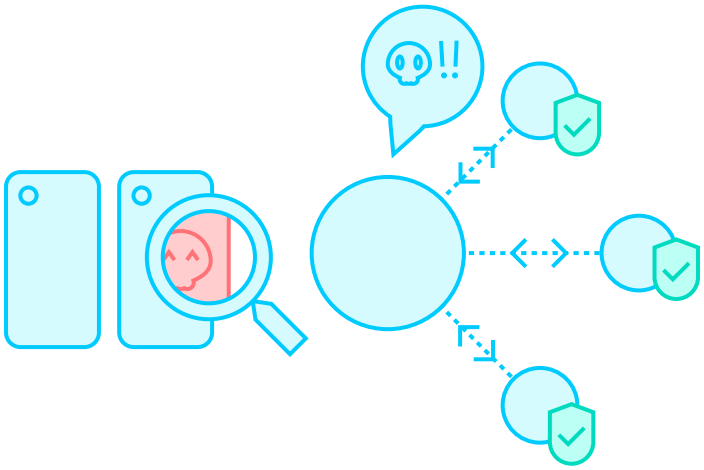
Arctic Security

USE CASE

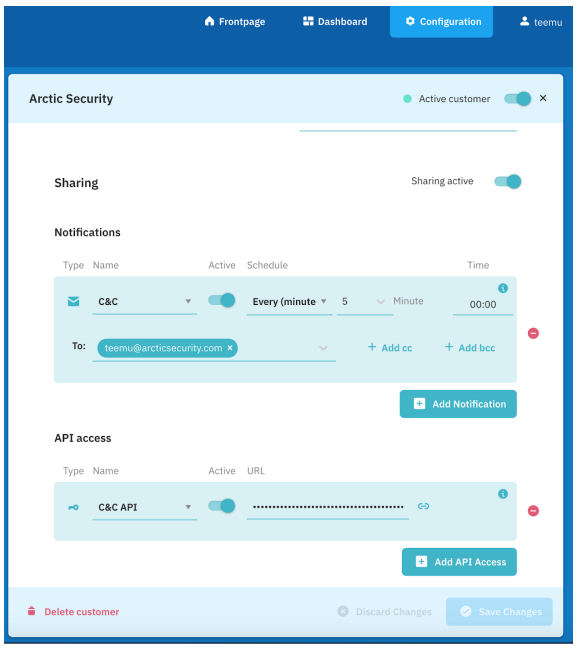
AUTOMATICALLY ALERT YOUR CONSTITUENTS

Cyber security authorities, CSIRT teams and ISACs can tap into a wealth of actionable and reliable abuse information. This information can alert your constituents on compromised or vulnerable systems and help them to remediate them in an efficient manner.



However, the information is sometimes hard to find, comes in various formats and is not readily attributed to specific organisations. Efficiently handling such abuse information allows to increase the security baseline of organisations and concentrate the time of your experts on work that requires a human touch.

In Arctic Hub, incoming abuse data is automatically harmonised and matched against your constituents' infrastructure, enabling the sharing of actionable and constituent-specific threat intelligence packages. The information is automatically qualified, enriched with other sources of data like passive DNS, WhoIs and geolocation data and deduplicated. Arctic Hub does all of this automatically after you configure your constituents using their domain information and IP ranges.



You can select what kind of threat intelligence packages you want to create and which packages to share to which constituents. Also, for each package you can choose if you want to share that via an email report or a direct API access. Finally you can determine if you want to follow up on the alerting by creating tickets in your ticketing system.

No further action is required from you if your constituents or their infrastructure don't change. Arctic Hub shares the constituent-specific threat intelligence packages automatically. We have an installed base with Arctic Hubs processing millions of events this way every day.