FalconForce

SENTRY DETECT

Enhancing threat detection with bespoke detection content

Olaf Hartong

Detection Engineer and Security Researcher

- Purple teaming, Threat hunting
- Microsoft Security MVP

Former documentary photographer
Father of 2 boys
“I like **warm hugs**”

@olafhartong
olafhartong.nl
github.com/olafhartong
Olaf falconforce.nl
olafhartong.nl / falconforce.nl

Henri Hambartsumyan

Offensive defender

- Red teaming & detection engineering
- Uses offensive skills to improve detection

Loves evading defensive software
Father of 2 boys

@ 0xffhh
github.com/0xffhh
henri@falconforce.nl
falconforce.nl

About FalconForce

- Founded in 2020 by a group of highly experienced cyber security professionals
- Vision to make cyber security more purple
- Applied research is at the core of everything we do
- Focus on highly technical project in corporates with a high security maturity

Goal of this webinar

1. Explore why custom detection is needed
2. Understand what makes detection engineering so hard
3. Learn how to approach detection engineering
4. Discover managed detection engineering

Why do we need custom detection content?

Do we need more detection content?

Built-in detections are sufficient against low-skill attackers

Built-in detections need to work for everyone, worldwide!

Attackers test their detections against built-in content

Custom detections are built and tuned for your environment

Why does my security product have blindspots?

Limited research effort

Security vendors often focus on detecting public tradecraft, rarely on new or modified techniques

Limited tuning possibilities

Built-in tuning tools only support basic tuning options. Complex, correlation based tuning not supported.

Cloud complexity

Requires understanding on how YOU use your cloud

Lacking correlation

Detection relies on single-vendor data with minimal cross-product correlation

Needs to work for everyone

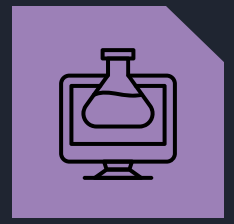
Detection logic lacks tailoring, aiming for global reliability

Lacks detailed understanding

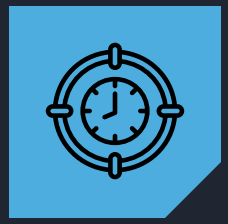
Detection needs deep environmental and infrastructure insights

Why is detection engineering hard?

