



FalconForce

SENTRY RESPOND

— Automate smarter. Respond faster. Secure better.






Henri Hambartsumyan

Offensive defender

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

Loves evading defensive software
Father of 2 boys

 @Oxffhh
 github.com/Oxffhh
 henri@falconforce.nl
 falconforce.nl

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






Gijs Hollestelle

Red teamer turned blue teamer

- Building detections and automations
- Dreams in KQL

Recovering CTF addict
Father of 2 boys

 github.com/gijsh
 gijs@falconforce.nl
 falconforce.nl



About FalconForce

- Founded in 2020 by a group of highly experienced red & blue teamers
- ♥ Mission: boost security teams' threat detection & response capabilities
- Applied research is at the core of everything we do
- Focus on highly technical projects in corporates with a high security maturity



What we will cover in this webinar

1

Current challenges with analysis and response

2

Why Microsoft's toolkit is not enough for mature SOCs

3

Why we made the Sentry Respond platform and how it works

4

A live demo of the platform

5

Time for questions & answers



We are actively looking for collaborations!

Contact us if you

Want to do a
proof of
concept with
Sentry
Respond



Have further
input and
feedback based
on what you saw
in this webinar



Are interested in
other
FalconForce
(Sentry) services
or R&D



1

Current challenges

In threat detection & reponse

What's the title of a SOC employee that handles incidents?



We see many organizations struggle



Time wasted
gathering contextual
information and
potential impact for
incidents



Inefficient data
gathering (from
many sources)
and manual
response steps



Complexities to
correlate
incidents over a
large timeframe



Pain to connect
incidents that
are not
automatically
correlated



As a result, the current approach makes it hard to...



Work
efficiently at
scale



Allocate analyst
time where it
matters most



Ensure
consistency and
accuracy under
pressure



Keep analysts
engaged with
meaningful
work

... which ultimately affects decision quality and increases alert fatigue



So, the analyst needs a platform to



1

Automate
(complex)
enrichment and
response steps

2

Reduce number
of alerts to
decrease alert
fatigue

3

Spend their
valuable analysis
time spent on
actual high-risk
incidents

4

Better protect
their company
(and enhance
their job
satisfaction)




2

What does Microsoft offer

To help the analyst fight the good
fight?

What does XDR offer you for enrichments?




webinar-desktop
■ ■ ■ Medium ▲ Medium


[➔ Open device page](#) [🗺 View in map](#) [⬆ Device value](#) [👑 Set criticality](#) ⋮

Logged on users(last 30 days)

Most logons


 **R** [rogier](#)


Newest logon


 **R** [rogier](#)

[View all 2 logged on users](#)

VM details

Category Computers and Mobile	Type Unknown
Subtype Workstation	Discovery sources 
Domain AAD joined	OS Windows 11 64-bit (Release 22H2 Build 22621.5335)
SAM name -	Health state Inactive
Data sensitivity None	IP addresses 10.0.0.6 See IP addresses info



Klaus Mueller
HR Business Partner EMEA |  Enabled | Falcon Unlimited | Dept: HR | +1

[👤 Confirm user compromised](#) ⋮

Overview Policies

Protection ⌵

Last password change
24 Mar 2025 13:08:20

MFA status
Disabled

MFA type
No MFA methods enabled

User threat ⌵

Open incidents
[2](#)

Active alerts
[4](#)

Entra ID risk level
Not available

Insider risk severity
Not available

Source
Entra ID

Blast Radius
-



What does XDR offer you for response actions?

Custom detection

☒ General

☒ Impacted entities

☒ Automated actions

☐ Scope

☐ Review and create

Automated actions

Define actions to automatically take on affected entities in the generated alerts and incidents.

Remediation actions to take

Choose an applicable action to take on entities found by your query.

