SOC:OS

WHITEPAPER

INTRODUCING SOC.OS

SOC.OS IS A SECURITY ALERT INVESTIGATION AND TRIAGE AUTOMATION TOOL WHICH IS TACKLING THE PROBLEM OF ALERT-WHACK-A-MOLE AND FUNDAMENTALLY RE-IMAGINING HOW SECURITY OPERATIONS ARE CONDUCTED TODAY.

IT HAS BEEN DESIGNED AND DEVELOPED WITH THE BESPOKE AND FUNDAMENTAL NEEDS OF A SMALL AND STRETCHED IT SECURITY TEAM AT ITS VERY CORE.

THIS PAPER OUTLINES WHO OUR IDEAL CUSTOMER IS, THE PROBLEMS SOC.OS AIMS TO ADDRESS, THE VALUE THE PRODUCT DELIVERS, AND THE BENEFITS AVAILABLE TO THOSE WHO JOIN THE CUSTOMER COMMUNITY.

MEET SHAZ: OUR TYPICAL SOC.OS CUSTOMER

CHARACTERISTICS OF SHAZ:

- IT security manager
- Organisation that is progressing their cyber maturity
- Wears many hats and works within a small and stretched team

PROBLEM SHE FACES:

- Deployed a handful of security devices, which generate 100s if not 1000s of alerts daily
- No correlation or consolidation of these alerts across her tools, and each alert is addressed in isolation of the next
- Current SIEM/SOAR solutions are tailored to large SOCs or internal IT security teams, require a lot of maintenance overhead, and are typically cost prohibitive for Shaz and her organisation

ALERT FATIGUE AND WHACK-A-MOLE

Alerts are valuable. Each warning and notification can be the difference between a minor incident and a business-hobbling disruption. However, there can be too much of any good thing, even alerts. Especially when limited IT and cyber security resources must deal with evaluating and responding to alerts manually and in an isolated fashion. Manually triaging 1000s of alerts on a daily basis is overwhelming and ineffective.

ALERTS: A RACE YOU AREN'T WINNING – BUT CAN'T AFFORD TO LOSE

Currently, over a third of mid-sized organizations surveyed (37%) are still investigating alerts manually, and a shocking 7% - as many as over 1,200 US medium-sized businesses (footnote 1)– are doing nothing with the alerts they receive.

On average, of the alerts that make it through the current security tools these organizations have in place, fewer than 20% are actually investigated.

* Except where attributed otherwise, the quotes throughout this guide come from an online survey conducted by Spiceworks on behalf of BAE Systems in early 2018. Some 600 IT decision makers in the UK and US, from organisations ranging from 250 to 9,999 employees in a variety of commercial sectors, responded to the survey. Those respondents were required to be involved in the selection of security solutions at their respective organisations, and to employ security solutions that produce alerts.

SOC.OS HELPS FIND THE NEEDLE IN THE HAYSTACK

To further compound and complicate the problem faced by IT security teams, the vast majority of alerts produced by an organisation's security tooling are false positives. To manually sift through a deluge of alerts in a whack-a-mole fashion in hope of finding the needle in the haystack is next to impossible for a human analyst to achieve.

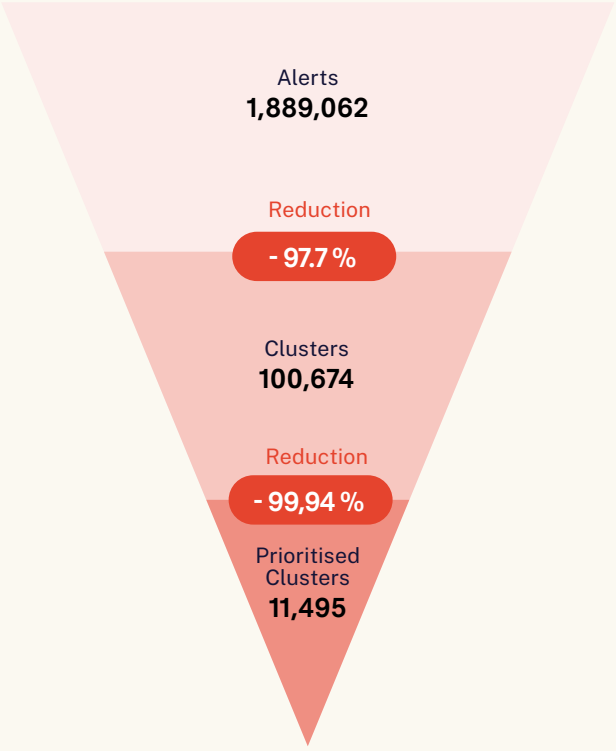
HOW IT WORKS

Ingested alerts are enriched with 3rd party threat intelligence data sources (e.g. Whois information) and the MITRE ATT&CK threat associated with the alert is automatically identified.

The alerts are then correlated into groups or "clusters" based on shared entities and threat types. This ensures that, for example, alerts targeting the same part of your network with similar threat types would appear in the same cluster and can be easily examined in one go. These clusters are then ranked so that the ones deemed to require urgent investigation can be found easily on the SOC.OS workbench.

Users also have the ability to define and specify, within SOC.OS, what the critical assets are within their network, such that clusters containing these assets are boosted further up the priority ranking list. These clusters can then be investigated from the SOC.OS workbench using a bespoke data visualisation tool that illustrates the time evolution of the cyber event. To see an example in action, please download and read our product sheet from the landing page.

To highlight just how challenging this problem is for our customer community, and how SOC.OS can help find the needle in the haystack, in the 3 month period of March - May 2020, SOC.OS analysed 1,889,062 security alerts, correlated these into 100,674 clusters and of these clusters, prioritised 11,495 (which is an equivalent volume reduction of circa 99.4%).



OUR MISSION AND THE SOC.OS COMMUNITY

In the early days of SOC.OS, before an ounce of effort went into designing or developing a technical solution, before the first architecture diagram appeared or the first line of was code written; we spent many months speaking to a long list of customers and infosec professionals to explore in great depths the problems outlined in this white paper. Listening and collecting feedback about the problems our peers and colleagues faced day-day, fuelled our determination to challenge the notion that "security-alert-whack-a-mole" was here to stay.

Thus, our mission was born; to tackle alert fatigue head on in a unique way and by doing so, fundamentally re-write the playbook that dictates how security operations are conducted today. If that mission resonates with you and you feel as passionate as we do about solving this problem, we'd love to hear from you.

Similar to the early days, we still love listening to and hearing our customers' feedback, and adopt a collaborative and user centric product development philosophy within our company. Becoming part of the early adopting and innovative customer community means you'll have the exciting opportunity to work directly with the founding team and influence the roadmap through feedback.

If you'd like to learn more, or see a product demo, please get in touch with the SOC.OS team at


info@socos.io

Alternatively, you can register your details on our website at www.socos.io and a team member will get in touch as soon as possible.


www.socos.io

SOC.OS

SOC.OS Cyber Security Ltd.

info@socos.io

www.socos.io

https://www.linkedin.com/company/socoscyber