Secure Logstash connections to Microsoft Sentinel with R0t8r

DUTCH MICROSOFT SECURITY MEETUP

Invoke-AzSpeaker | Format-List

[]$ Invoke-AzSpeaker | Format-List

Koos Goossens

Microsoft Cloud &
Security Consultant

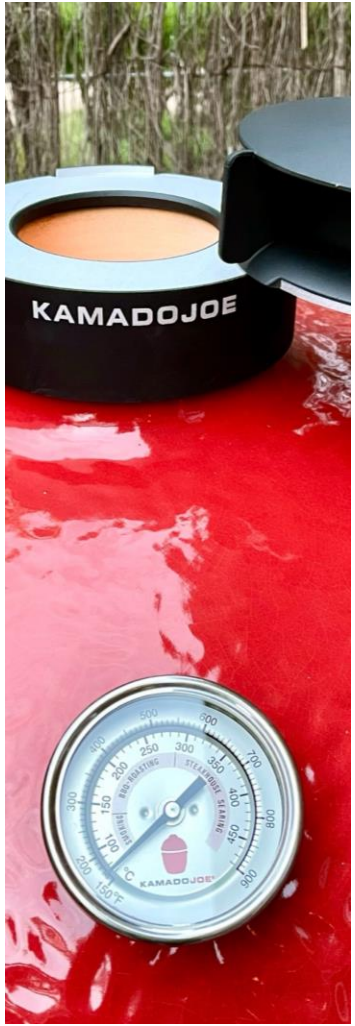
koos.goossens@wortell.nl

@koosgoossens

aka.ms/koos

[]$ _

MVP
Microsoft®
Most Valuable
Professional


PRIVATE
ROAD

KAMADOJOE
KAMADOJOE


I  Microsoft Sentinel

DUTCH MICROSOFT SECURITY MEETUP

Agenda

- Log ingestion challenges
- Logstash?
- Managing keys
- `ROt8r` to the rescue?