Devices

☐ Isolate device

☐ Collect investigation package

☐ Run antivirus scan

☐ Initiate investigation

☐ Restrict app execution

Files

☐ Allow/Block

☐ Quarantine file

Users

☐ Mark user as compromised

☐ Disable user

☐ Force password reset

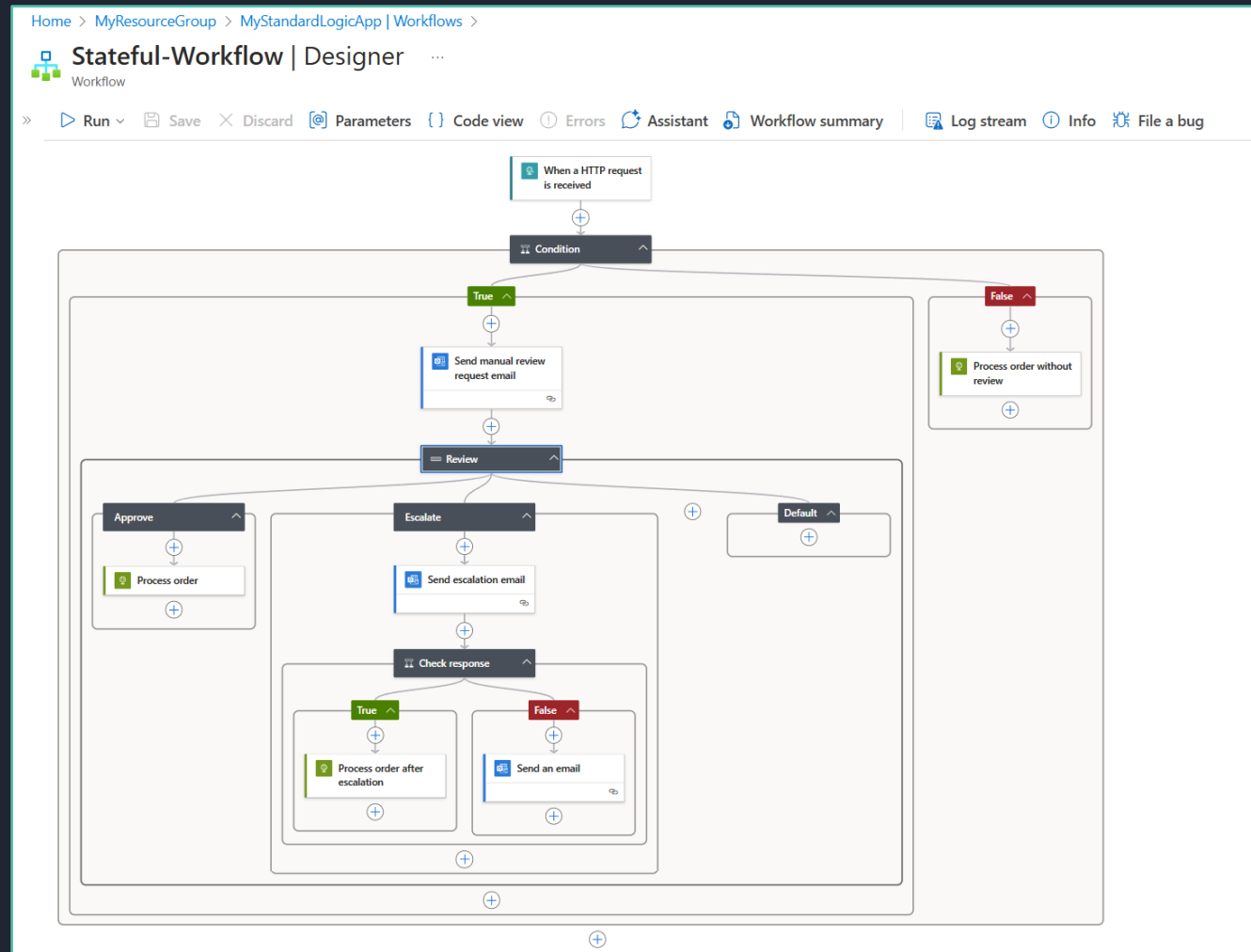
Emails

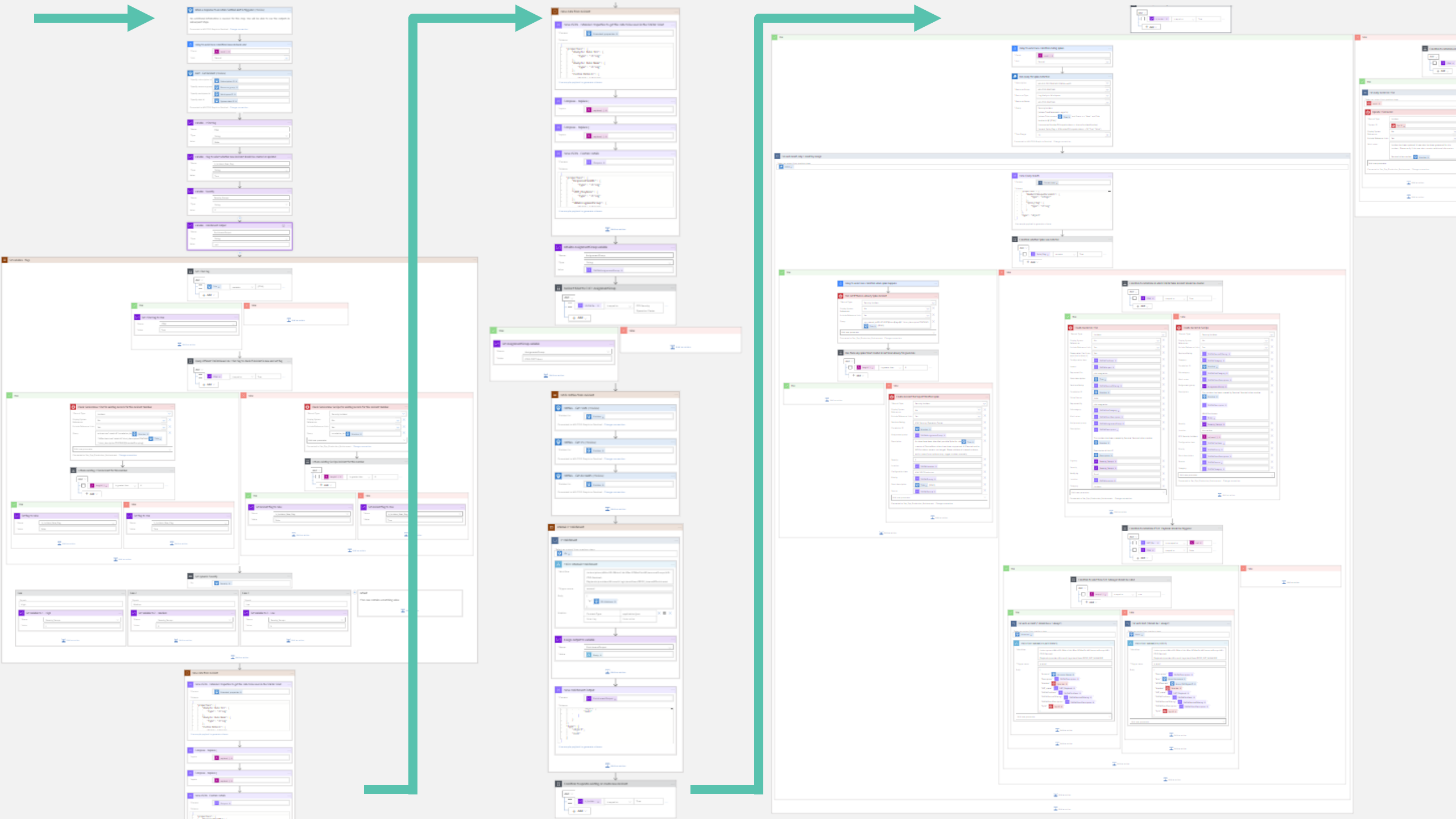
☐ Move to mailbox folder

☐ Delete email



What does Sentinel (in XDR) offer you for automations?





The (top) issues we encounter with the existing platform

Logic apps

1

Nice for simple automation, not for complex SOC

2

Lack of foundation for production grade automations

3

Lack of proper reusability and modular design

XDR enrichments

1

Only Microsoft cloud enrichments: not extendable

2

Enrichments are only “visible” in UI, not usable in automations

3

Enrichment fetched live, slow and not always best option



3

Why Sentry Respond?