Hands-on offensive skills



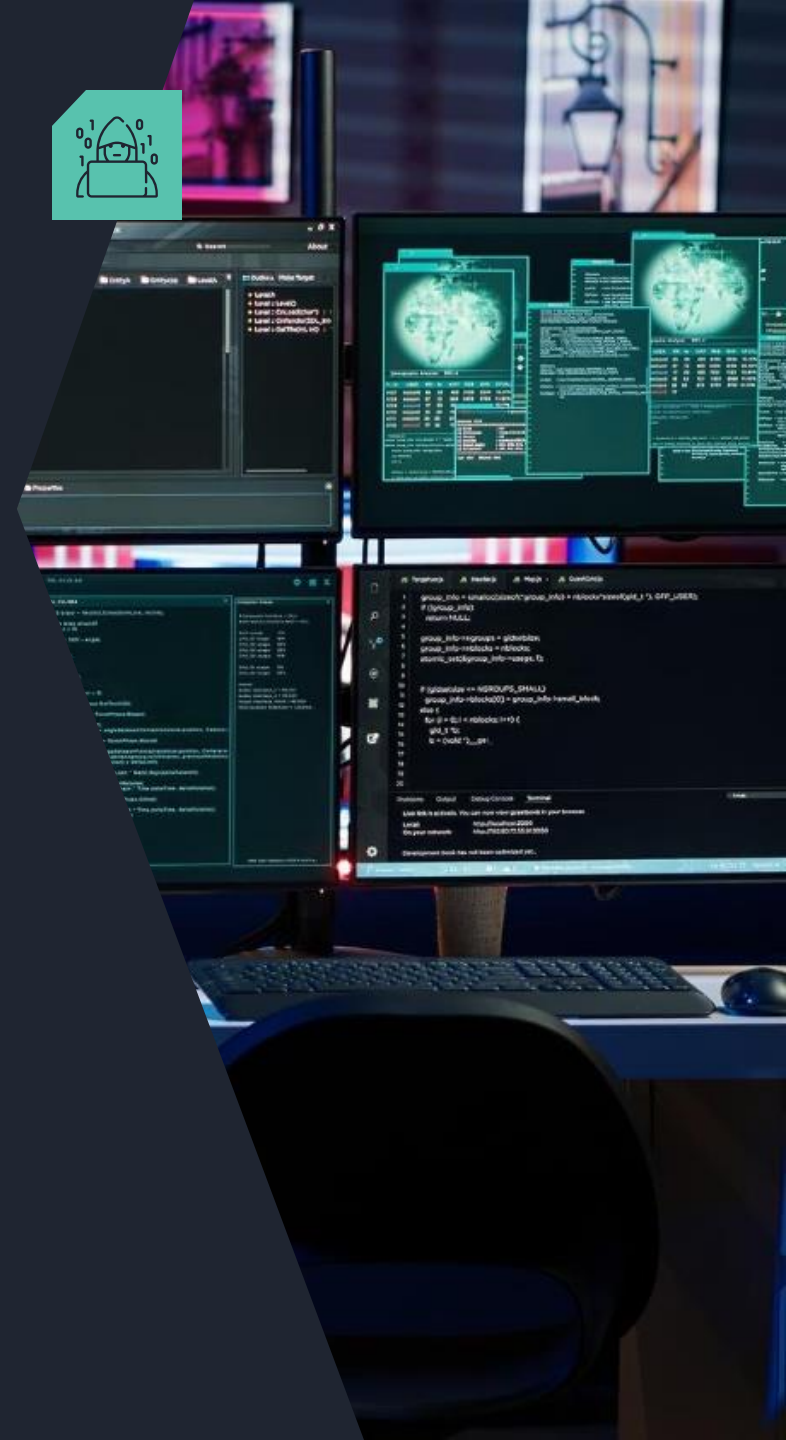
Realistic lab environment



Time and focus

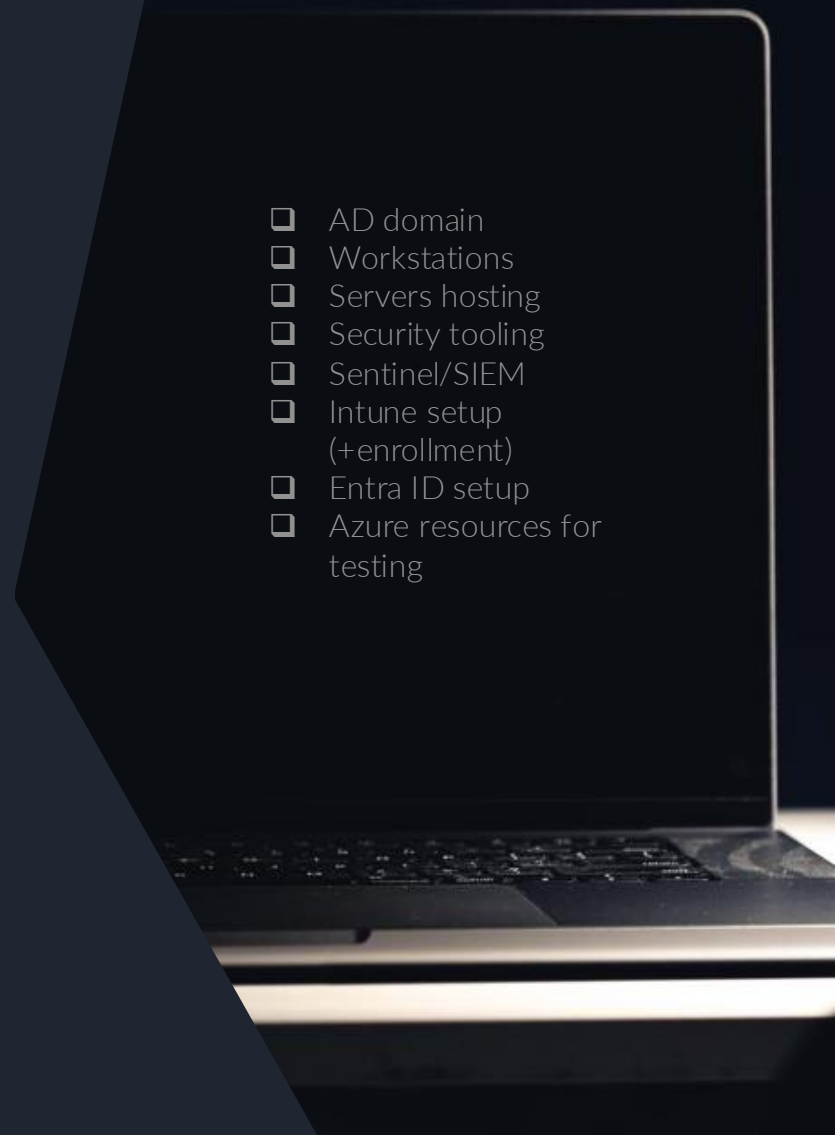
Hands-on offensive skills

- Executing attacks for telemetry requires strong offensive security skills
- They must also possess blue team skills to create production-ready detections
- Splitting roles is possible but sacrifices efficiency and finesse



Realistic lab environment

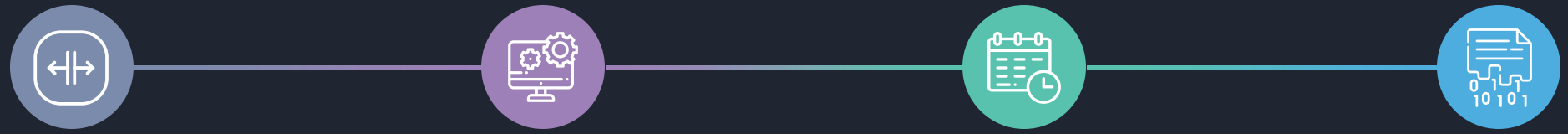
- Simulating attack techniques requires a realistic lab, as most TTPs can't run in production
- Maintaining a realistic lab for detection engineers demands significant effort
- Organizations vary in environments, including Linux, Mac, AWS, and GCP
- Labs need regular cleanup due to disruptions from attack techniques and untrusted tools



Time and focus

- Proper detection engineering requires 1-2 full-time engineers
- Creating a production-ready detection takes 1-3 days, including engineering, testing, and documentation
- Detection engineering needs dedicated time and focus, not just during downtime

How we approach detection engineering



Environment completely separated from any “production”

