MICROSOFT SENTINEL USER FORUM

Session #7

26/10/2023

CONTENTS

01 **INTRODUCTION – 10’**

Objectives of MS Sentinel User Forum fifth session

02 **THIRD-PARTY DATA INGESTION – 45’**

03 **THE NEVER ENDING STRUGGLE : INCIDENT OPTIMIZATION – 45’**

04 **REMINDER OF NEXT SUBJECTS**

05 **CLOSE**

1 INTRODUCTION – 10’

Introduction

Seventh session objectives

Various information sharing

- General Recap
- Introduce new joiners
- Share various information

Content session

Third-party data ingestion
Robbe Van den Daele

The never-ending struggle : incident optimization
Louis Mastelinck

Reminder of next subjects

- Remind the next sessions agenda and start preparing topics

Various information

New joiners

Please extend a warm welcome to the new members of the Forum :

- The Collective (Belgium)
  - Robbe Van den Daele

Companies: 23

Members: 47

Various information

Leavers

The following persons moved within or left their company, and are no longer part of the forum:

- From InSpark (Netherlands):
  - Achraf Chennan
  - Alex Shaer

Membership

Outlined below are the principles for membership of the Sentinel User forum

1. Organisation must be users of MS Sentinel or supply services related to MS Sentinel
2. Sentinel end user organisations, consulting firms, SOC service provides can be members of the community
3. New members must be invited by an existing member of the community
4. Members must have signed the relevant NDA with Microsoft
5. The contact details of participants of the forum will be open to all participants
6. Participants are allowed to directly contact other participants of the forum

Meeting governance

Outlined below are the principles for meeting governance

1. Meetings will be held every 3 months
2. Each meeting will be 2 hours in duration
3. The chair of the meeting is accountable to supply meeting minutes to the attendees of the meeting.
4. Meetings are held under Chatham house rule (https://www.chathamhouse.org/about-us/chatham-house-rule)
5. No entity will attempt to sell product or services within the forum meetings

2

THIRD-PARTY DATA INGESTION – 45’

Who am I?

Overview

- Robbe Van den Daele
- Security Engineer/SOC Analyst @ The Collective
- Microsoft Technology; Security Procedures; MITRE ATT&CK Gap Analysis
- https://hybridbrothers.com

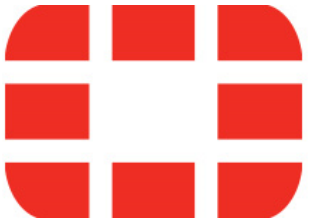
01

How to forward logs to Sentinel

Custom log ingestion

Custom log ingestion

- In most cases (but not limited to) syslog forwarding
- On-premise devices / security appliances



Did you integrate third-party solutions in Sentinel via syslog already?

Custom log ingestion

Why

- Detect threats and correlate data
- Full control of normalization and filtering
- Ingest data in standard and custom tables
- Split verbose and non-verbose logs

Pitfalls

- Implementation complexity
- Custom normalization and filtering
- Different parts

FORWARD AGENT TYPES

01

Microsoft Monitoring Agent (MMA)

02

Azure Monitoring Agent (AMA)