An Azure-native solution

Meet Sentry Respond

Build better
automations, faster



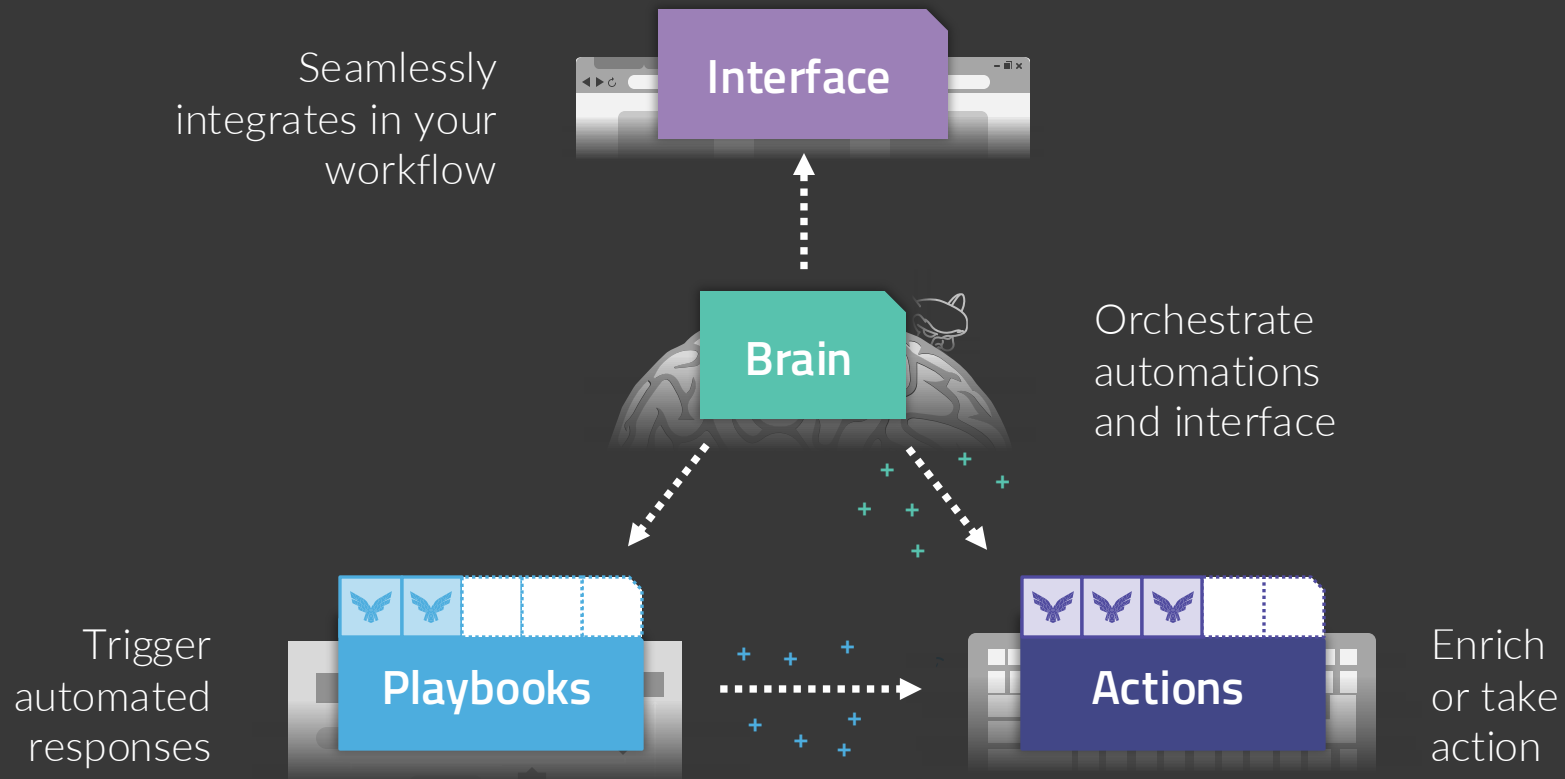
Adapts to your
development needs



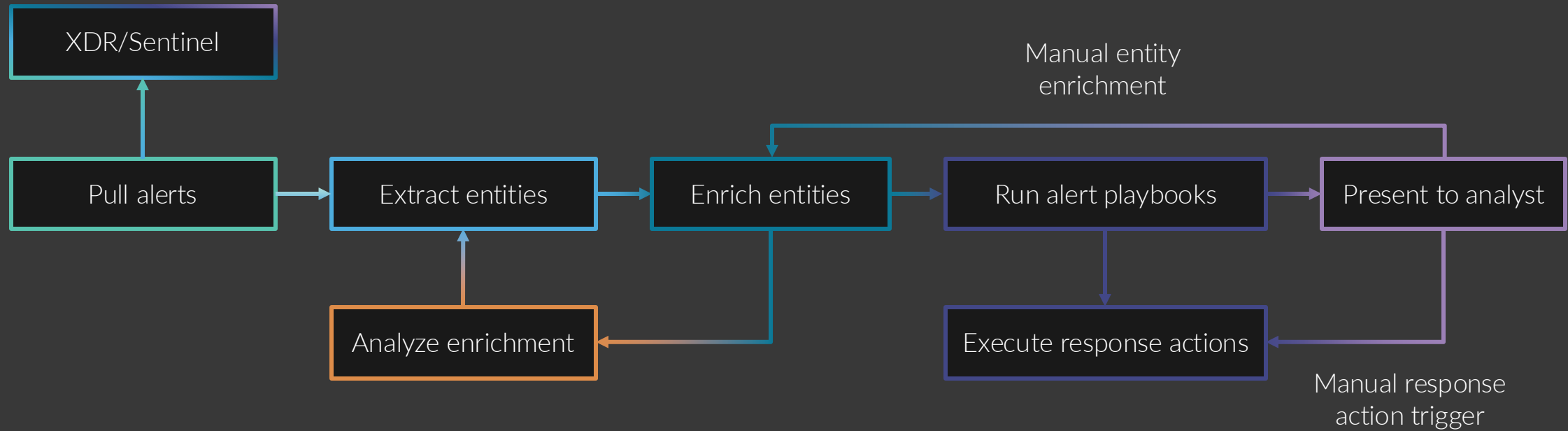
Secure Azure-native
in your tenant



What does Sentry Respond look like?



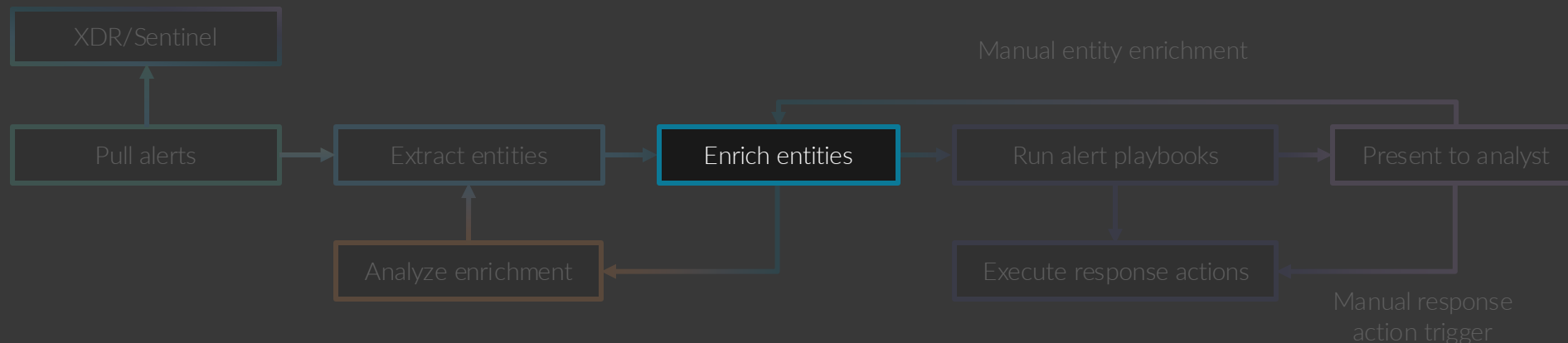
How does Sentry Respond work?