Agenda

-
-
-
-

Photography by Albert Dros

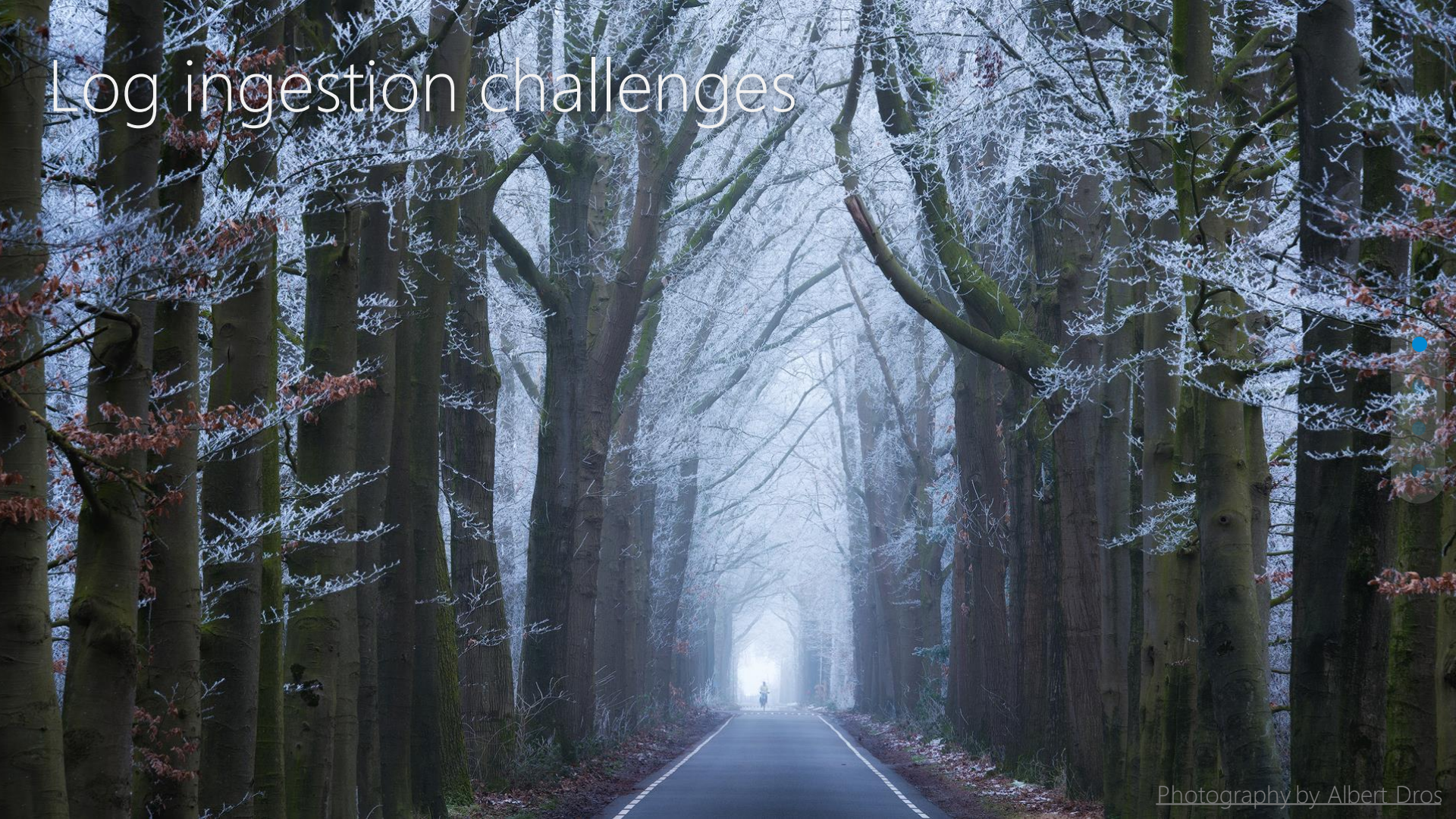
Log ingestion challenges

Photography by Albert Dros

Log ingestion challenges

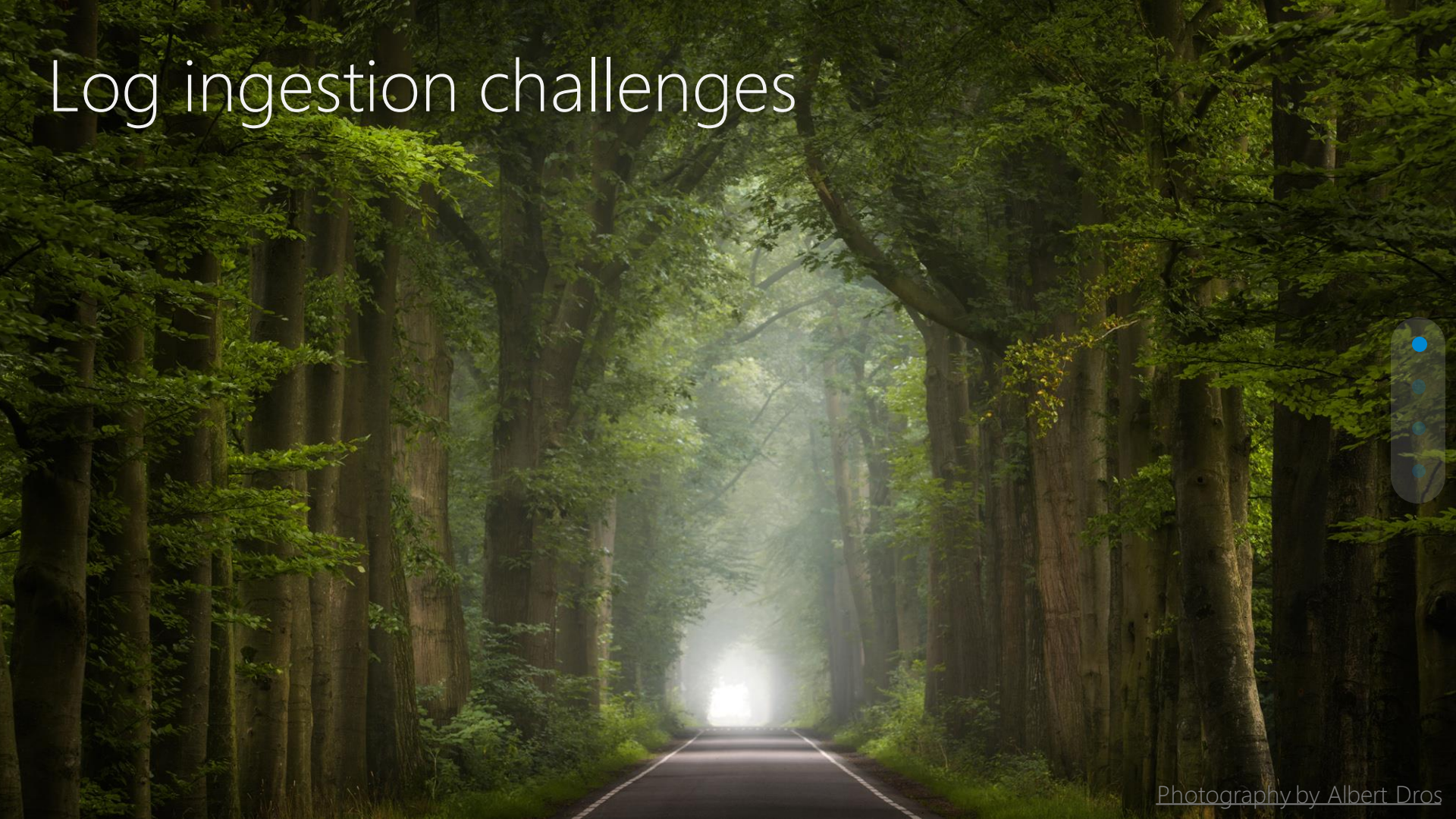
Photography by Albert Dros

Log ingestion challenges



Photography by Albert Dros

Log ingestion challenges

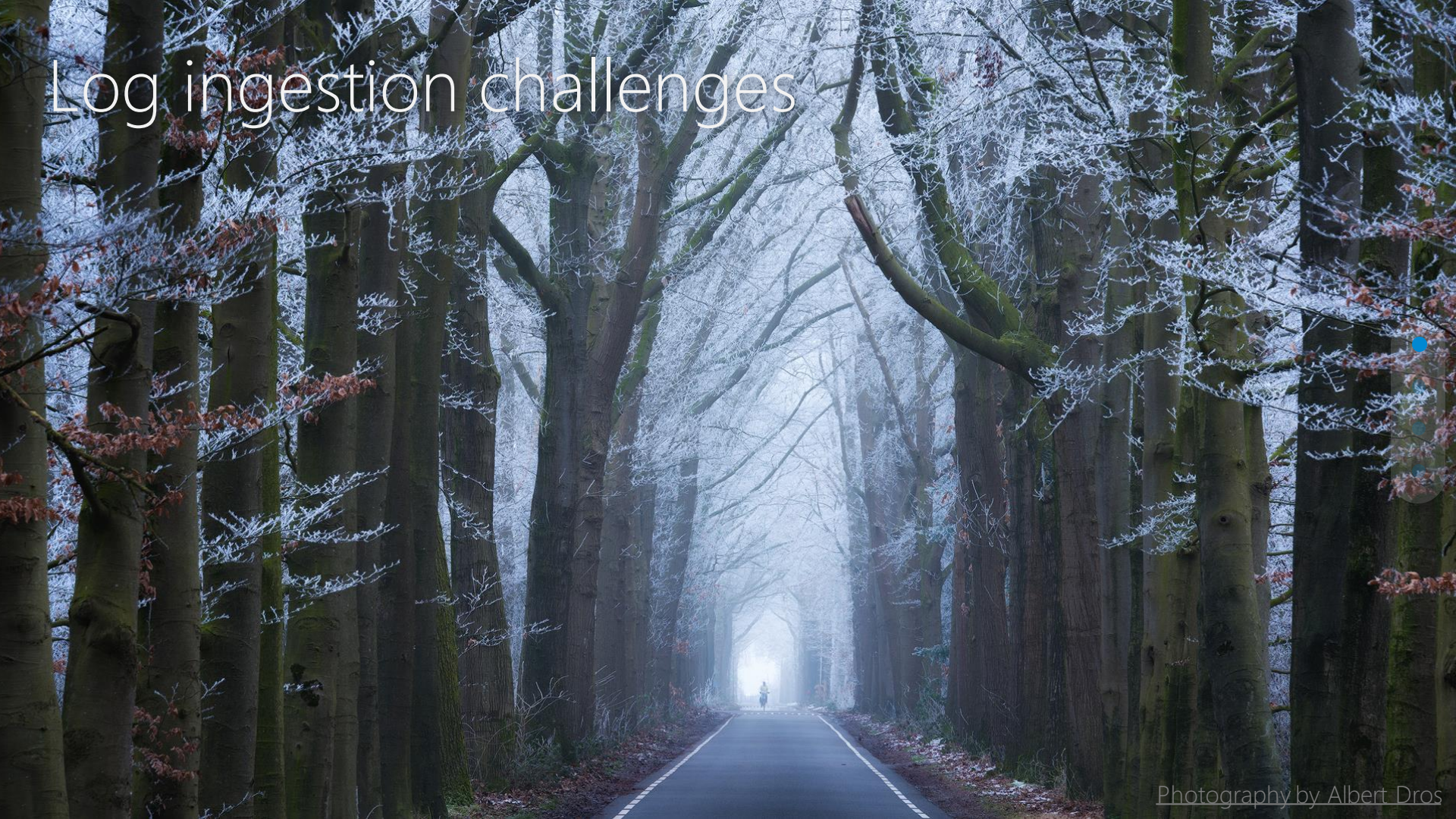


Photography by Albert Dros

Log ingestion challenges

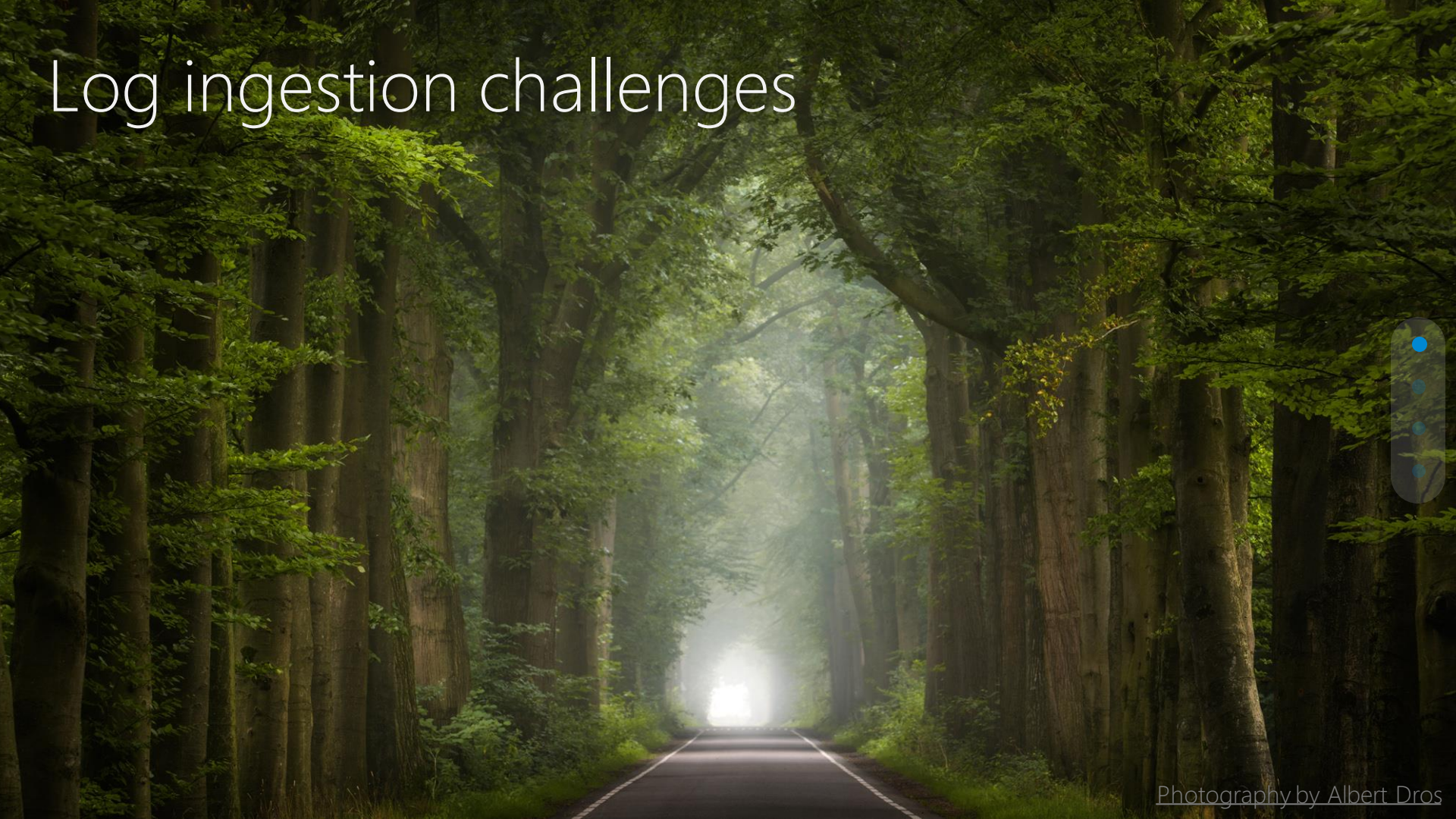
Photography by Albert Dros

Log ingestion challenges



Photography by Albert Dros

Log ingestion challenges

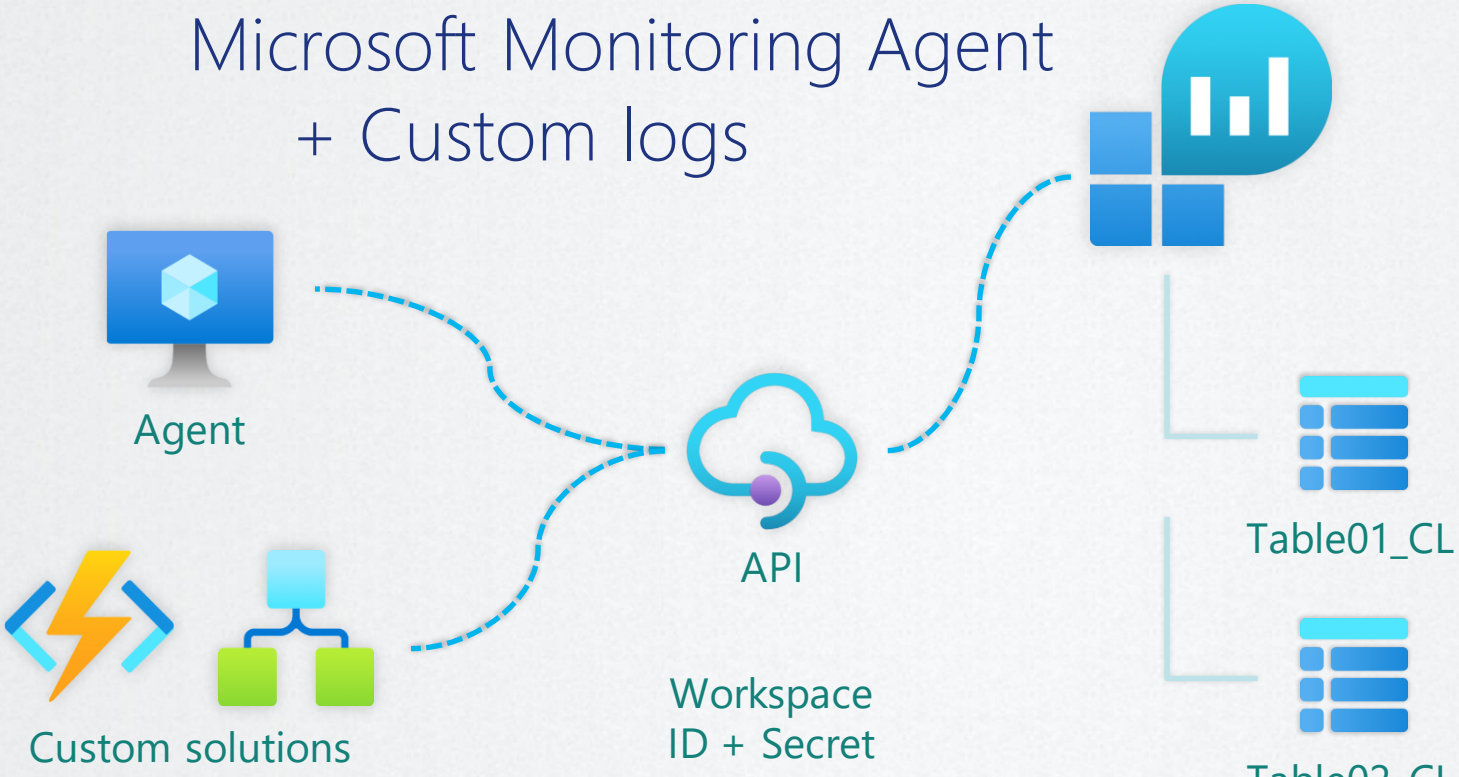


Photography by Albert Dros

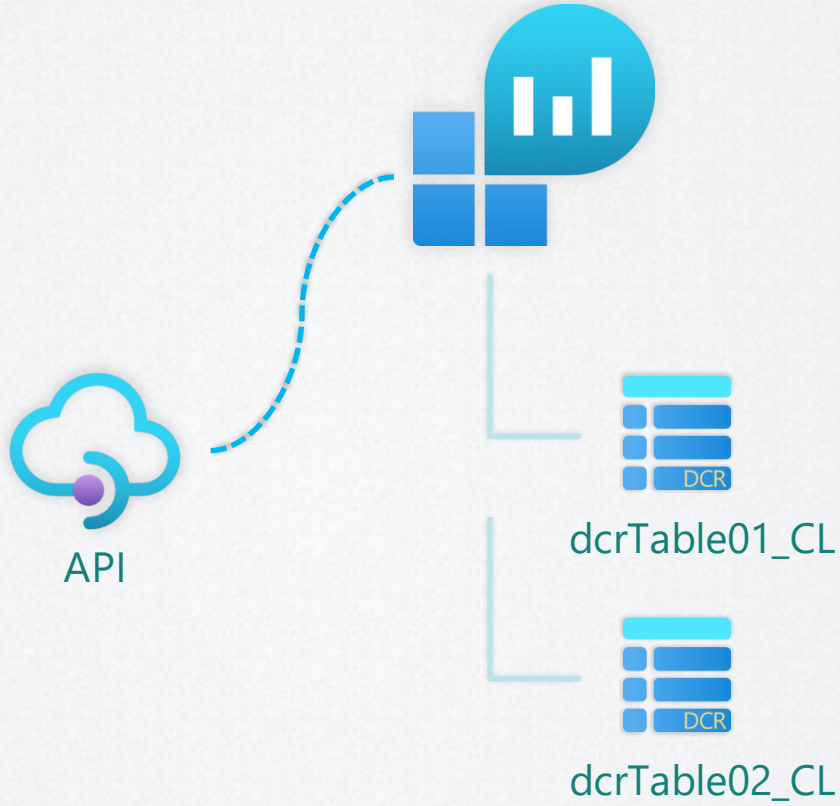