03

Third-party solutions

Microsoft Agent Types

Microsoft Monitoring Agent

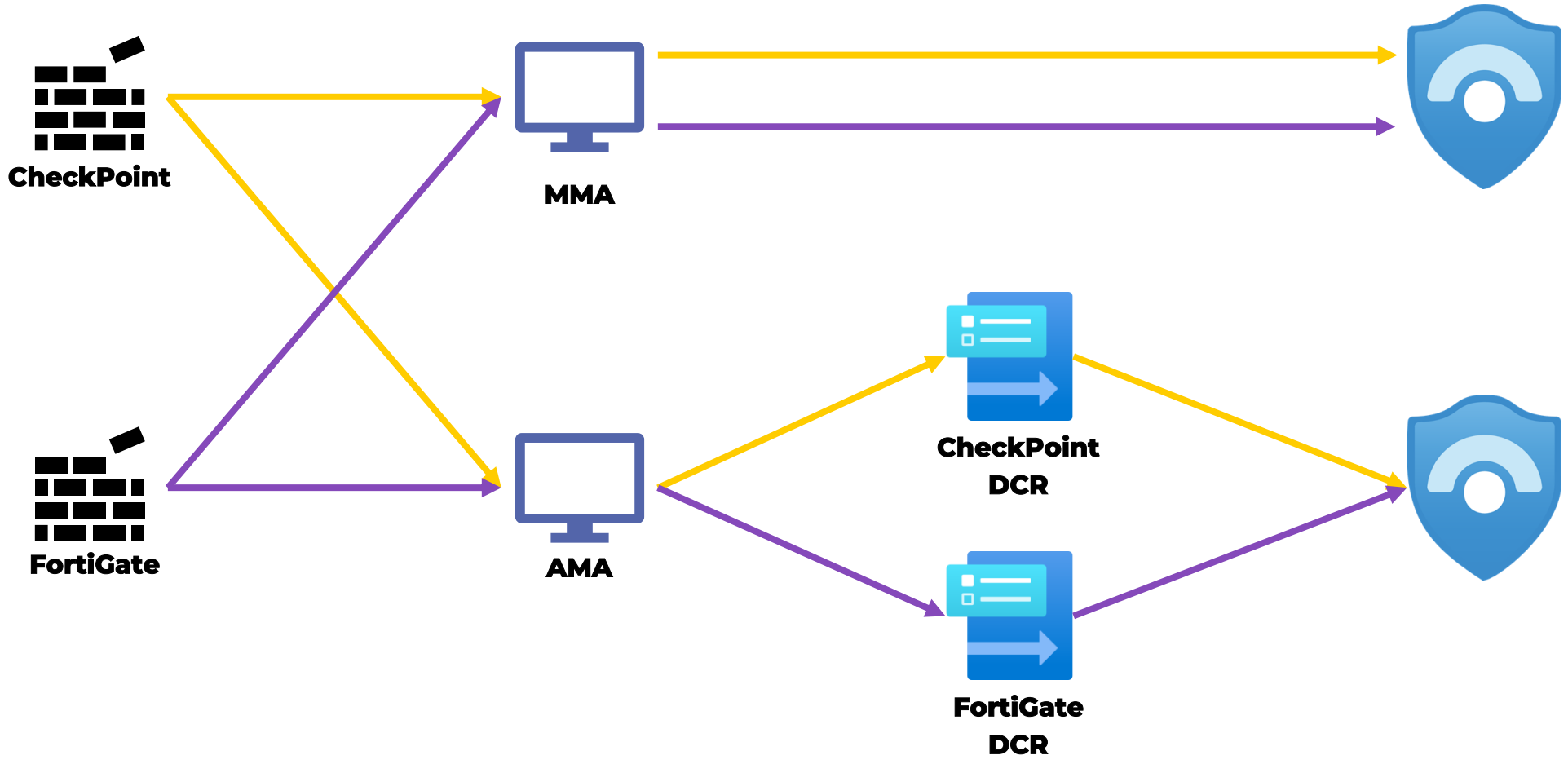
- Legacy
- Less flexibility
- No data transformations
- Connected to Log Analytics Workspace
- End of life: Augustus 2024

Azure Monitoring Agent

- More flexibility
- Data transformations available
- Association to DCRs
- Azure ARC

Ingesting Windows Security Logs
Ingesting Linux Syslog data
Ingesting 3rd party syslog (syslog forwarder)