Example enrichments

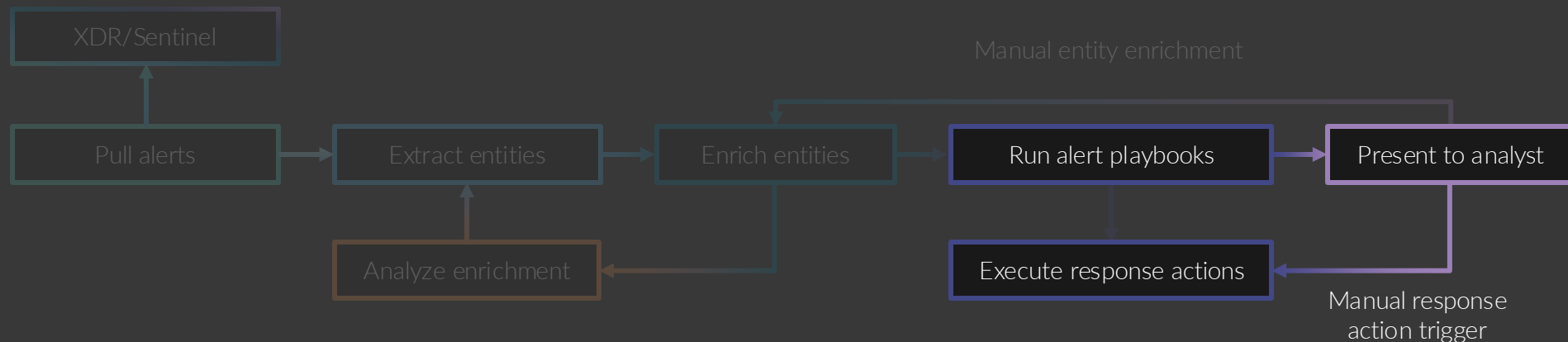
- Fetch HR info on a user from SailPoint
- Lookup blast radius of a service principal in BloodHound (Enterprise) / exposure management
- Obtain recently issued HTTPS certificates for a domain
- Lookup application owner / details from Service Now using a hostname





Example response action

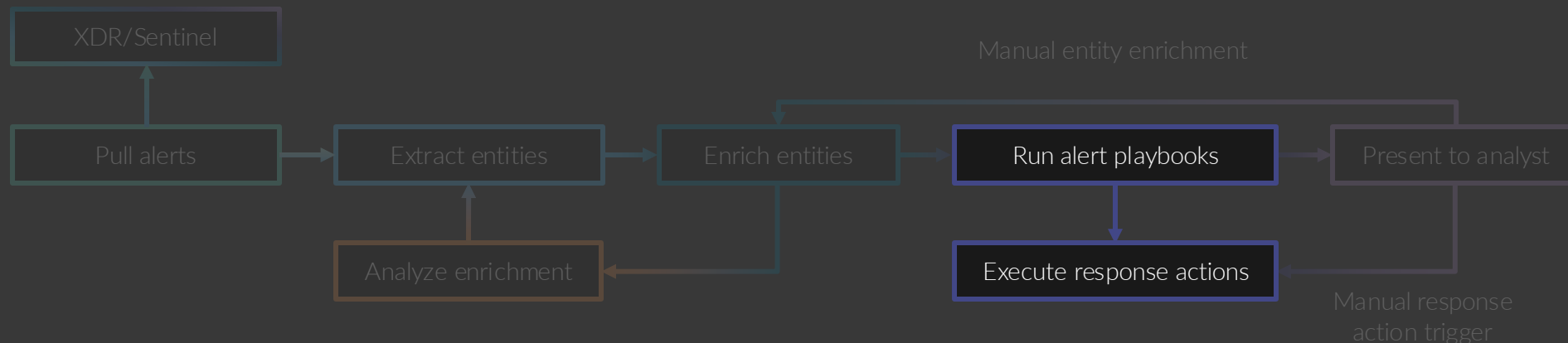
- Block user / force password reset in EntraID
- Take screenshot from a webpage in a sandbox
- Send teams message and wait for response
- Block outbound HTTP traffic for this host in Zscaler
- Store object in SOC blob storage / SharePoint / Teams



Example playbook triggering automated response actions



- Take a screenshot of a website if a phishing mail is reported
- Close impossible travel alert if the first source IP is from country X and the second source IP is our VPN range
- If a phishing alert is classified as true positive, force password reset for all users that clicked the link. Reset all active Entra ID session of users that clicked the link. Add list of all users that clicked the link to closing notes of case in Jira



What are the key differentiators?

Modular system

Easily integrates with any API-enabled system, providing flexible, rule-based actions tailored to you.

Automation results cached

All enrichment data is cached to minimize API calls to external systems. Caching is based on configurable conditions.

UI integrates with XDR

The UI integrates seamlessly in an analyst workflow using a browser plugin or Sentinel workbook. It shows relevant data to accelerate analyst investigations.

Flexible automations in any language

Automate in your preferred language. Native support for Logic Apps, REST APIs, and a robust C# SDK.

Entity normalization

Sentry Respond systematically normalizes and tracks entities for consistent and reliable analysis.

Resilient by design

Built-in resilience ensures robust error handling and transparent logging, freeing your automations from manual error management.



Modular system



- You can build playbooks and actions.
- FalconForce provides you with a growing library of actions and playbooks. To be used as is or modified to your requirements.
- Integrates with any internal OR external system. As long as there is a network connection and an interface.



Modular system



servicenow®



Microsoft
Threat
Intelligence



What are the key differentiators?

Modular system

Easily integrates with any API-enabled system, providing flexible, rule-based actions tailored to you.

Automation results cached

All enrichment data is cached to minimize API calls to external systems. Caching is based on configurable conditions.

UI integrates with XDR

The UI integrates seamlessly in an analyst workflow using a browser plugin or Sentinel workbook. It shows relevant data to accelerate analyst investigations.

Flexible automations in any language

Automate in your preferred language. Native support for Logic Apps, REST APIs, and a robust C# SDK.

