FalconForce

Supporting SOCs with premium detection content

We help you detecting advanced adversaries

To detect and catch advanced and ever-evolving cyber adversaries, you need sophisticated and up-to-date detection content. Creating this quality detection content requires constant effort, expertise and time from often understaffed SOC teams.

We offer a way to save your security team's time, and provide access to a steady stream of great detection content. So your team can focus on what really matters: keeping your organization secure.

With premium, constantly improved, detection content

Our detection content is focused on Splunk, Azure Sentinel, and Microsoft Defender for Endpoints. The curated use-cases are tailored to the client and implemented by FalconForce professionals in your own environment.

We offer subscription-based packages of 10 use-cases per month. This package includes per use-case:

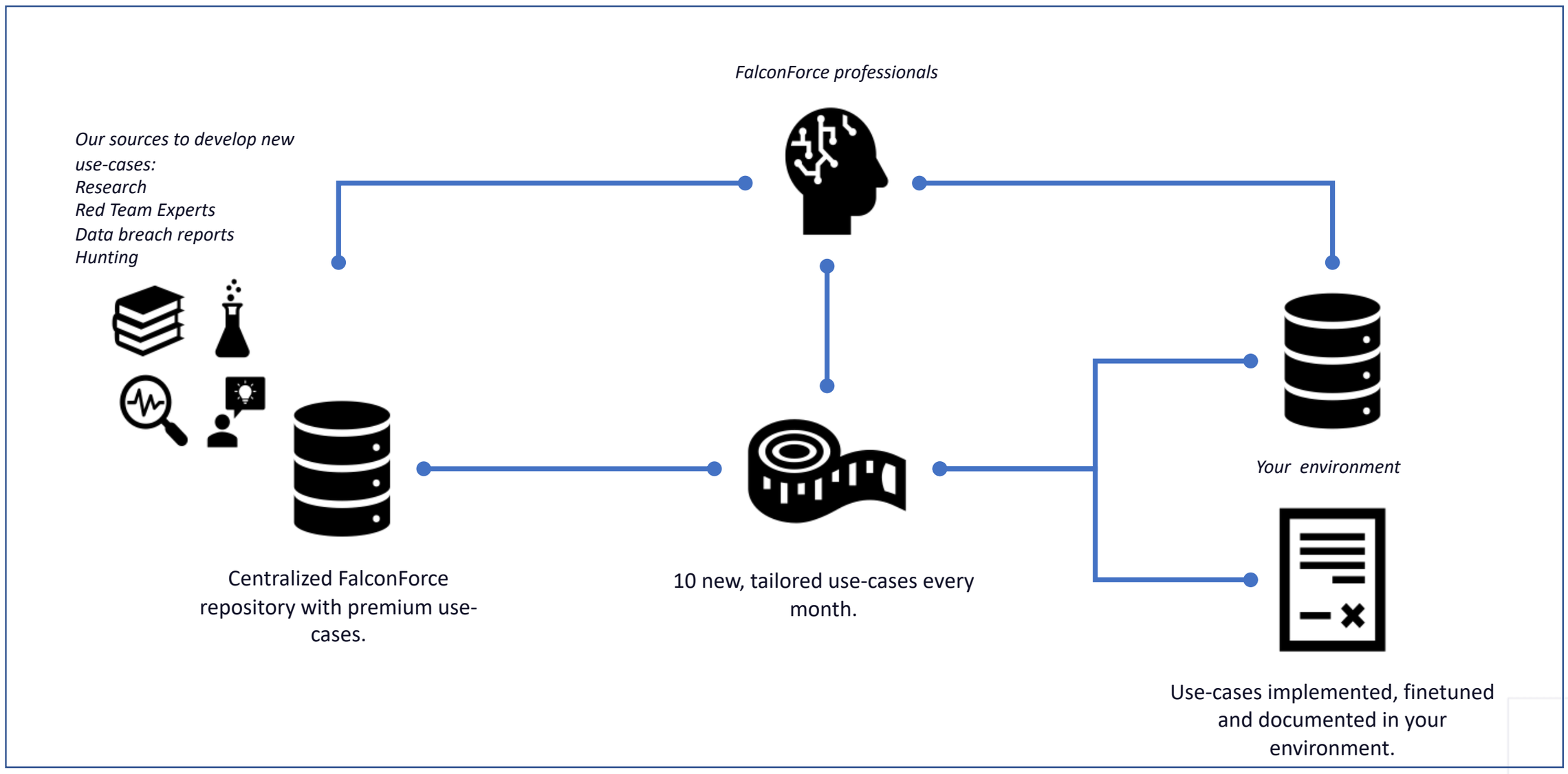
- KQL or SPL query and meta-data.
- Use-case documentation.
- Deployment and finetuning use-case in your environment.
- Use-case maintenance.

And onboarding you is easy

During the onboarding process, we will make an inventory of your existing use-cases, internal processes and systems involved with the use-case development process.

Together we make a roadmap based on current threats and detection coverage (e.g., MITRE ATT&CK).

In case you would like to go faster or have no content yet: we have optional accelerator packages that can rapidly increase the detection content in your environment.



High-level process overview of content subscription

Would you like to know more?

info@falconforce.nl

https://falconforce.nl

@falconforceteam

https://linkedin.com/company/falconforce

FalconForce