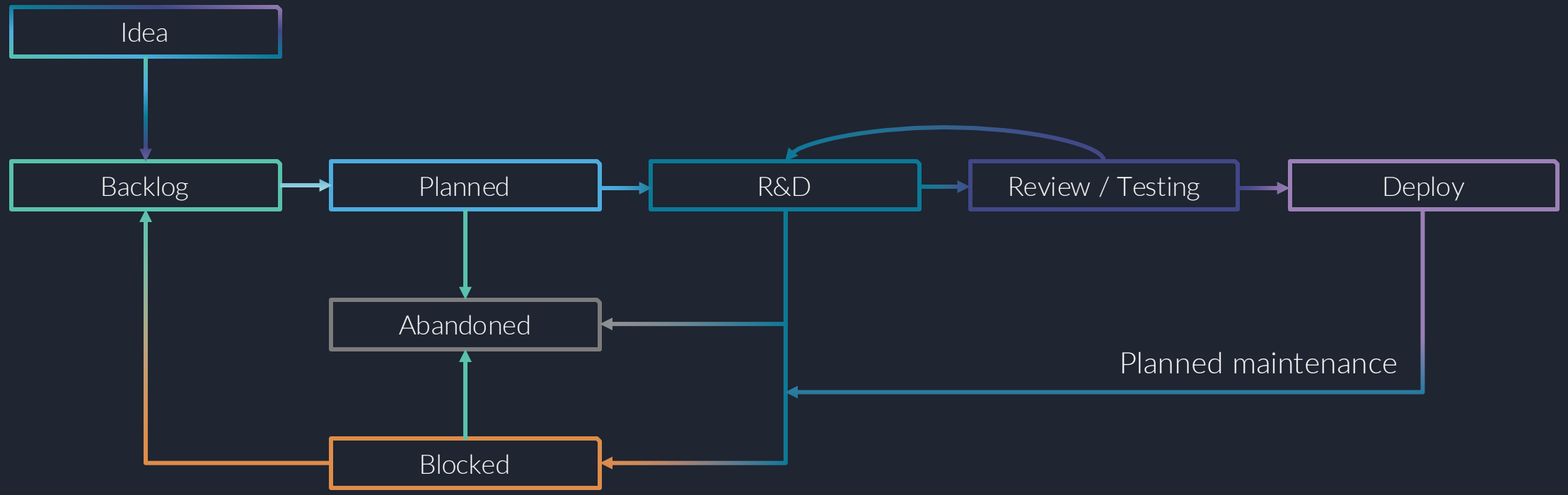
- Offensive
- Detection engineering

Services and tools that are seen in a common enterprise

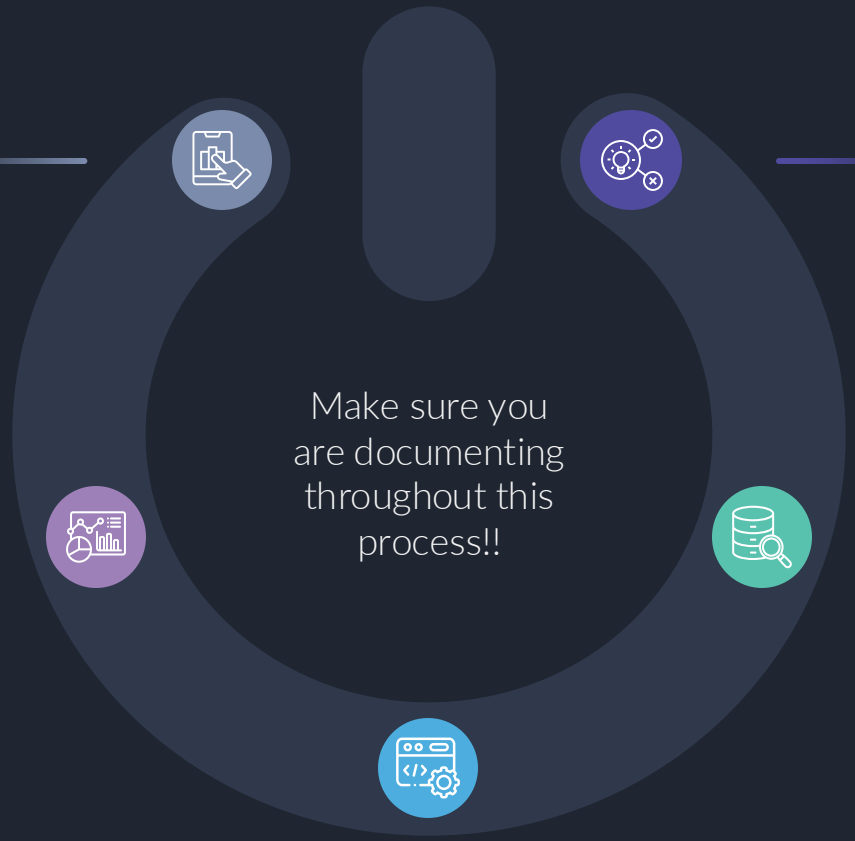
Patches installed and snapshotted every month

Stuff breaks approximately once per month – bitrot

Our (simplified) process flow



FalconForce Detection engineering cycle



1. Hypothesize

2. Investigate & research

3. Develop analytics

4. Analyze & implement

5. Report & revise

Automation

People make mistakes – you can use automation to catch mistakes as early as possible

Git is the single source of truth. Everything else is derived from the version on git.

Automation use cases

- ❑ Syntax validation of the produced output by detection engineer
- ❑ Semantic validation of “standards” (e.g., naming convention, time conventions, function usage, etc.)
- ❑ Automatic deployment to your security tools
- ❑ Generating (and export) nice looking documentation files (Confluence/Markdown/ Word/…)
- ❑ Generating MITRE ATTACK mappings for reporting
- ❑ Performing generic maintenance tasks (e.g., are the URLs in my documentation still active?)