Entity normalization

Sentry Respond systematically normalizes and tracks entities for consistent and reliable analysis.

Resilient by design

Built-in resilience ensures robust error handling and transparent logging, freeing your automations from manual error management.



Flexible automations in any language

A circular icon with a dark blue border containing the code symbols "</>" in white.

- Need a simple automation? Use a logic app with HTTP trigger.
- Want to build Python automations? Deploy as Azure function with REST API and automate away.
- Prefer a full object model for developing, debugging and maintaining (complex) automations? Use the C# SDK.



What are the key differentiators?

Modular system

Easily integrates with any API-enabled system, providing flexible, rule-based actions tailored to you.

Automation results cached

All enrichment data is cached to minimize API calls to external systems. Caching is based on configurable conditions.

UI integrates with XDR

The UI integrates seamlessly in an analyst workflow using a browser plugin or Sentinel workbook. It shows relevant data to accelerate analyst investigations.

Flexible automations in any language

Automate in your preferred language. Native support for Logic Apps, REST APIs, and a robust C# SDK.

Entity normalization

Sentry Respond systematically normalizes and tracks entities for consistent and reliable analysis.

Resilient by design

Built-in resilience ensures robust error handling and transparent logging, freeing your automations from manual error management.



Slide on built-in caching



- Prevents hitting API limits / credits
- Faster / more efficient



What are the key differentiators?

Modular system

Easily integrates with any API-enabled system, providing flexible, rule-based actions tailored to you.

Automation results cached

All enrichment data is cached to minimize API calls to external systems. Caching is based on configurable conditions.

UI integrates with XDR

The UI integrates seamlessly in an analyst workflow using a browser plugin or Sentinel workbook. It shows relevant data to accelerate analyst investigations.

Flexible automations in any language

Automate in your preferred language. Native support for Logic Apps, REST APIs, and a robust C# SDK.

Entity normalization

Sentry Respond systematically normalizes and tracks entities for consistent and reliable analysis.

Resilient by design

Built-in resilience ensures robust error handling and transparent logging, freeing your automations from manual error management.



Entity normalization



- Is henri@falconforce.nl , falconforce\henri or S-1-5-21-3623811015-3361044348-30300820-1013 the same user? Brain tells you.
- Is user “Administrator” in this alert the same as the user “Administrator” in the other alert? Brain tells you.
- Is azure resource “/subscription/f3a9e2c4-7b16-4f26-9c8f-1dba4be2e935” the same as subscription “Hello World”? Brain tells you.



What are the key differentiators?

Modular system

Easily integrates with any API-enabled system, providing flexible, rule-based actions tailored to you.

Automation results cached

All enrichment data is cached to minimize API calls to external systems. Caching is based on configurable conditions.

UI integrates with XDR

The UI integrates seamlessly in an analyst workflow using a browser plugin or Sentinel workbook. It shows relevant data to accelerate analyst investigations.

Flexible automations in any language

Automate in your preferred language. Native support for Logic Apps, REST APIs, and a robust C# SDK.

