SOCURA

Why Google Chronicle for the Public Sector?

Improve threat hunting capability with more comprehensive security investigations

Chronicle

> “Only by ensuring that cyber attacks neither disrupt our core functions, nor erode vital trust and public confidence can we use the full potential of cyber as a lever to protect and promote our interests in a world that is being fundamentally and rapidly reshaped by technology.”

STEVE BARCLAY, CHANCELLOR OF THE DUCHY OF LANCASTER AND MINISTER FOR THE CABINET OFFICE

SECURITY ANALYTICS:

Where are we now

Objective 1 of the Government Cyber Security Strategy focusses on managing cyber security risk, and a large part of this lies in the visibility and understanding of assets, their vulnerabilities, and the threat to them.

However, the evolving threat landscape, the requirement to collect and process more security data, and a growing attack surface, means that public sector organisations find it difficult to keep up with the operational needs of their cyber security.

35%

More than one-third of organisations say they collect more security data today than two years ago.[1]

63%

Nearly two-thirds of organisations believe security analytics and operations is more difficult today than it was two years ago.[1]

29%

Of organisations admit to finding it difficult to keep up with the operational needs of our cyber security analytics and operations technologies.[1]

SOCURA INSIGHT

Telemetry must be collected from every asset/device, and across all parts of the IT infrastructure (including IaaS, PaaS, SaaS, endpoints, firewalls, email, directory services, DNS, Proxies, VPN, etc). Data should go back a year for maximum visibility.

[1] ESG Research - The rise of cloud-based security analytics and operations technologies - 2019

The Volume Challenge

Better use of data can help organisations of every kind succeed, and in the public sector is central to the delivery of a whole range of vital public services and societal goals, from tackling climate change to supporting the National Health Service.

The UK governments National Data Strategy seeks to harness the power of data to boost productivity, create new businesses and jobs, improve public services and position the UK as the forerunner of the next wave of innovation.[2]

Data volumes are already an order of magnitude higher than they were just a few years ago due to growing infrastructure, more applications, and, in the case of security, more tools. Beyond storage costs, today's security data volumes require a significant infrastructure investment to enable scalable and performant analysis.

Traditional security analytics pricing models are primarily based on data volume, or number of monitored devices, incentivising you to limit the collection and analysis of information.

[2] Department for Digital, Culture, Media and Sport - Policy Paper - National Data Strategy 2020

The Visibility Challenge

In January 2020, NHS Digital completed migration of two key public-facing services, the e-Referral Service (e-RS) and the NHS 111 Directory of Services (DoS), to public cloud infrastructure. Many more are set to follow into this cloudy future under the government's Cloud First policy.

However, as infrastructure evolves from on-premises to IaaS/PaaS/SaaS platforms, coverage and visibility have also emerged as critical barriers to security operations. Some cloud providers focus primarily on delivering security monitoring for their own stack.

Such siloed coverage limits visibility into modern attacks that commonly span on-premises and hybrid cloud infrastructure.

Socura has partnered with Google Cloud Chronicle to allow us to ingest all the security data that an organisation's systems generate, resulting in complete visibility across all data sources.

This data is retained for 12 months, and is searchable in milliseconds, meaning that we can instantly and retroactively match newly discovered threats against the entire historical telemetry dataset.

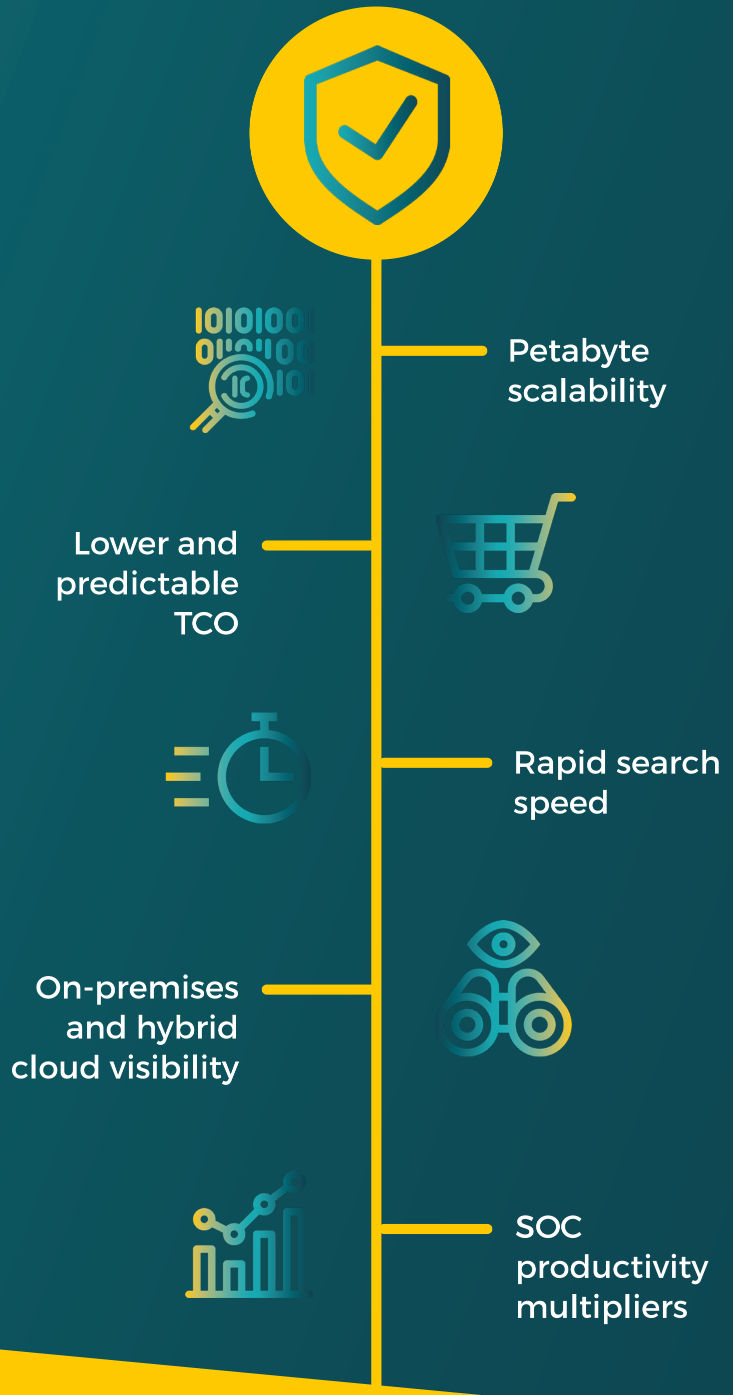
Holding more data for longer, enables us to see the bigger picture with no blind spots.

Chronicle

Modern security analytics requirements

It’s time to take a fresh look at what is possible and how it can be achieved using the latest tools and approaches on offer. It’s time to refactor for this new world. It’s time to re-evaluate the threat, and how best to defend against it.

Chronicle, the Security Analytics element of Socura’s MDR service, is provided by Google. The elastic scale and speed of search that they are renowned for can be brought to bear on the problem of hunting for malicious activity amongst vast amounts of data.



Petabyte scalability

Lower and predictable TCO

Rapid search speed

On-premises and hybrid cloud visibility

SOC productivity multipliers

SOCURA