Log challenges

- Cloud is always changing
  - MMA → AMA

Microsoft Monitoring Agent + Custom logs

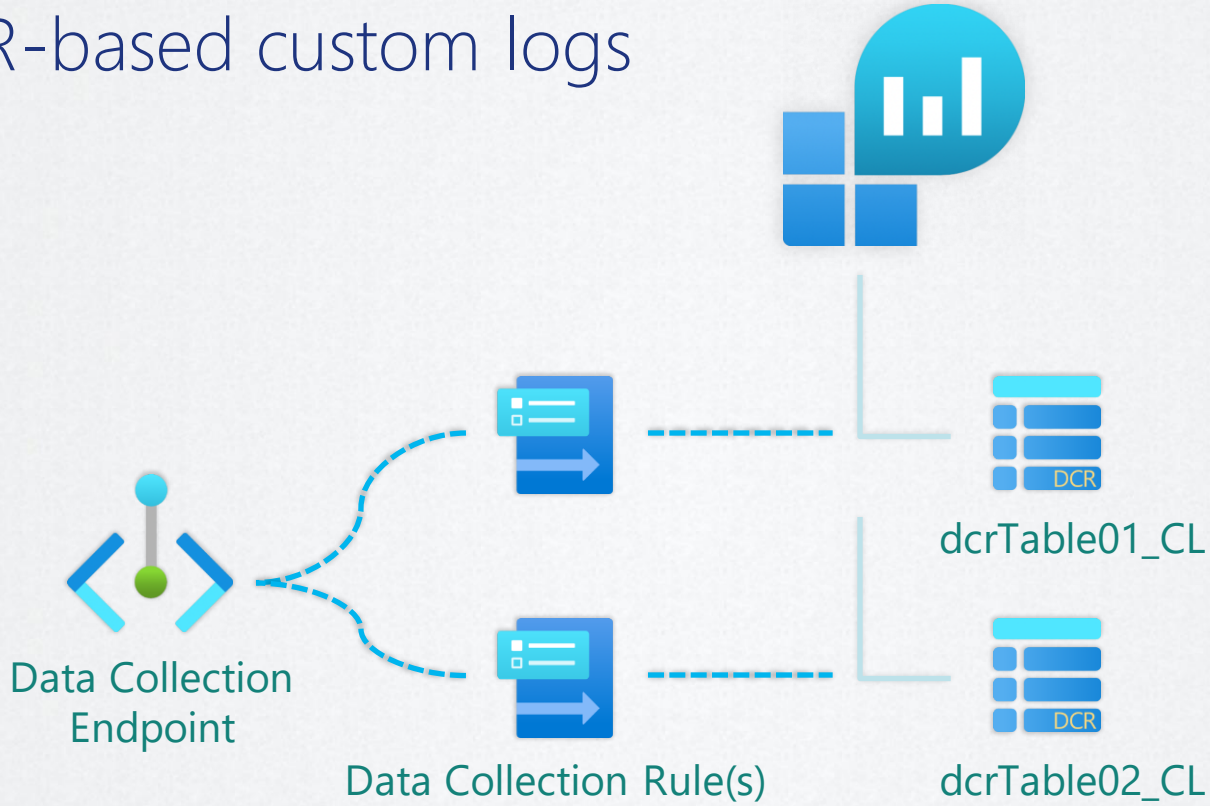


Microsoft Monitoring Agent + Custom logs

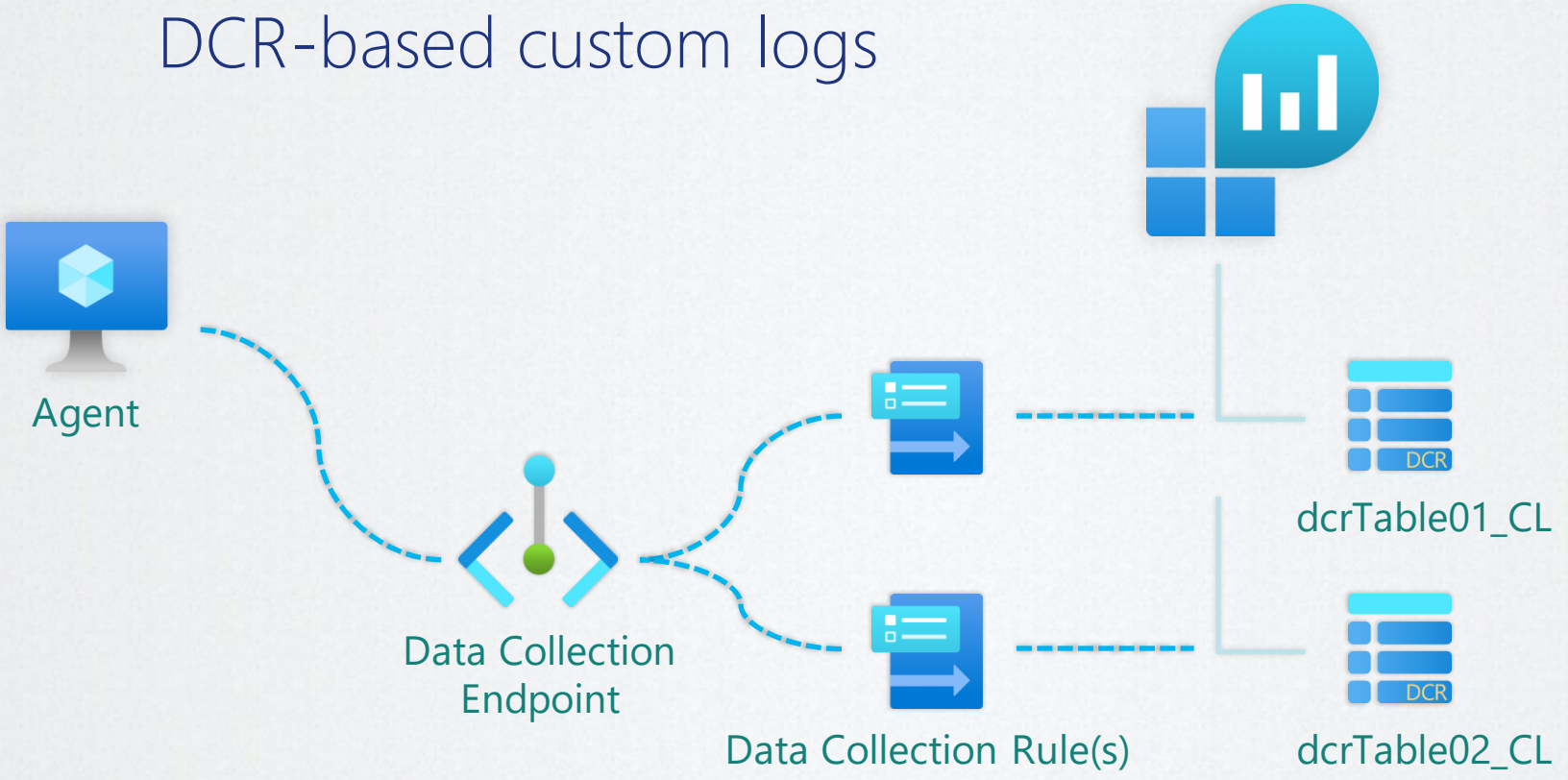

DCR
dcrTable01_CL
API
DCR
dcrTable02_CL

DCR-based custom logs

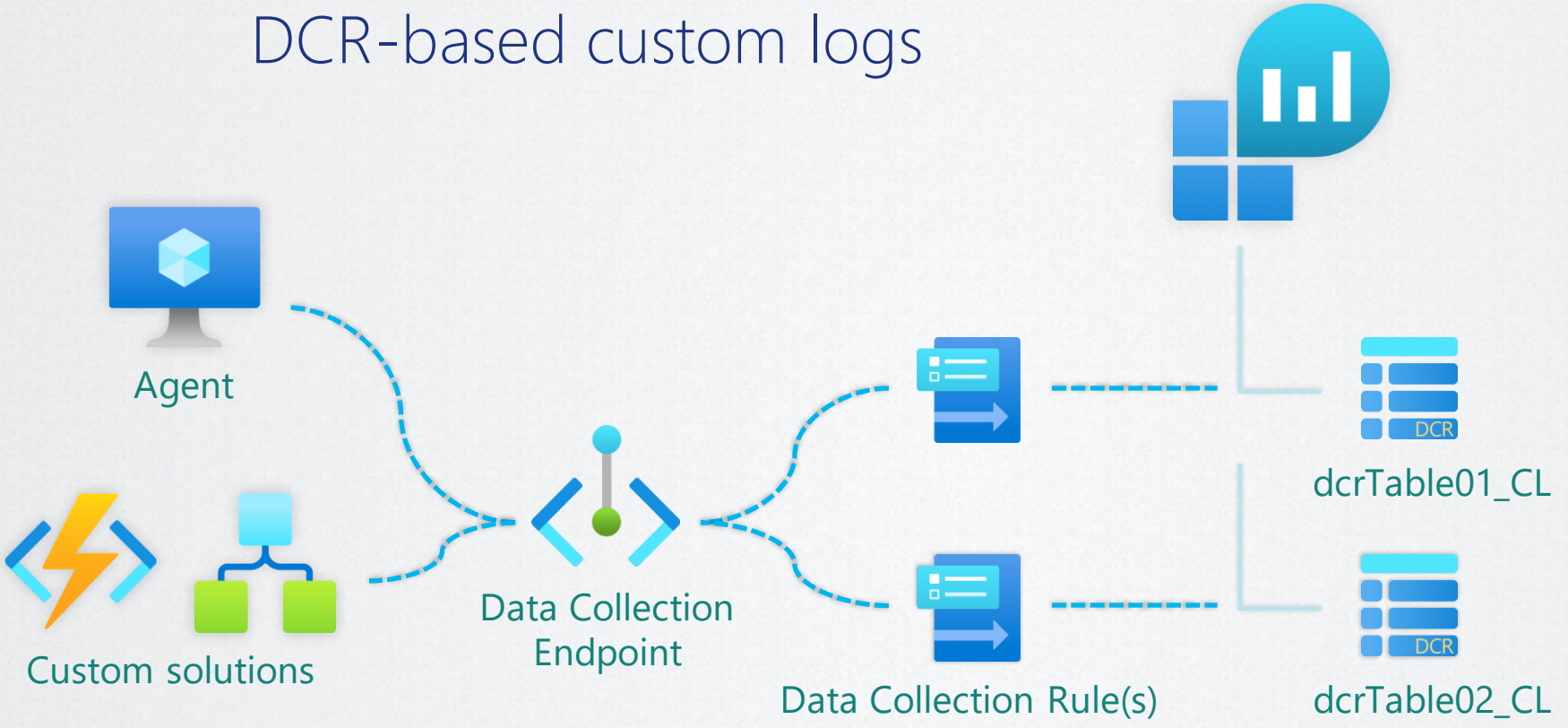
DCR-based custom logs



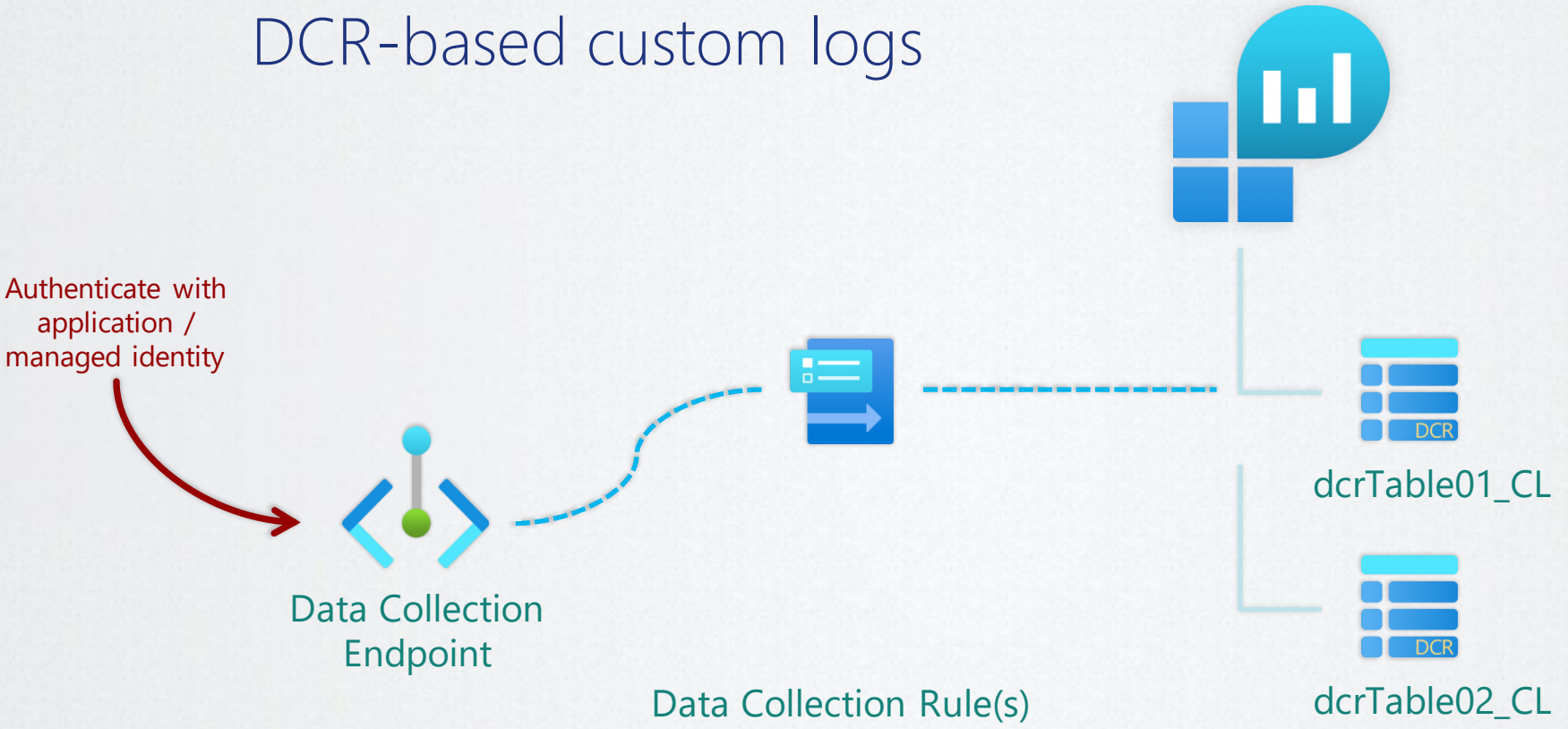
DCR-based custom logs



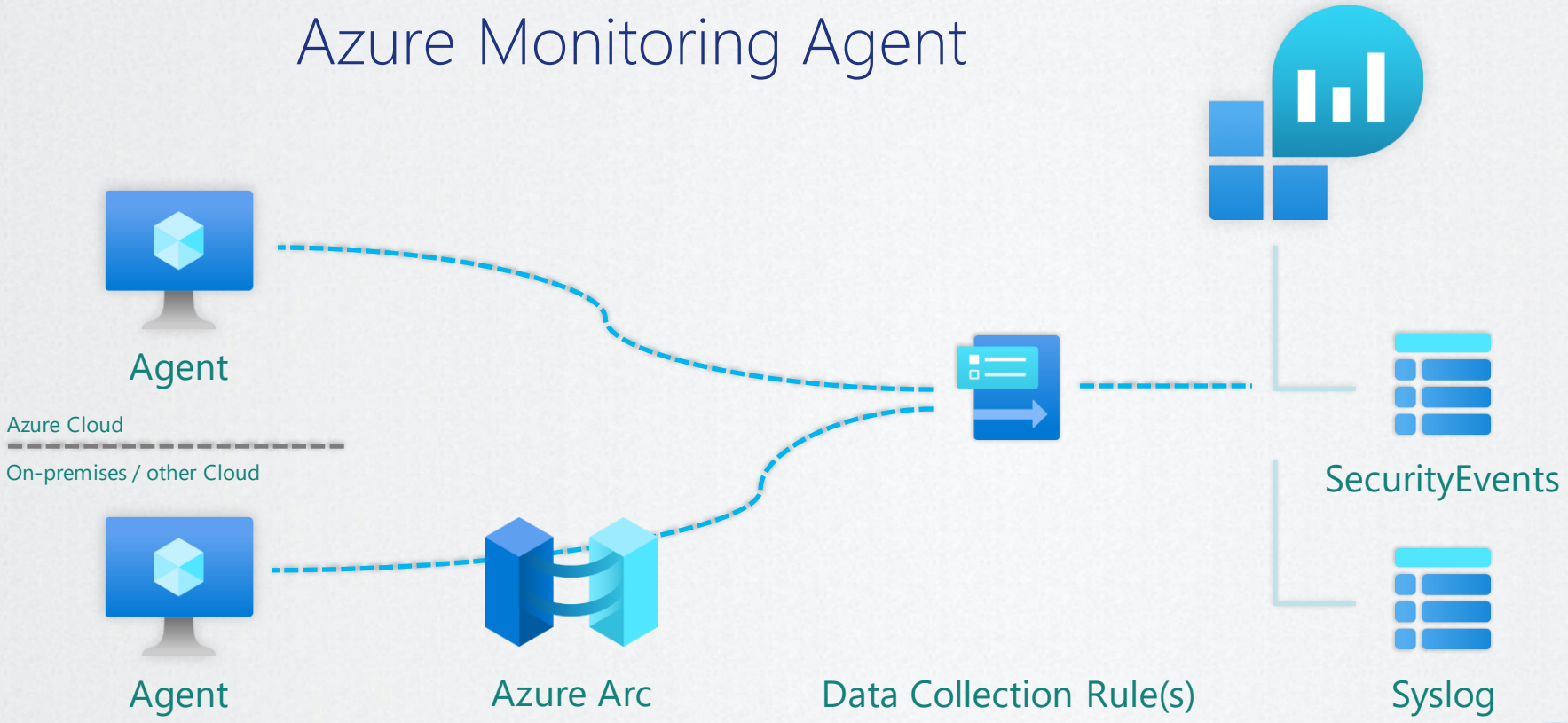
DCR-based custom logs



DCR-based custom logs



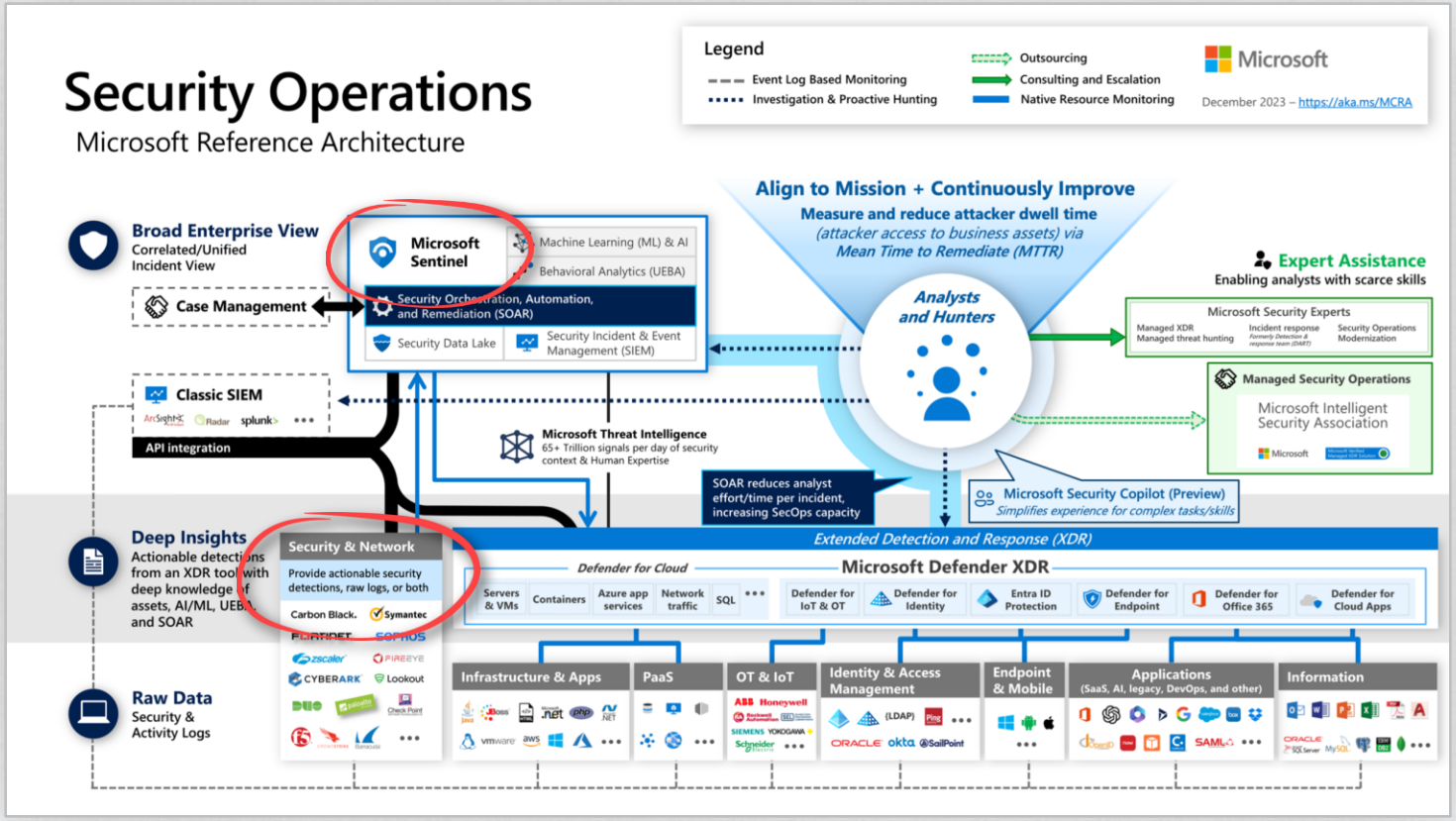
Azure Monitoring Agent



Log ingestion challenges

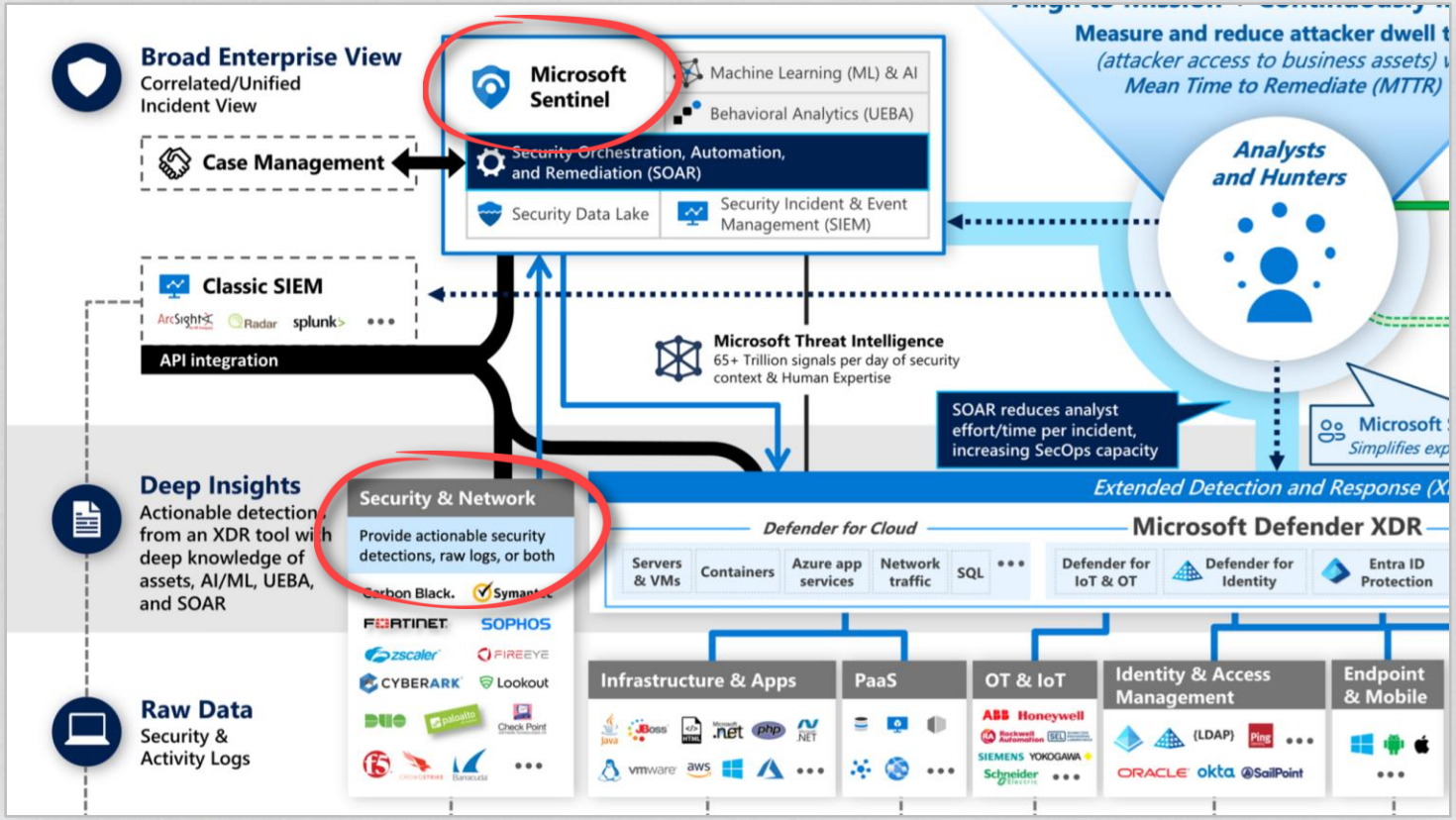