Entity normalization

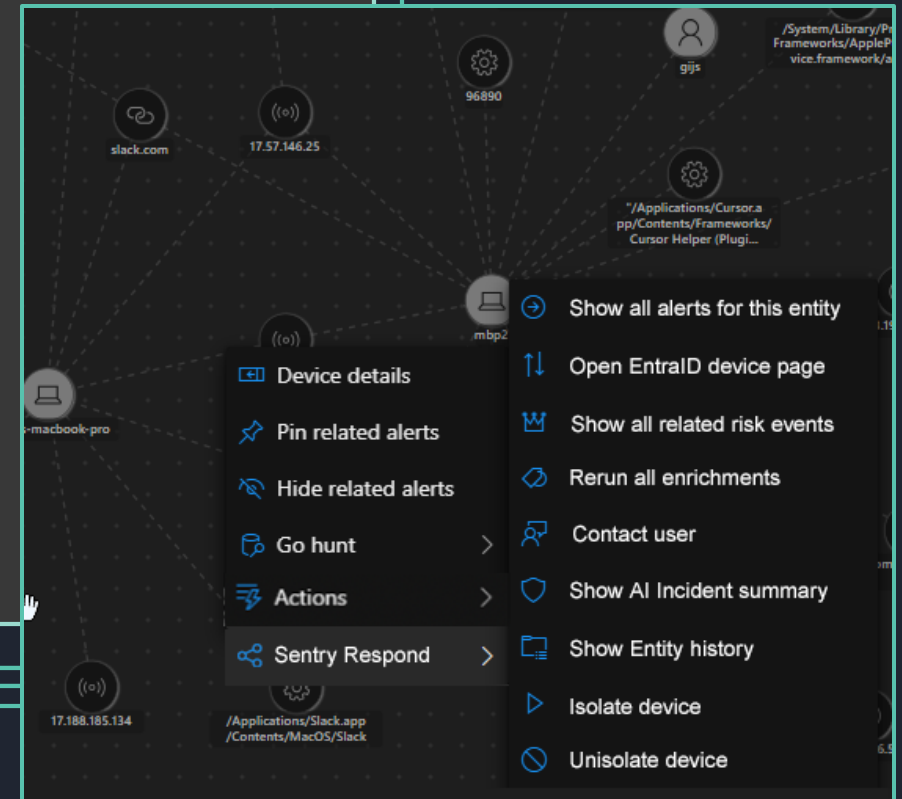
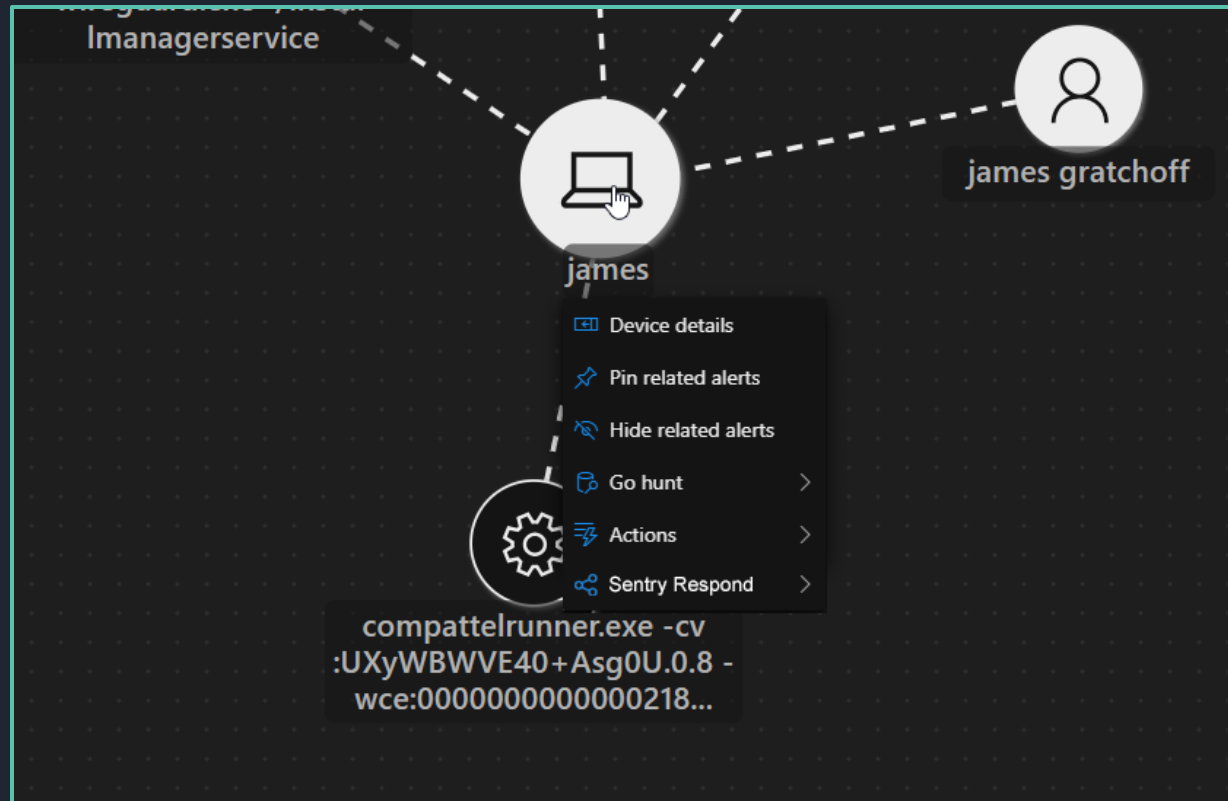
Sentry Respond systematically normalizes and tracks entities for consistent and reliable analysis.

Resilient by design

Built-in resilience ensures robust error handling and transparent logging, freeing your automations from manual error management.



User Interface of Sentry Respond (experimental)



What are the key differentiators?

Modular system

Easily integrates with any API-enabled system, providing flexible, rule-based actions tailored to you.

Automation results cached

All enrichment data is cached to minimize API calls to external systems. Caching is based on configurable conditions.

UI integrates with XDR

The UI integrates seamlessly in an analyst workflow using a browser plugin or Sentinel workbook. It shows relevant data to accelerate analyst investigations.

Flexible automations in any language

Automate in your preferred language. Native support for Logic Apps, REST APIs, and a robust C# SDK.

Entity normalization

Sentry Respond systematically normalizes and tracks entities for consistent and reliable analysis.

Resilient by design

Built-in resilience ensures robust error handling and transparent logging, freeing your automations from manual error management.



Resilient by design



- Dealing with APIs requires resilience.
- What if an API is (temporary) down or hitting rate limits ?
- You don't have to write this error handling code in every automation. Brain has sane defaults, and you can configure it the way you like.
- Something went wrong with Brain or you automation in ops? Full logging and call graphs available for troubleshooting.