Microsoft Agent Types



Microsoft Agent Types

MMA

AMA

AMA VS Third-party Logstash

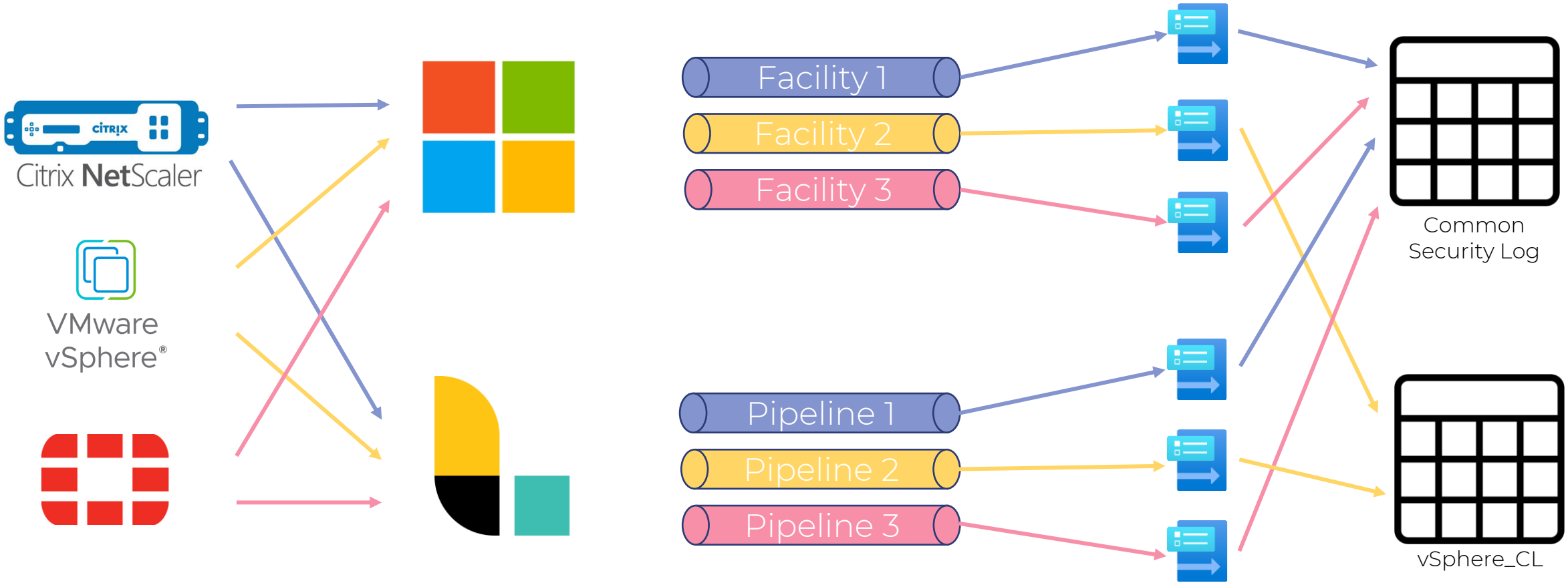
Azure Monitoring Agent

- Easier than Logstash
- Normalization and transformation via DCR

Logstash

- Local filtering possible
- DCR support
- Can run in containers
- Not limited to Syslog data
- No Azure ARC onboarding

AMA VS Third-party Logstash



Which forwarding solution are you using?

02

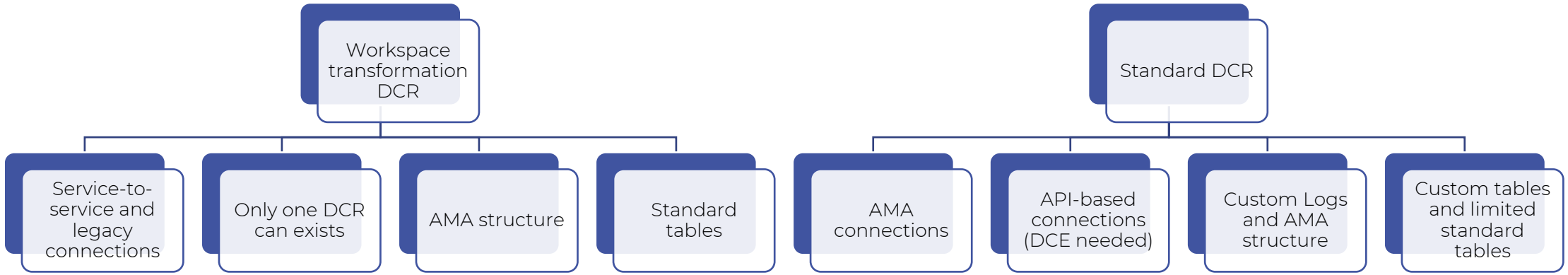
Data collection rules

Into the rabbit hole

Did you use data collection rules before?