- Cloud is always changing
  - MMA → AMA
  - Lots of specific features (still) in preview
- Azure Arc is not to be underestimated
- Co-operate with other ops teams and vendors
  - Managing DCRs
- Sentinel as a “security data lake”?

Microsoft Cybersecurity Reference Architectures (MCRA)



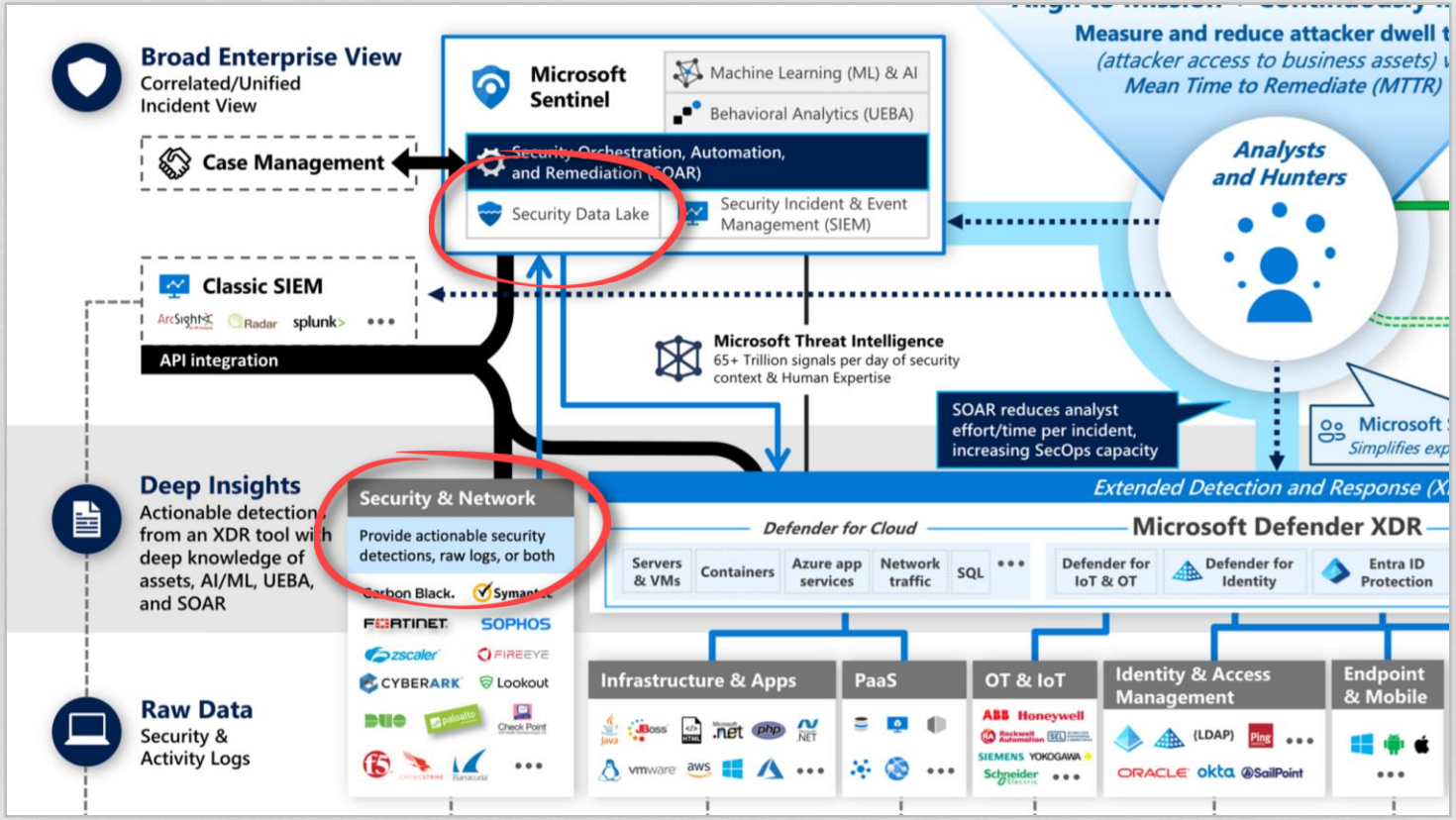
DUTCH MICROSOFT SECURITY MEETUP

Microsoft Cybersecurity Reference Architectures (MCRA)



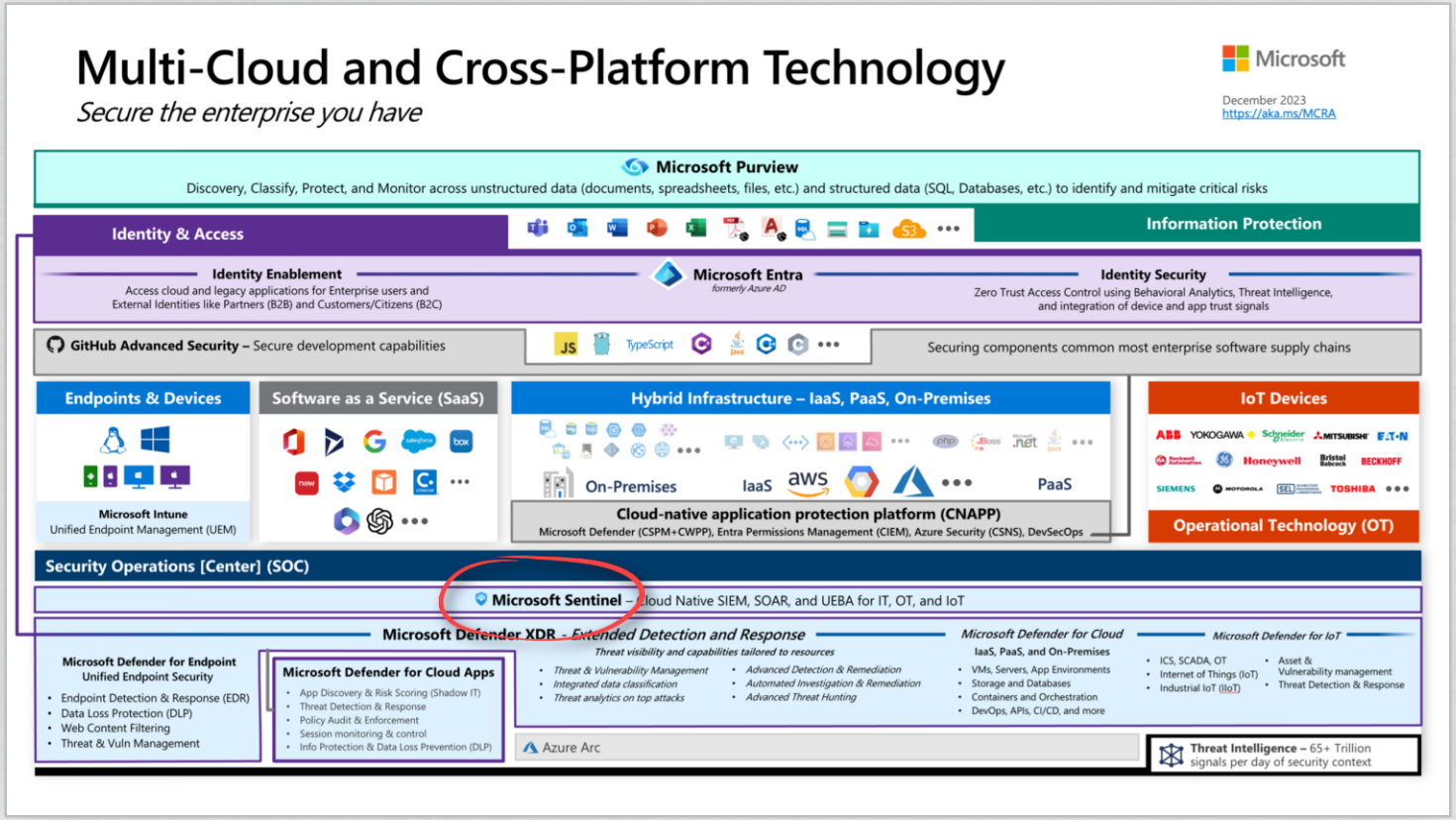
DUTCH MICROSOFT SECURITY MEETUP

Microsoft Cybersecurity Reference Architectures (MCRA)



DUTCH MICROSOFT SECURITY MEETUP

Microsoft Cybersecurity Reference Architectures (MCRA)



DUTCH MICROSOFT SECURITY MEETUP

techcommunity.microsoft.com

Microsoft Sign In

Automation: Integrate Azure Data Explorer as Long-Term Log Retention for Microsoft Sentinel

By Sreedhar Ande
Published Oct 26 2021 02:54 PM 7,465 Views

Out of the box, Microsoft Sentinel provides 90 days of data retention for free. In some parts of the world and within certain industries, there are regulations that organizations must adhere to which require data retention up to 7 years or longer. The current challenge is that the max retention for Log Analytics workspaces is 2 years. There has been a need for a solution that will allow for more time and cost saving for long-term retention.