More on automation in the next webinar!

Testing

Recent examples

- 1 out of 14 DCs stopped sending security event logs
- Microsoft has accidently excluded XLL loads from the DeviceImageLoadEvents table.
- GraphAPI logs started to behave erratic, only a small percentage of logs makes it into Sentinel – rest is lost.
- The log format has changed in Azure, the same action now triggers slightly different looking telemetry.

- Detection break silently all the time: you need to test detections!
- World around us has changed (intentionally)
- Something in the IT stack is broken (accidentally)

Minimal Tools

- Lab as discussed before
- Clean VMs to work from
- A solid editor for working with YAML files (VSCode)

Why Managed Detection Engineering?

1. Struggle to build high-fidelity detections which catch advanced actors
2. Common detection engineering mistakes often go unrecognized
3. Limited resources hinder adapting detections to evolving threats

What we offer

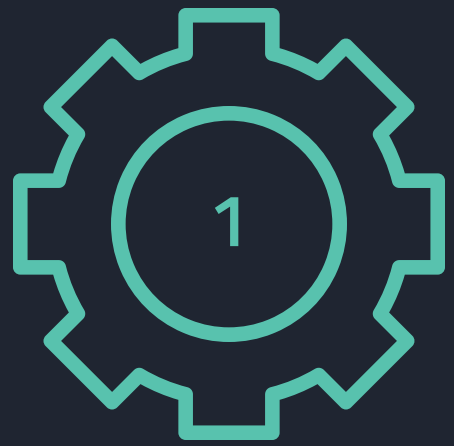
High-fidelity MS stack detections, detecting attacker behavior instead of tools

Built and tested by purple teamers that have hands-on offensive security expertise

Implemented and maintained for you

Low number of false-positives

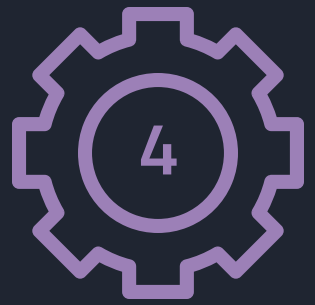
Sentry Detect – Managed Detection Engineering



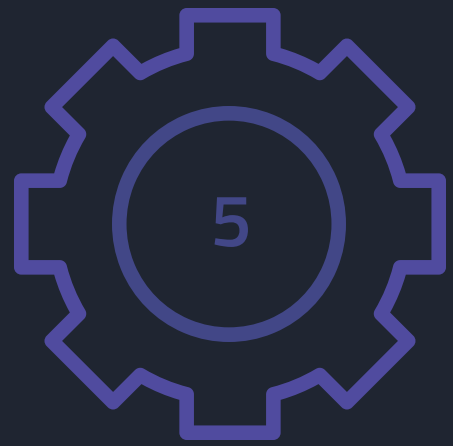
You choose detections from our portal - we give recommendations based on your environment

We validate if the detections are feasible in your environment

We tune detections and stage detections & documentation for deployment



We discuss tuning results together



We (or you) push from staging to production

Sentry Detect – collaboration models

Booster

- Go fast
- One-time fee

- **High fidelity custom detections**

Pro

- Regular new detections
- Subscription

- High fidelity custom detections
- **Detection-as-code pipelines**
- **Maintenance**