Data Collection Rules – Structure

Data Collection Rules – Workspace VS Standard



Want a deep dive?

Demystifying Data Collection Rules and Transformations (hybridbrothers.com)

03

Creating pipelines

Logstash and DCR

Logstash Input and Output

```
input {
    syslog {
        type => "syslog"
        port => 1521
    }
}
filter {
    mutate {
        add_tag => [ "FORTIGATE" ]
    }
}
output {
    pipeline { send_to => sentinel }
}
```

```
input {
    pipeline { address => sentinel }
}
output {
    if "FORTIGATE" in [tags] {
    // dc-fortigate-tst-westeurope-001 to CommonSecurityLogs table
        microsoft-sentinel-logstash-output-plugin {
            client_app_Id => "95a36bd9-[redacted]"
            client_app_secret => "YouWishYouHadThis"
            tenant_id => "30aafeef-[redacted]"
            data_collection_endpoint => "https://[redacted].westeurope-1.ingest.monitor.azure.com"
            dcr_immutable_id => "dcr-6d021ecccfe545d6b8ef8f1c74578a14"
            dcr_stream_name => "Custom-FortigateTest_CL"
        }
    // dc-fortigate-tst-westeurope-002 to Custom FortiGate table
    microsoft-sentinel-logstash-output-plugin {
            client_app_Id => "95a36bd9-[redacted]"
            client_app_secret => "YouWishYouHadThis"
            tenant_id => "30aafeef-[redacted]"
            data_collection_endpoint => "https://[redacted].westeurope-1.ingest.monitor.azure.com"
            dcr_immutable_id => "dcr-79b00076065043788bb675ee8899e56c"
            dcr_stream_name => "Custom-FortigateTest_CL"
        }
    }
}
```

DCRs

04

Building a highly scalable forwarding solution

The power of Logstash and Azure

05

Sharing my experience

Learning from eachother

Custom logs best practices

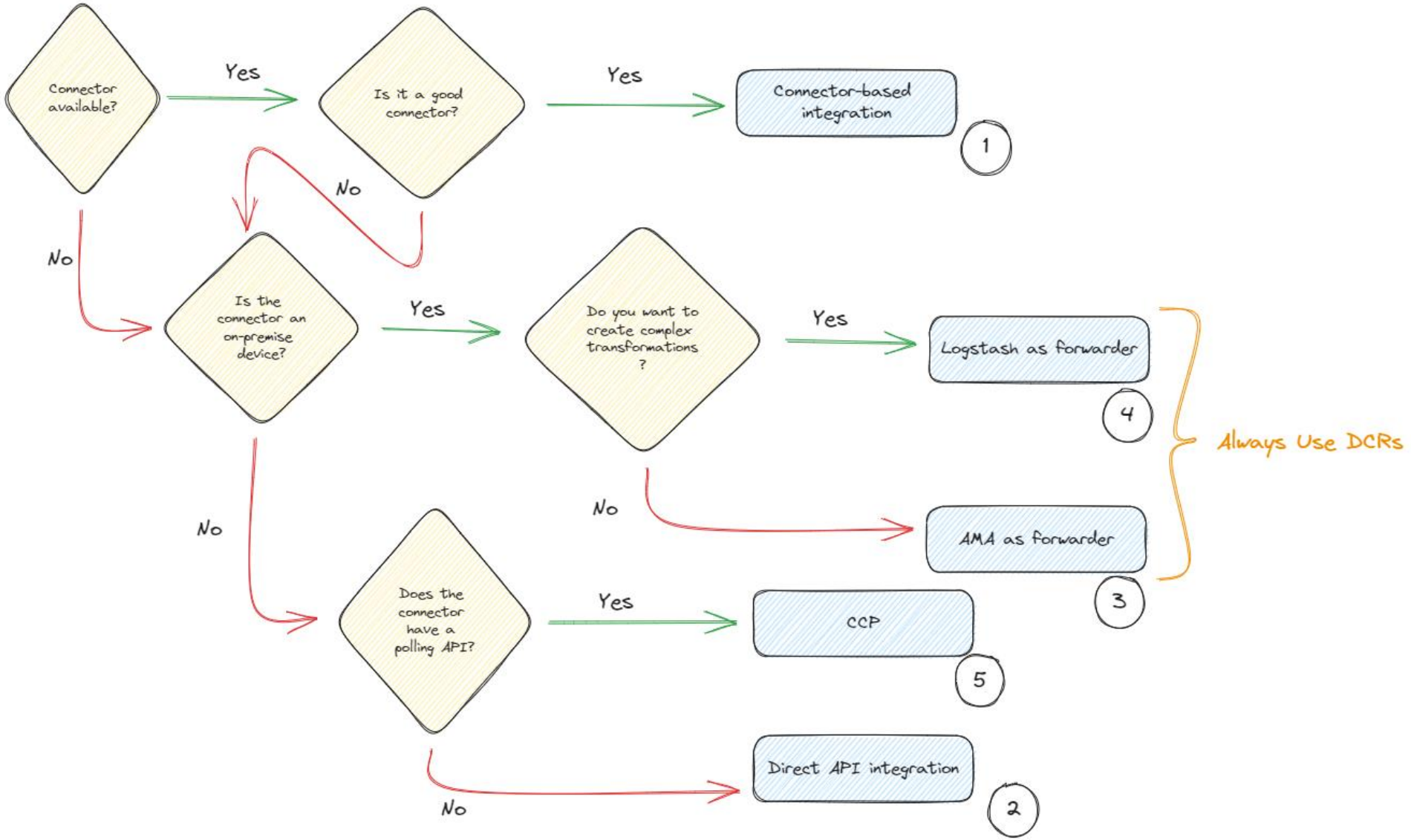
Use ama for simple connectors <-> Use Logstash for complex connectors