This blog is going to detail how logs from Log Analytics workspace can easily be migrated into long-term storage using Azure Data Explorer (ADX) to comply with retention standards as well as reduce costs with the help of PowerShell script.

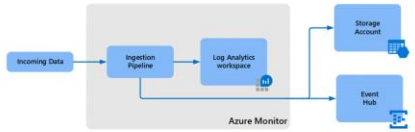
Thanks to @Javier Soriano for his inputs into this blog post

Azure Data Explorer (ADX)

Azure Data Explorer is a big data analytics platform that is highly optimized for log and data analytics. Since Azure Data Explorer uses Kusto Query Language (KQL) as its query language, it's a good alternative for Microsoft Sentinel data storage. Using Azure Data Explorer for your data storage enables you to run cross-platform queries and visualize data across both Azure Data Explorer and Microsoft Sentinel.
For more information, see the Azure Data Explorer documentation and blog

Log Analytics Data Export Architecture

The following image shows a sample flow of exported data through the Azure Monitor ingestion pipeline. Your data is directed to Log Analytics by default, but you can also configure it to export to an Azure Storage Account or Event Hub



DUTCH MICROSOFT SECURITY MEETUP

techcommunity.microsoft.com

Microsoft Sign In

Automation: Integrate Azure Data Explorer as Long-Term Log Retention for Microsoft Sentinel

By Sreedhar Ande
Published Oct 26 2021 02:54 PM 7,465 Views

Out of the box, Microsoft Sentinel provides 90 days of data retention for free. In some parts of the world and within certain industries, there are regulations that organizations must adhere to which require data retention up to 7 years or longer. The current challenge is that the max retention for Log Analytics workspaces is 2 years. There has been a need for a solution that will allow for more time and cost saving for long-term retention.

This blog is going to detail how logs from Log Analytics workspace can easily be migrated into long-term storage using Azure Data Explorer (ADX) to comply with retention standards as well as reduce costs with the help of PowerShell script.

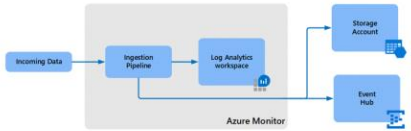
Thanks to @Javier Soriano for his inputs into this blog post

Azure Data Explorer (ADX)

Azure Data Explorer is a big data analytics platform that is highly optimized for log and data analytics. Since Azure Data Explorer uses Kusto Query Language (KQL) as its query language, it's a good alternative for Microsoft Sentinel data storage. Using Azure Data Explorer for your data storage enables you to run cross-platform queries and visualize data across both Azure Data Explorer and Microsoft Sentinel.
For more information, see the Azure Data Explorer documentation and blog

Log Analytics Data Export Architecture

The following image shows a sample flow of exported data through the Azure Monitor ingestion pipeline. Your data is directed to Log Analytics by default, but you can also configure it to export to an Azure Storage Account or Event Hub



learn.microsoft.com

Microsoft Documentation

Learn / Azure / Architecture Center /

Azure Data Explorer monitoring

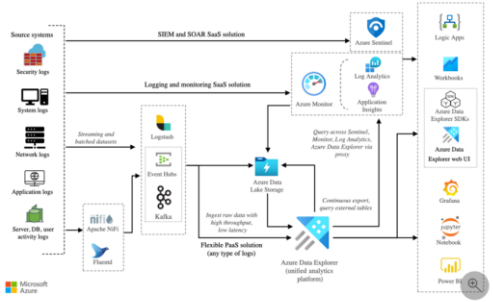
Solution ideas

This article is a solution idea. If you'd like us to expand the content with more information, such as potential use cases, alternative services, implementation considerations, or pricing guidance, let us know by providing **GitHub feedback**.

This solution idea demonstrates a hybrid end-to-end monitoring solution integrated with Microsoft Sentinel and Azure Monitor for ingesting streamed and batched logs from diverse sources, on-premises, or any cloud, within an enterprise ecosystem.

Apache®, Apache Nifi® and Apache Kafka are either registered trademarks or trademarks of the Apache Software Foundation in the United States and/or other countries. No endorsement by The Apache Software Foundation is implied by the use of these marks. Fluentd, Logstash, Grafana, and Jupyter Notebooks are trademarks of their respective companies. No endorsement is implied by the use of these marks.

Architecture



Download a Visio file of this architecture.

Dataflow

1. Combine features provided by Microsoft Sentinel and Azure Monitor with Azure Data Explorer to build a flexible and cost-optimized end-to-end monitoring solution. Below are some examples:

DUTCH MICROSOFT SECURITY MEETUP

techcommunity.microsoft.com

Microsoft Sign In

Automation: Integrate Azure Data Explorer as Long-Term Log Retention for Microsoft Sentinel

By Sreedhar Ande

Published Oct 26 2021 02:54 PM 7,465 Views

Out of the box, Microsoft Sentinel provides 90 days of data retention for free. In some parts of the world and within certain industries, there are regulations that organizations must adhere to which require data retention up to 7 years or longer. The current challenge is that the max retention for Log Analytics workspaces is 2 years. There has been a need for a solution that will allow for more time and cost saving for long-term retention.

This blog is going to detail how logs from Log Analytics workspace can easily be migrated into long-term storage using Azure Data Explorer (ADX) to comply with retention standards as well as reduce costs with the help of PowerShell script.

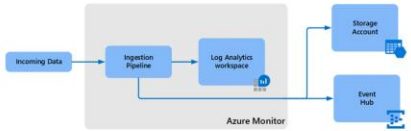
Thanks to @Javier Soriano for his inputs into this blog post

Azure Data Explorer (ADX)

Azure Data Explorer is a big data analytics platform that is highly optimized for log and data analytics. Since Azure Data Explorer uses Kusto Query Language (KQL) as its query language, it's a good alternative for Microsoft Sentinel data storage. Using Azure Data Explorer for your data storage enables you to run cross-platform queries and visualize data across both Azure Data Explorer and Microsoft Sentinel.
For more information, see the Azure Data Explorer documentation and blog

Log Analytics Data Export Architecture

The following image shows a sample flow of exported data through the Azure Monitor ingestion pipeline. Your data is directed to Log Analytics by default, but you can also configure it to export to an Azure Storage Account or Event Hub

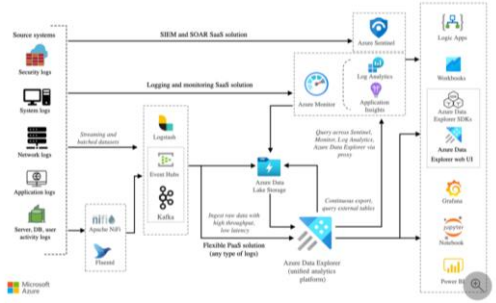


learn.microsoft.com

Microsoft Documentation

the use of these marks.

Architecture



Download a Visio file of this architecture.

Dataflow

1. Combine features provided by Microsoft Sentinel and Azure Monitor with Azure Data Explorer to build a flexible and cost-optimized end-to-end monitoring solution. Below are some examples:
   - Use Microsoft Sentinel as a SIEM and SOAR component in the overall monitoring solution where you can ingest security logs from firewalls, Defender for Cloud, and so on. SIEM is short for *security information and event management*, whereas SOAR is short for *security orchestration, automation and response*.
   - Use Azure Monitor's native capabilities for IT asset monitoring, dashboarding, and alerting so you can ingest logs from VMs, services, and so on.
   - Use Azure Data Explorer for full flexibility and control in all aspects for all types of logs in the following scenarios:
     - No *out of the box* features provided by Microsoft Sentinel and Azure Monitor SaaS solutions such as application trace logs.
     - Greater flexibility for building quick and easy near-real-time analytics dashboards, granular role-based access control, time series analysis, pattern recognition, anomaly detection and forecasting, and machine learning. Azure Data Explorer is also well integrated with ML services such as Databricks and Azure Machine Learning. This integration allows you to build models using other tools and services and export ML models to Azure Data Explorer for scoring data.
     - Longer data retention is required in cost effective manner.
     - Centralized repository is required for different types of logs. Azure Data Explorer, as a unified big data analytics platform, allows you to build advanced analytics scenarios.

DUTCH MICROSOFT SECURITY MEETUP

techcommunity.microsoft.com

Microsoft Sign In

Automation: Integrate Azur
Explorer as Long-Term Log
Microsoft Sentinel

By Sreedhar Ande
Published Oct 26 2021 02:54 PM 7,465 Views

Out of the box, Microsoft Sentinel provides 90 days of data retention
within certain industries, there are regulations that organizations mus
up to 7 years or longer. The current challenge is that the max retentic
years. There has been a need for a solution that will allow for more ti
retention.

This blog is going to detail how logs from Log Analytics workspace c
storage using Azure Data Explorer (ADX) to comply with retention sta
help of PowerShell script.

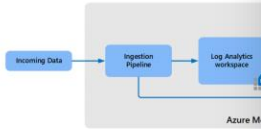
Thanks to @Javier Soriano for his inputs into this blog post

Azure Data Explorer (ADX)

Azure Data Explorer is a big data analytics platform that is highly opti
Azure Data Explorer uses Kusto Query Language (KQL) as its query la
Microsoft Sentinel data storage. Using Azure Data Explorer for your d
platform queries and visualize data across both Azure Data Explorer a
For more information, see the Azure Data Explorer documentation an

Log Analytics Data Export Architectur

The following image shows a sample flow of exported data through t
Your data is directed to Log Analytics by default, but you can also cor
Account or Event Hub



Dataflow

1. Combine features provided by Microsoft Sentinel and Azure Monitor with Azure Data Explorer to build a flexible and cost-optimized end-to-end monitoring solution. Below are some examples:

   - Use Microsoft Sentinel as a SIEM and SOAR component in the overall monitoring solution where you can ingest security logs from firewalls, Defender for Cloud, and so on. SIEM is short for *security information and event management*, whereas SOAR is short for *security orchestration, automation and response*.
   - Use Azure Monitor's native capabilities for IT asset monitoring, dashboarding, and alerting so you can ingest logs from VMs, services, and so on.
   - Use Azure Data Explorer for full flexibility and control in all aspects for all types of logs in the following scenarios:
     - No *out of the box* features provided by Microsoft Sentinel and Azure Monitor SaaS solutions such as application trace logs.
     - Greater flexibility for building quick and easy near-real-time analytics dashboards, granular role-based access control, time series analysis, pattern recognition, anomaly detection and forecasting, and machine learning. Azure Data Explorer is also well integrated with ML services such as Databricks and Azure Machine Learning. This integration allows you to build models using other tools and services and export ML models to Azure Data Explorer for scoring data.
     - Longer data retention is required in cost effective manner.
     - Centralized repository is required for different types of logs. Azure Data Explorer, as a unified big data analytics platform, allows you to build advanced analytics scenarios.

DUTCH MICROSOFT SECURITY MEETUP

techcommunity.microsoft.com

Microsoft Sign In

Automation: Integrate Azure Data Explorer as Long-Term Log Retention for Microsoft Sentinel

By Sreedhar Ande

Published Oct 26 2021 02:54 PM 7,465 Views

Out of the box, Microsoft Sentinel provides 90 days of data retention for free. In some parts of the world and within certain industries, there are regulations that organizations must adhere to which require data retention up to 7 years or longer. The current challenge is that the max retention for Log Analytics workspaces is 2 years. There has been a need for a solution that will allow for more time and cost saving for long-term retention.