Resilient by design



▼ OTHER ObtainInvestigationPackage	...	5.1 mins	[Progress bar]		
▼ OTHER InitiateInvestigationPackageCollection		367.1 ms	:		
login.microsoftonline.com	POST /a92a42cd-bf8c-46ba-a	200	145.5 ms	:	
api.securitycenter.microsoft.com	POST /api/machines/a	201	211.1 ms	:	
▼ OTHER FetchDownloadUrl		203.3 ms	:		
login.microsoftonline.com	POST /a92a42cd-bf8c-46ba-a	200	113.6 ms	:	
api.security.microsoft.com	GET /api/machineactions/87d	400	87.2 ms	:	
▼ OTHER FetchDownloadUrl		292.8 ms	:		
login.microsoftonline.com	POST /a92a42cd-bf8c-46ba-a	200	111.9 ms	:	
api.security.microsoft.com	GET /api/machineactions/87d	400	177.6 ms	:	
▼ OTHER FetchDownloadUrl		155.9 ms	:		
login.microsoftonline.com	POST /a92a42cd-bf8c-46ba-a	200	109.8 ms	:	
api.security.microsoft.com	GET /api/machineactions/87d	400	44.6 ms	:	
▼ OTHER FetchDownloadUrl		139.9 ms	:		
login.microsoftonline.com	POST /a92a42cd-bf8c-46ba-a	200	83.9 ms	:	
api.security.microsoft.com	GET /api/machineactions/87d	400	54.7 ms	:	
▼ OTHER FetchDownloadUrl		366.2 ms	:		
login.microsoftonline.com	POST /a92a42cd-bf8c-46ba-a	200	128.9 ms	:	
api.security.microsoft.com	GET /api/machineactions/87d	200	235.2 ms	:	
wdatpprd-weu.securitycenter.windows.com	GET /api/cloud	200	956.7 ms	:	
▼ BlobContainerClient.CreateIfNotExists		74.1 ms	:		
ffsesabrainb5a24a	PUT ffsesabrainb5a24a	409	35.4 ms	:	
▼ BlobClient.Upload		519.1 ms	:		
ffsesabrainb5a24a	PUT ffsesabrainb5a24a	201	514.1 ms	:	





Sentry Respond

Modular system

Easily integrates with any API-enabled system, providing flexible, rule-based actions tailored to you.

Automation results cached

All enrichment data is cached to minimize API calls to external systems. Caching is based on configurable conditions.

UI integrates with XDR

The UI integrates seamlessly in an analyst workflow using a browser plugin or Sentinel workbook. It shows relevant data to accelerate analyst investigations.

**Everything runs in your
Azure environment**



**All data remains under
your control**

Automations in any language

Automate in your preferred language. Native support for Logic Apps, REST APIs, and a robust C# SDK.

Entity normalization

Sentry Respond systematically normalizes and tracks entities for consistent and reliable analysis.

Resilient by design

Built-in resilience ensures robust error handling and transparent logging, freeing your automations from manual error management.

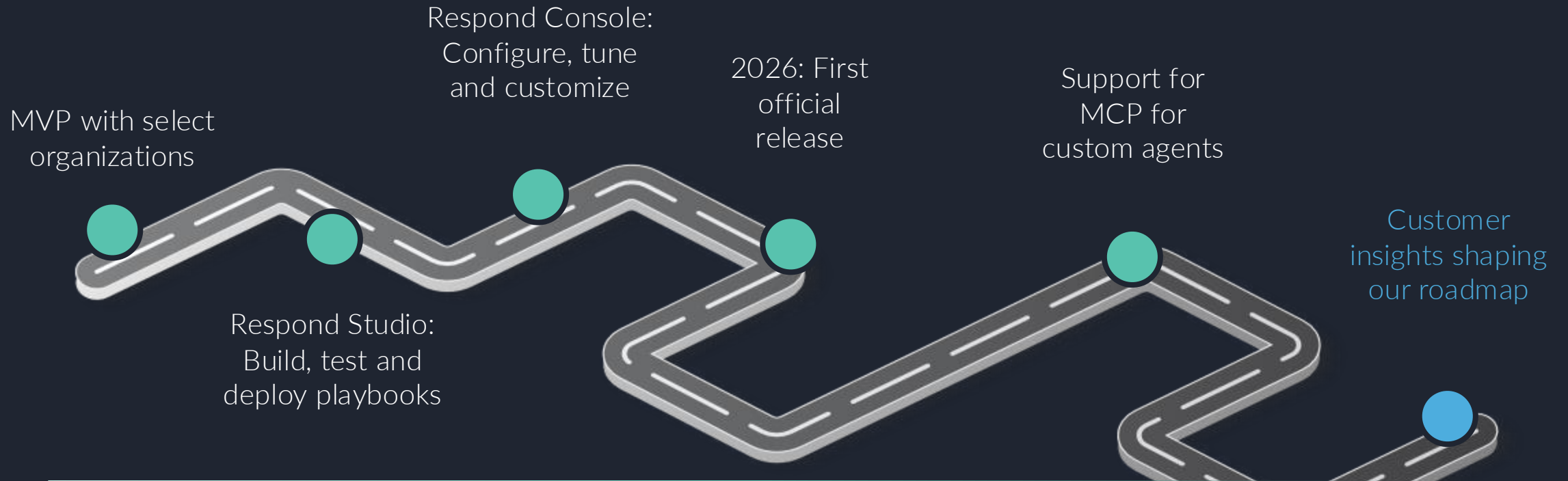


4

Live Demo!

Experience Sentry Respond

Roadmap



New content is being added continuously for integration with (third-party) systems.



We are actively looking for collaborations!

Contact us if you

Want to do a
proof of
concept with
Sentry
Response



Have further
input and
feedback based
on what you saw
in this webinar



Are interested in
other
FalconForce
(Sentry) services
or R&D



5

Questions & Answers

(Hopefully)



Thank you! Questions?



info@falconforce.nl



<https://falconforce.nl>



[@falconforceteam](https://twitter.com/falconforceteam)



<https://linkedin.com/company/falconforce>