Create DCR per data connector / per destination table

Mix basic and analytics tables for high data amounts

Workspace transformation DCR cannot have other DCR as a source

How to choose between connector types



3

THE NEVER ENDING STRUGGLE : INCIDENT OPTIMIZATION

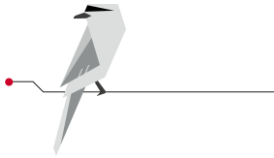
Who am I?

Overview

- Louis Mastelinck
- Soc analyst & Security consultant

I make ugly slides

Agenda



Alert fatigue

Personal experience

Methods we used

Interested in your solutions

3a

ALERT FATIGUE

Alert fatigue

The never-ending battle

It comes in waves

focus and motivation of analysts

consumes time you can spend on better things

Work smarter not harder

Question: Do you recognize the battle against alert fatigue in your organization?

I have no holy grail

Some examples: Bruteforce against the azure portal

Microsoft's default rules

Early stages only failures would also trigger:

Has been updated over time with thresholds you can tweak:

```
62          | join kind=inner (
63              table(tableName)
64              | where TimeGenerated > ago(7d)
65              | where AppDisplayName has "Azure Portal"
66              | extend FailureOrSuccess = iff(ResultType in ("0", "50125", "50140", "70043", "70044"), "Success", "Failure")
67              | summarize avgFailures = avg(todouble(FailureOrSuccess == "Failure")) by UserPrincipalName
68          ) on UserPrincipalName
69          | extend Deviation = abs(FailureCountBeforeSuccess - avgFailures) / avgFailures
70          // Filter records based on deviation and failure count criteria
71          | where Deviation > threshold and FailureCountBeforeSuccess >= 10
72          // Expand the IPAddress array
73          | mv-expand IPAddress
74          | extend IPAddress = tostring(IPAddress)
75          | extend timestamp = StartTime
76      };
```

Unfamiliar sign-in properties

The doc’s are vague

“Sign in with properties we’ve not seen recently for the given user.”

Unfamiliar sign-in properties

Calculated in real-time. This risk detection type considers past sign-in history to look for anomalous sign-ins. The system stores information about previous sign-ins, and triggers a risk detection when a sign-in occurs with properties that are unfamiliar to the user. These properties can include IP, ASN, location, device, browser, and tenant IP subnet. Newly created users are in "learning mode" period where the unfamiliar sign-in properties risk detection is turned off while our algorithms learn the user's behavior. The learning mode duration is dynamic and depends on how much time it takes the algorithm to gather enough information about the user's sign-in patterns. The minimum duration is five days. A user can go back into learning mode after a long period of inactivity.