This blog is going to detail how logs from Log Analytics workspace can easily be migrated into long-term storage using Azure Data Explorer (ADX) to comply with retention standards as well as reduce costs with the help of PowerShell script.

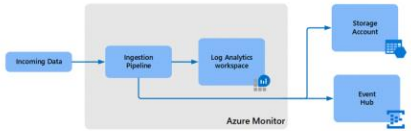
Thanks to @Javier Soriano for his inputs into this blog post

Azure Data Explorer (ADX)

Azure Data Explorer is a big data analytics platform that is highly optimized for log and data analytics. Since Azure Data Explorer uses Kusto Query Language (KQL) as its query language, it's a good alternative for Microsoft Sentinel data storage. Using Azure Data Explorer for your data storage enables you to run cross-platform queries and visualize data across both Azure Data Explorer and Microsoft Sentinel.
For more information, see the Azure Data Explorer documentation and blog

Log Analytics Data Export Architecture

The following image shows a sample flow of exported data through the Azure Monitor ingestion pipeline. Your data is directed to Log Analytics by default, but you can also configure it to export to an Azure Storage Account or Event Hub

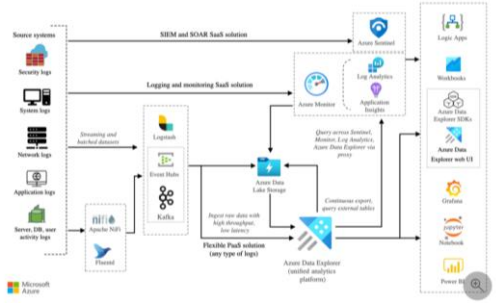


learn.microsoft.com

Microsoft Documentation

the use of these marks.

Architecture



Download a Visio file of this architecture.

Dataflow

1. Combine features provided by Microsoft Sentinel and Azure Monitor with Azure Data Explorer to build a flexible and cost-optimized end-to-end monitoring solution. Below are some examples:

   - Use Microsoft Sentinel as a SIEM and SOAR component in the overall monitoring solution where you can ingest security logs from firewalls, Defender for Cloud, and so on. SIEM is short for *security information and event management*, whereas SOAR is short for *security orchestration, automation and response*.
   - Use Azure Monitor's native capabilities for IT asset monitoring, dashboarding, and alerting so you can ingest logs from VMs, services, and so on.
   - Use Azure Data Explorer for full flexibility and control in all aspects for all types of logs in the following scenarios:
     - No *out of the box* features provided by Microsoft Sentinel and Azure Monitor SaaS solutions such as application trace logs.
     - Greater flexibility for building quick and easy near-real-time analytics dashboards, granular role-based access control, time series analysis, pattern recognition, anomaly detection and forecasting, and machine learning. Azure Data Explorer is also well integrated with ML services such as Databricks and Azure Machine Learning. This integration allows you to build models using other tools and services and export ML models to Azure Data Explorer for scoring data.
     - Longer data retention is required in cost effective manner.
     - Centralized repository is required for different types of logs. Azure Data Explorer, as a unified big data analytics platform, allows you to build advanced analytics scenarios.

DUTCH MICROSOFT SECURITY MEETUP

techcommunity.microsoft.com

Microsoft Sign In

Automation: Integrate Azure Data Explorer as Long-Term Log Retention for Microsoft Sentinel

By Sreedhar Ande
Published Oct 26 2021 02:54 PM 7,465 Views

Out of the box, Microsoft Sentinel provides 90 days of data retention for free. In some parts of the world and within certain industries, there are regulations that organizations must adhere to which require data retention up to 7 years or longer. The current challenge is that the max retention for Log Analytics workspaces is 2 years. There has been a need for a solution that will allow for more time and cost saving for long-term retention.

This blog is going to detail how logs from Log Analytics workspace can easily be migrated into long-term storage using Azure Data Explorer (ADX) to comply with retention standards as well as reduce costs with the help of PowerShell script.

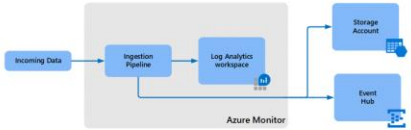
Thanks to @Javier Soriano for his inputs into this blog post

Azure Data Explorer (ADX)

Azure Data Explorer is a big data analytics platform that is highly optimized for log and data analytics. Since Azure Data Explorer uses Kusto Query Language (KQL) as its query language, it's a good alternative for Microsoft Sentinel data storage. Using Azure Data Explorer for your data storage enables you to run cross-platform queries and visualize data across both Azure Data Explorer and Microsoft Sentinel.
For more information, see the Azure Data Explorer documentation and blog

Log Analytics Data Export Architecture

The following image shows a sample flow of exported data through the Azure Monitor ingestion pipeline. Your data is directed to Log Analytics by default, but you can also configure it to export to an Azure Storage Account or Event Hub

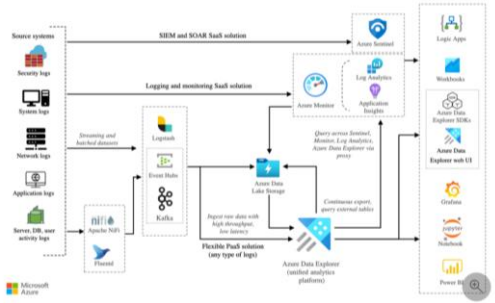


learn.microsoft.com

Microsoft Documentation

the use of these marks.

Architecture



Download a Visio file of this architecture.

Dataflow

1. Combine features provided by Microsoft Sentinel and Azure Monitor with Azure Data Explorer to build a flexible and cost-optimized end-to-end monitoring solution. Below are some examples:
   - Use Microsoft Sentinel as a SIEM and SOAR component in the overall monitoring solution where you can ingest security logs from firewalls, Defender for Cloud, and so on. SIEM is short for *security information and event management*, whereas SOAR is short for *security orchestration, automation and response*.
   - Use Azure Monitor's native capabilities for IT asset monitoring, dashboarding, and alerting so you can ingest logs from VMs, services, and so on.
   - Use Azure Data Explorer for full flexibility and control in all aspects for all types of logs in the following scenarios:
     - No *out of the box* features provided by Microsoft Sentinel and Azure Monitor SaaS solutions such as application trace logs.
     - Greater flexibility for building quick and easy near-real-time analytics dashboards, granular role-based access control, time series analysis, pattern recognition, anomaly detection and forecasting, and machine learning. Azure Data Explorer is also well integrated with ML services such as Databricks and Azure Machine Learning. This integration allows you to build models using other tools and services and export ML models to Azure Data Explorer for scoring data.
     - Longer data retention is required in cost effective manner.
     - Centralized repository is required for different types of logs. Azure Data Explorer, as a unified big data analytics platform, allows you to build advanced analytics scenarios.

techcommunity.microsoft.com

Microsoft Sign In

What's New: Azure Sentinel Hunting supports ADX cross-resource queries

By Ben Nick
Published Jul 14 2021 12:00 PM 7,744 Views

Now in preview, you can use Azure Data Explorer (ADX) cross-resource queries from with-in the hunting query page, the livestream page, and the logs (Log Analytics) page. Although Log Analytics remains the primary data storage location for performing analysis with Azure Sentinel, there are cases where ADX is required to store data due to cost, retention periods, or other factors.

You can learn more about sending logs from Azure Sentinel to Azure Data Explorer for long-term retention here: Integrate Azure Data Explorer for long-term log retention

Creating cross-resource queries
To query data stored in ADX clusters, simply use the adx() function to specify the ADX cluster, database name, and desired table. You can then query the output as you would any other table. If you have access to an ADX cluster with active data, it is super easy to try.

Here is a brief summary of the adx() function syntax to help get you started:

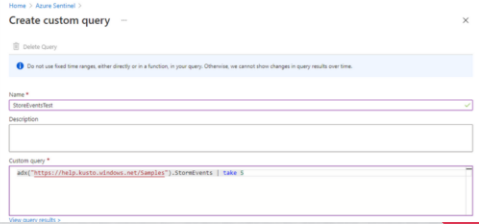
```
adx("<Cluster URI>/<Database Name>).<Table Name>
```

Here is an example query that accesses public data:

```
adx("https://help.kusto.windows.net/Samples").StormEvents | take 5
```

You can find the full details here: Cross-query your Log Analytics or Application Insights resources and Azure Data Explorer

Using cross-resource queries on the hunting queries, livestream, and logs pages
Once you know how to construct cross-reference queries, using them in the hunting experience is easy. Go to the hunting queries page and click "+ New query" to create a new custom query. Add your cross-resource query to the "Custom Query" field as you would for any other hunting query.



Log ingestion challenges

- Cloud is always changing
  - MMA → AMA
  - Lots of specific features (still) in preview
- Azure Arc is not to be underestimated
- Co-operate with other ops teams and vendors
  - Managing DCRs
- Sentinel as a "security data lake"?
  - Splitting and filtering logs into different destinations
- Virtual Machine vs Container
- Microsoft vs third-party option

Logstash

Logstash

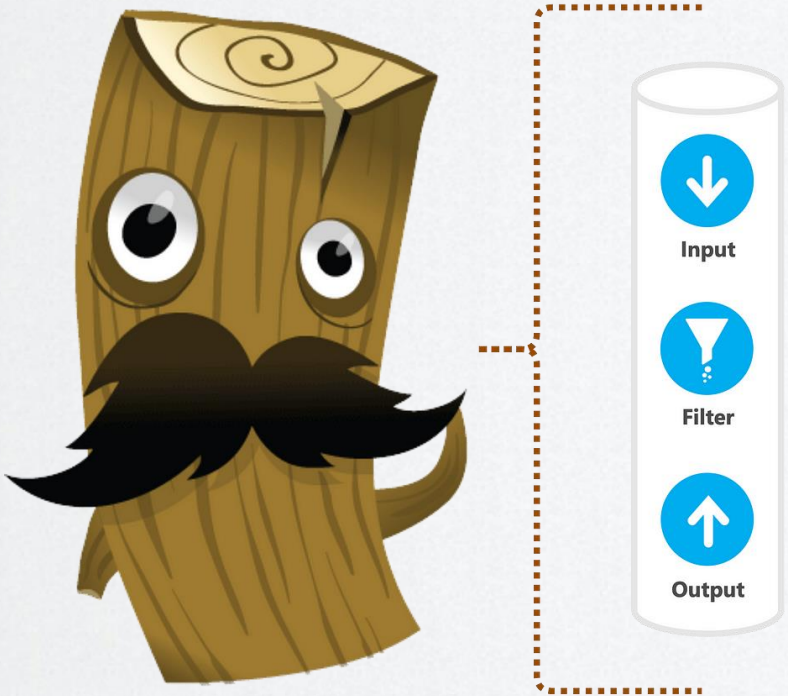
- "Swiss army knife" CH
- VERY flexible!
  - Plethora of input and output plug-ins available
    - Syslog, files, shares, databases
    - Log Analytics, Azure Data Explorer, Event Hub, Blob
  - On-the-fly parsing and filtering
  - Run within a container (ACI, AKS, …)