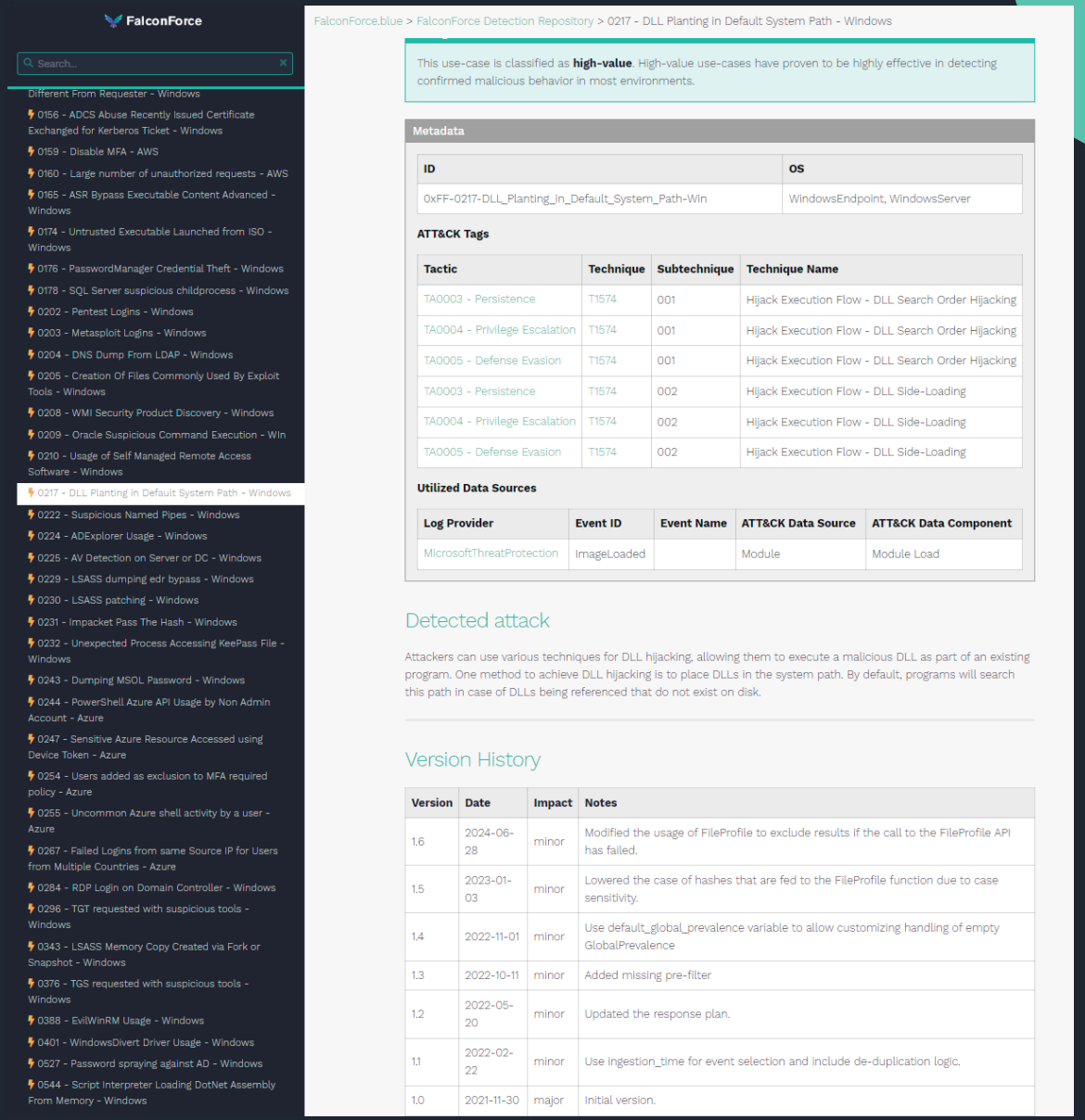
Enterprise

- Deploy and tune together
- Subscription

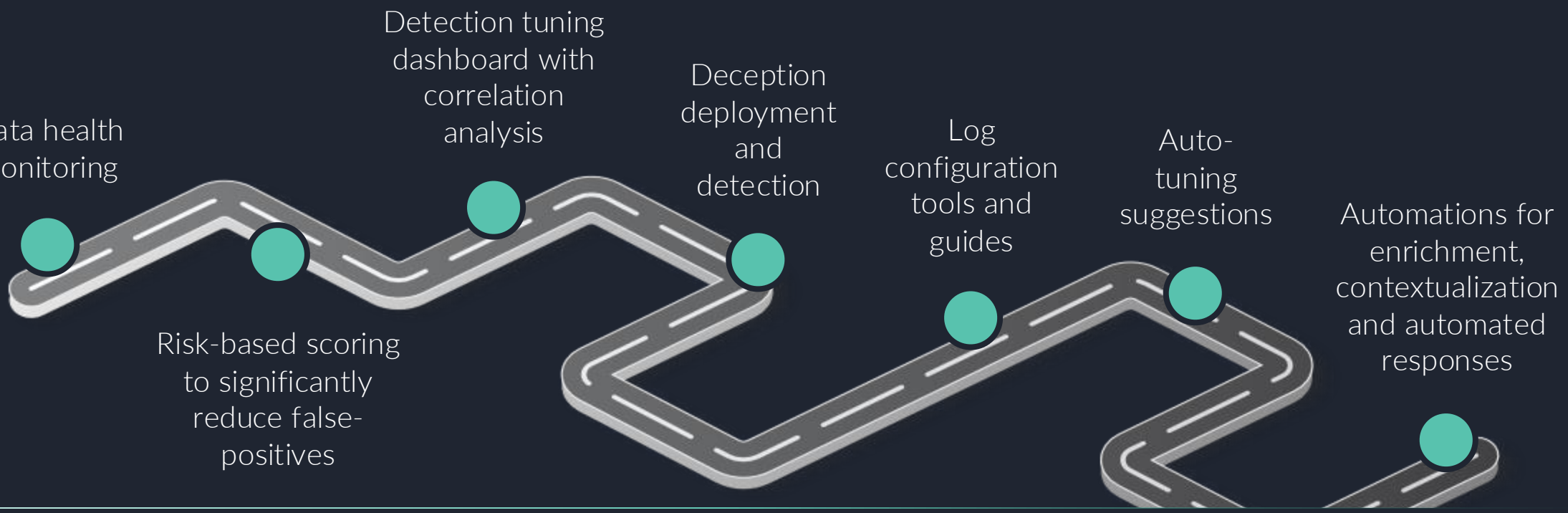
- High fidelity custom detections
- Detection-as-code pipelines
- Maintenance
- **Risk-based scoring dashboard**

Detection library – Live demo

- Depth and breadth of library
- Categorization
- MITRE mapping
- High-value detections



Roadmap



On top of only detection content, we're working on providing other high-quality content for your SOC!

Keep an eye out for the following webinar

Risk-based scoring

Automation

SOAR

Thank you! Questions?

info@falconforce.nl https://falconforce.nl @falconforceteam https://linkedin.com/company/falconforce

Relevant links

FalconFriday – a repository of free detections
https://github.com/FalconForceTeam/FalconFriday/

Deploying Detections at Scale — Part 0x01
https://falconforce.nl/deploying-detections-at-scale-part-0x01/

FalconForge – A basic version of our deployment tool
https://github.com/FalconForceTeam/FalconForge

The slides will be available soon
https://falconforce.nl/

Appendix

Sentry Detect models

Sentry Detect – Managed Detection Engineering

	Booster	Pro	Enterprise
		Usage of custom detection content	
Portal access to content	✅	✅	✅
Deployment automation	✅	✅	✅
Content available	All detections	All detections	All detections
Allowed deployment	Up to 50 detections	5 detections/month	Unlimited, fair use
Tuning and major versions	Up to 50 service credits Used for new detections + tuning	5 service credits/month Used for new detections or major version updates + tuning	10 service credits/month Used for new detections or major version updates + tuning
FalconForce support	❌	Minor version updates Ongoing detection tuning	Minor version updates Ongoing detection tuning
Custom development	❌	✅	✅
Self-deployment & tuning	❌	❌	✅
	Go fast	Regular new detections	Deploy and tune together

Sentry Detect – Managed Detection Engineering

	Booster	Pro	Enterprise
		Pipelines-as-code	
Implementation of pipelines	Optional	✅	✅
Usage of pipelines	Optional	✅	✅
Updates and support	❌	✅	✅
		Risk-based scoring dashboard	
Risk-based scoring engine & dashboard	❌	❌	✅
Updates on engine	❌	❌	✅
		Fee and licensing	
Fee structure	One-time fee	Subscription	Subscription
License model	License to keep	License to use or to keep	License to use or to keep