Question: Do you agree with the unfamiliar sign-in properties alerts?

Our objective

Resolve them faster

Or

Don’t raise them when proven to Benign Positive

Common scenario’s

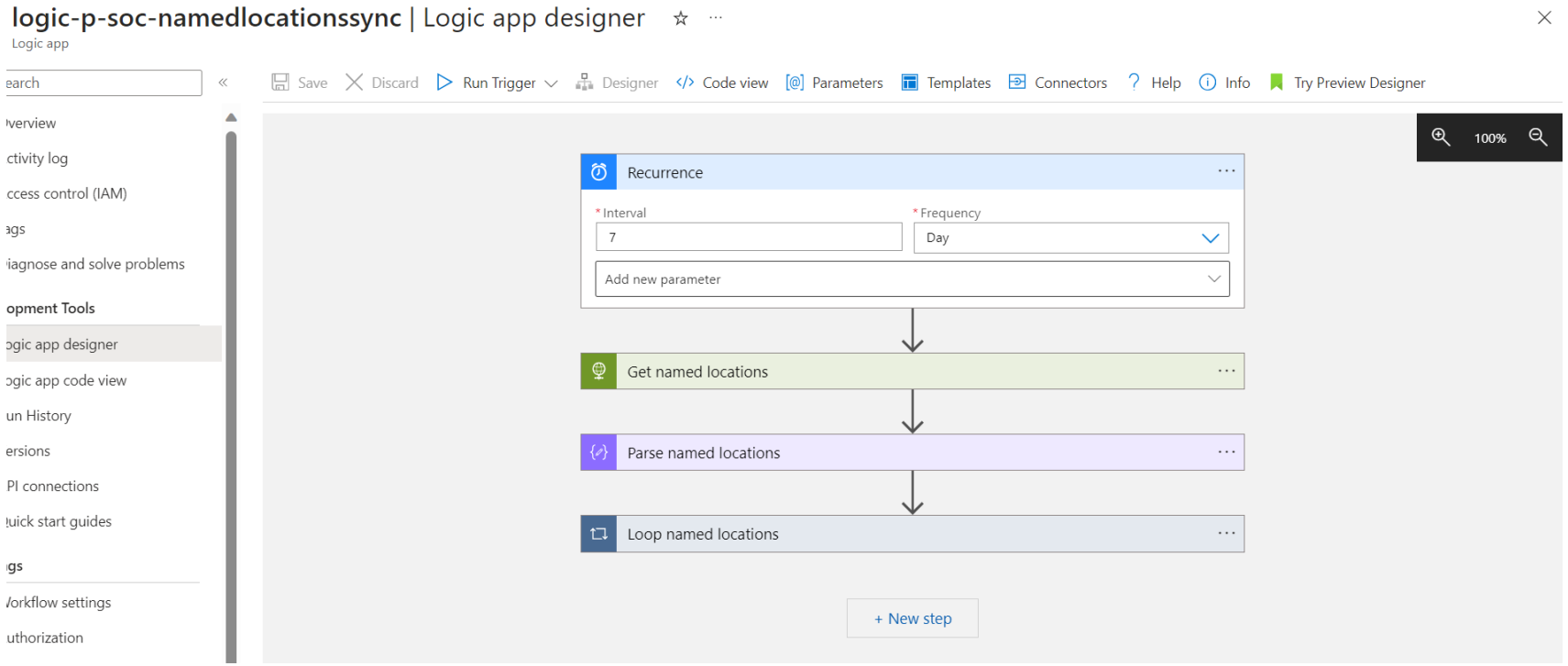
Unfamiliar sign-in

- Recently created users but sleeping for a month
- Sleeping users (active … sleeping…active…)
- Company VPN ranges (for example: Zscaler)
- Company trusted locations
- Sign-in activity confirmed with compliant devices
- Sign-in activity with greater authentication strength (no claim in token)
- Expected locations

We need to enrich!

We started simple

A logic app that retrieves the trusted locations



Context is everything

OOO enrichment

Hello,

Thank you for your email. I wanted to let you know that I am currently out of the office and traveling to Japan. I will not be available to respond to emails during this time.

