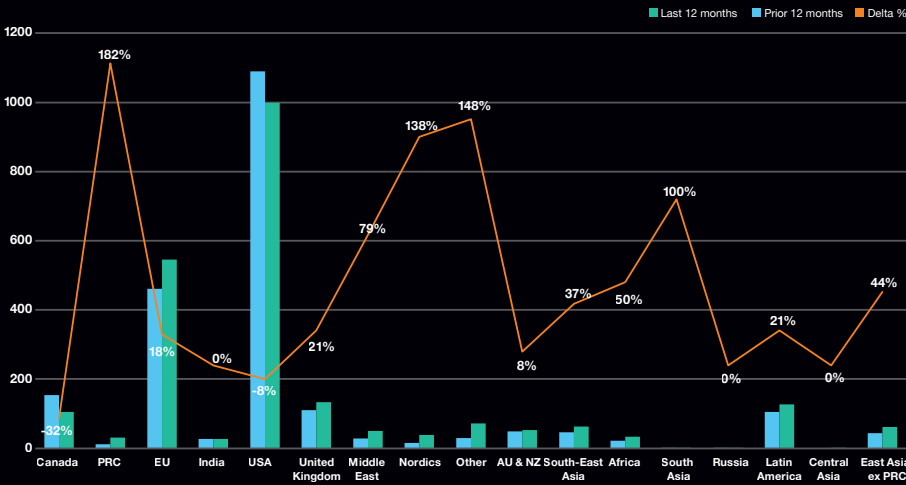
## A matter of scale: Incidents by business size

■ Malware ■ Network & Application ■ System ■ Account ■ Policy Violations ■ Social Engineering ■ Others





## Cy-X & Ransomware: The geographic shift



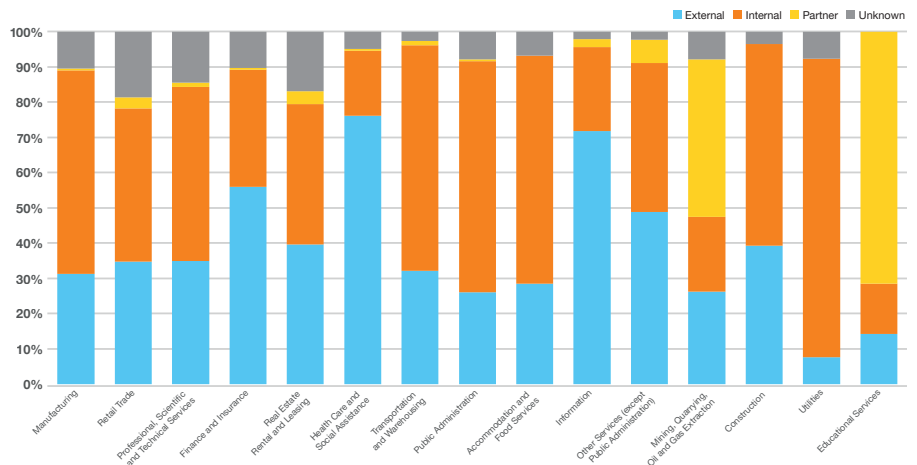
Traditionally, large, English-speaking countries have been impacted the most by Cyber Extortion. This however started changing in 2021 and has continued to do so throughout 2022. The location of victims seems to be shifting – from the US and Canada, through the UK and Western Europe, and toward the rest of the world.

These changes accelerated during the last 6 months, with decreases of 34%, 33% and 20% in the UK, USA and Europe respectively, while East Asia and South-east Asia grew by 30% and 33% over the same period.

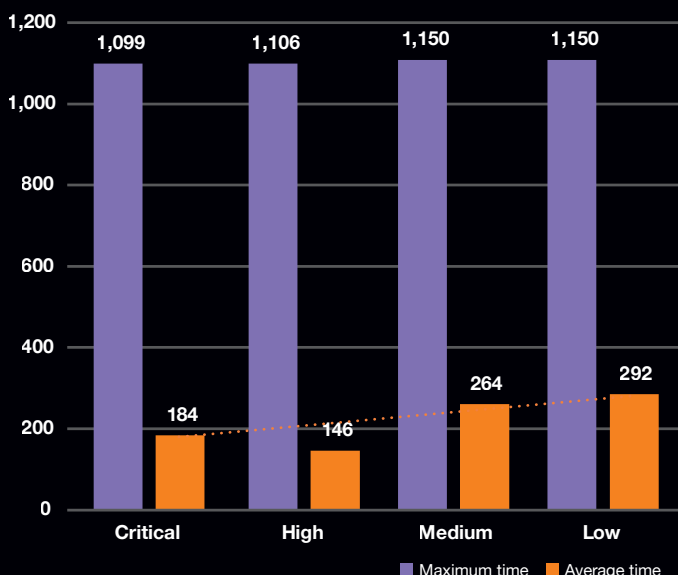
## A first glimpse of VERIS: Incident Sources

The breakdown on the right shows an overview of all verticals and the threat actors considered responsible for their incidents. While we are still in the process of adopting VERIS, it does provide some insight into what kinds of actors are being encountered by each industry. Of course, these findings can be significantly shaped by the detection capabilities of each customer in the respective vertical.

It is somewhat remarkable how many industries seem to deal with more internal 'actors' than external ones.



## Vulnerabilities & Patching



### Average/max age of findings by severity

Taking a closer look at the readings of average vs. maximum time for different ratings of criticality, we end up with the chart on the left.

Even Critical Vulnerabilities are taking around 6 months on average to resolve, but that is encouragingly at least 36% faster than the time for low severity issues.

While our conclusion of critical issues being resolved faster stands for the average mitigation time, the maximum time is consistently high regardless of criticality.