If your matter is urgent, please contact [Alternative Contact Person's Name] at [Alternative Contact Person's Email] for assistance. Otherwise, I will do my best to get back to you as soon as possible when I return on [Your Return Date].

Thank you for your understanding, and I look forward to connecting with you upon my return.

Best regards,

[Your Name]

Question: Do you trust Microsoft's IP geo location’s?

IP enrichments

Calculation

For each ip: calculate how many different users have signed in

How much office activity do we see from the user and what type

- Send email
- Create inbox rules
- Delete emails
- Download emails
- ….

how many sign-ins (failure success ratio & authentication method)

Enriching IP

Use 3rd party to enrich IP's and get more value

APIvoid
Get the reputation
Network owner

UEBA

User and Entity Behavior Analytics

A great source to get enrichments about your user entities or make correlations

Examples:
Location
Department
Company function
Group memberships
...

Adapt the KQL

You got the data

You have a specific use case in mind

Now you need…

A smart guy to do the KQL

- 100 ways of writing stuff in KQL
- it’s a learning curve

Run the rules in validation

example

Identity

Country:
Department: [redacted]
Job Title:
Manager:
Phone:
User Created at: 16-11-2022 [13:07:06].
PWReset executed on 27-09-2023 [6:26:45] by [redacted]

Authentication

All countries in the last 14d with the most recent logon data:

- NL: 25-10-2023 [13:28:50]

All platforms in the last 14d with the most recent logon data:

- Android: 25-10-2023 [13:28:50]
- Windows 10: 05-06-2023 [13:18:07]
- Windows10: 27-09-2023 [6:34:06]
- Windows: 27-09-2023 [6:32:33]

Message:

OOFStatus: disabled

Enrichment IP
No threats were found on [redacted]
Country: Netherlands
Service Provider: [redacted].
This IP has showed 3 sign-in activities in the last 90 days.
1 users have activity from this IP.
This IP has showed 4 office activities in the last 90 days.
The IP is linked to [redacted] and has 3 succeeded sign-ins and 0 failed sign-ins on this IP. It has 0 succeeded MFA sign-ins and 0 failed MFA sign-ins on this IP.
Operating System details:
* "Android"
Browser details:
* "Chrome Mobile 118.0.0"
User Agents:
* "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML
* like Gecko) Chrome/118.0.0.0 Mobile Safari/537.36"

Question: What API’s do you use?

Share with the community

Type in chat or take the mic

But there is a risk.. What if.. And then that...?

Totally agree....
There could be a scenario where an on site users his device gets compromised and they steal his session.
Any many other scenario's...

The bigger the maturity the easier to optimize

Our tip:
Take it slow
Start with a small improvement

But let the numbers speak for itself!
If you can solve auto close majority of you incidents with your enrichments
Make sure you have detections that overlap the X%

Big struggle: impossible travel

Impossible travels due to roaming!

We honestly struggle with this one:

Country of origin of the sim card / aka usage location / office location

Mobile phones / entra ID registered devices

Map Mobile providers IP ranges (Watchlists in combination API IP enrichments?)

Difficulties:
User agent’s can be changed (they don’t do it often, but they can)

Hotspot tethering

Session token theft contains compliance of a device…

Question: Do you encounter the roaming effect as an obstacle in your investigations?


IS THIS THING ON?

4

NEXT SUBJECTS REMINDER

Next sessions agenda & volunteers

Name	Truls DAHLSVEEN	Lorraine Hickson	Younes Khaldi Helena Gleczman	TBC	Kristopher Jackson
Organization	Sopra Steria	AXA	Microsoft	TBC	BOK Financial
Topics	Sentinel as a code presentation	Machine learning on Azure	• New Sentinel cost model overview • Sentinel User Forum feedback	ADX journey : • API vs custom dev • Cost reduction	Logic Apps feedback (chatbot implemented)
Date	13/06	26/10	19/01	TBC	TBC

<u>Want to take lead on a specific topic not mentioned above ?</u>
➔ Please let us know during next session, or
➔ Send an email to Timo.muller@axa.com

5 CLOSE

Thank you all !