DUTCH MICROSOFT SECURITY MEETUP

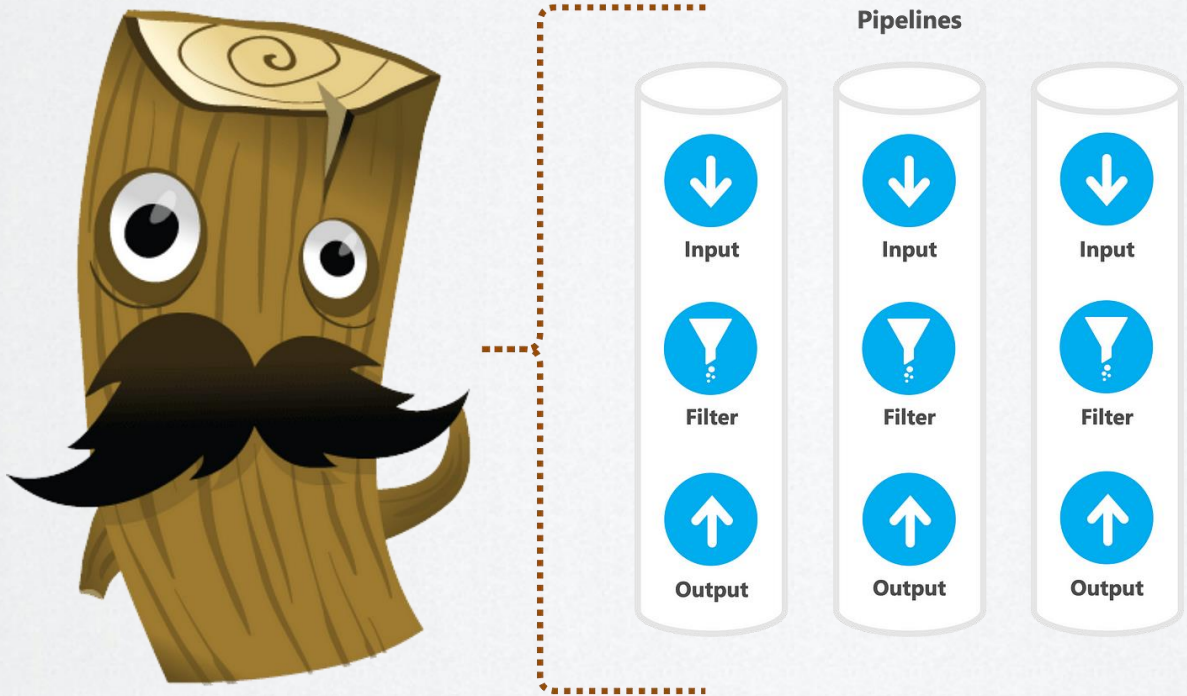
Logstash

DUTCH MICROSOFT SECURITY MEETUP

Logstash

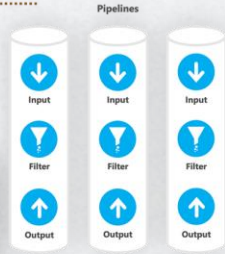


Logstash



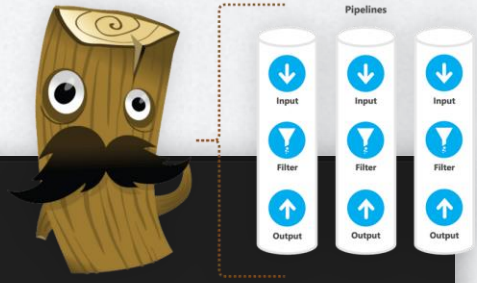
DUTCH MICROSOFT SECURITY MEETUP

Logstash




```
input {
    jdbc {
        # Postgres jdbc connection string to our database, mydb
        jdbc_connection_string => "jdbc:postgresql://localhost:5432/security"
        # The user we wish to execute our statement as
        jdbc_user => "dbuser"
        # The user we wish to execute our statement as
        jdbc_password => "{$dbpassword}"
        # The path to our downloaded jdbc driver
        jdbc_driver_library => "/usr/share/logstash/modules/postgres/postgresql-42.2.12.jar"
        # The name of the driver class for Postgresql
        jdbc_driver_class => "org.postgresql.Driver"
        # postgres query with column tracking to avoid importing duplicates
        statement => "SELECT uid, timestamp, event, message, username, ipaddress FROM authentications WHERE uid > :sql_last_value"
        use_column_value => true
        tracking_column => "uid"
        # schedule to run every 5 minutes
        schedule => "*/5 * * * *"
    }
}

output {
    microsoft-logstash-output-azure-loganalytics {
        workspace_id => "${SENTINEL_ID}"
        workspace_key => "${SENTINEL_KEY}"
        log_type => "postgreSQLauthentications"
        key_names  => ['timestamp','event','message','username','ipaddress']
        flush_items => 10
        flush_interval_time => 5
    }
    # for debug
    stdout { codec => rubydebug }
}
```

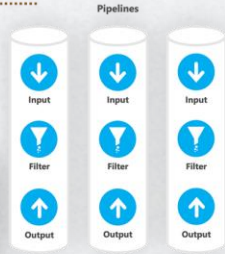
Logstash




```
input {
    jdbc {
        # Postgres jdbc connection string to our database, mydb
        jdbc_connection_string => "jdbc:postgresql://localhost:5432/security"
        # The user we wish to execute our statement as
        jdbc_user => "dbuser"
        # The user we wish to execute our statement as
        jdbc_password => "{$dbpassword}"
        # The path to our downloaded jdbc driver
        jdbc_driver_library => "/usr/share/logstash/modules/postgres/postgresql-42.2.12.jar"
        # The name of the driver class for Postgresql
        jdbc_driver_class => "org.postgresql.Driver"
        # postgres query with column tracking to avoid importing duplicates
        statement => "SELECT uid, timestamp, event, message, username, ipaddress FROM authentications WHERE uid
        use_column_value => true
        tracking_column => "uid"
        # schedule to run every 5 minutes
        schedule => "*/5 * * * *"
    }
}
```

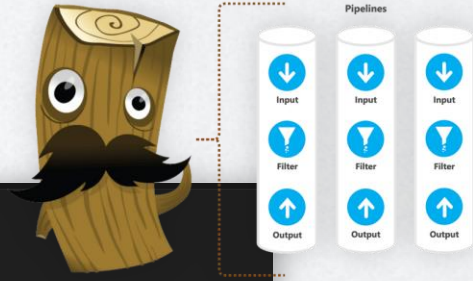
DUTCH MICROSOFT SECURITY MEETUP

Logstash




```
input {
    jdbc {
        # Postgres jdbc connection string to our database, mydb
        jdbc_connection_string => "jdbc:postgresql://localhost:5432/security"
        # The user we wish to execute our statement as
        jdbc_user => "dbuser"
        # The user we wish to execute our statement as
        jdbc_password => "{$dbpassword}"
        # The path to our downloaded jdbc driver
        jdbc_driver_library => "/usr/share/logstash/modules/postgres/postgresql-42.2.12.jar"
        # The name of the driver class for Postgresql
        jdbc_driver_class => "org.postgresql.Driver"
        # postgres query with column tracking to avoid importing duplicates
        statement => "SELECT uid, timestamp, event, message, username, ipaddress FROM authentications WHERE uid > :sql_last_value"
        use_column_value => true
        tracking_column => "uid"
        # schedule to run every 5 minutes
        schedule => "*/5 * * * *"
    }
}

output {
    microsoft-logstash-output-azure-loganalytics {
        workspace_id => "${SENTINEL_ID}"
        workspace_key => "${SENTINEL_KEY}"
        log_type => "postgreSQLauthentications"
        key_names  => ['timestamp','event','message','username','ipaddress']
        flush_items => 10
        flush_interval_time => 5
    }
    # for debug
    stdout { codec => rubydebug }
}
```

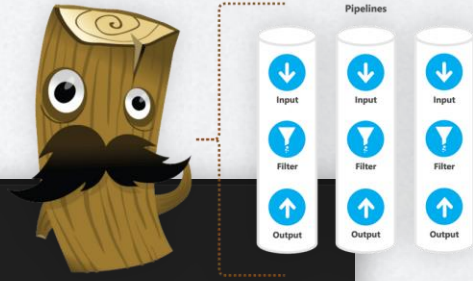
Logstash




```
input {
    syslog {
        port => 5514
    }
}

output {
    microsoft-logstash-output-azure-loganalytics {
        workspace_id => "${SENTINEL_ID}"
        workspace_key => "${SENTINEL_KEY}"
        proxy => "<http://proxy.domain.com:8080>"
        retransmission_time => 2
        plugin_flush_interval => 2
        custom_log_table_name => "${TABLE_NAME}"
    }
}
```

DUTCH MICROSOFT SECURITY MEETUP

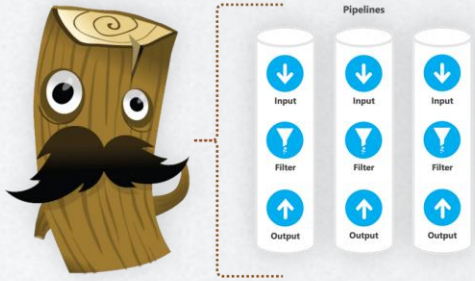
Logstash




```
input {
    syslog {
        port => 5514
    }
}

output {
    microsoft-sentinel-logstash-output-plugin {
        client_app_Id => "${APP_ID}"
        client_app_secret => "${APP_SECRET}"
        tenant_id => "${TENANT_ID}"
        proxy => "http://proxy.domain.com:8080"
        data_collection_endpoint => "https://${DCE_URI}.ingest.monitor.azure.com"
        dcr_immutable_id => "dcr-${IMMUTABLE_ID}"
        dcr_stream_name => "Custom-${TABLE_NAME}_CL"
    }
}
```

DUTCH MICROSOFT SECURITY MEETUP

Logstash

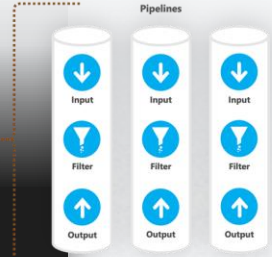



```
input {
    tcp {
        port ⇒ 514
        type ⇒ syslog
        host ⇒ "141.93.182.143"
        tags ⇒ ["gso_sentinel"]
    }
}
input {
    udp {
        port ⇒ 514
        type ⇒ syslog
        host ⇒ "141.93.182.143"
        queue_size ⇒ 16384
        workers ⇒ 4
        receive_buffer_bytes ⇒ 24576000
        codec ⇒ plain { charset ⇒ "ISO-8859-1" }
        tags ⇒ ["gso_sentinel"]
    }
}
input {
    tcp {
        port ⇒ 7514
        type ⇒ syslog
        mode ⇒ "server"
        host ⇒ "141.93.182.143"
        ssl_enable ⇒ true
        ssl_cert ⇒ "/apps1/log-jars/KPNCert/syslogserver.pem"
```

DUTCH MICROSOFT SECURITY MEETUP

Logstash

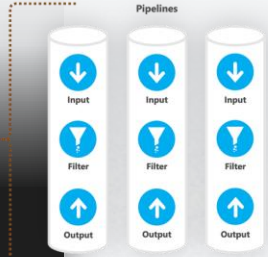
```
    pipeline_id => main
    workers => 4
    receive_buffer_bytes => 24576000
    codec => plain { charset => "ISO-8859-1" }
    tags => ["gso_sentinel"]
  }
}
input {
  tcp {
    port => 7514
    type => syslog
    mode => "server"
    host => "141.93.182.143"
    ssl_enable => true
    ssl_cert => "/apps1/log-jars/KPNCert/syslogserver.pem"
    ssl_key => "/apps1/log-jars/KPNCert/syslogserverkey.pem"
    ssl_certificate_authorities => [ "/apps1/log-jars/KPNCert/RootCA.pem" ]
    ssl_verify => true
    ssl_key_passphrase => "${CERT_PASS}"
    ssl_supported_protocols => ['TLSv1.1', 'TLSv1.2', 'TLSv1.3']
    tags => ["gso_sentinel"]
  }
}

filter {
  if ("gso_sentinel" in [tags]){
    mutate {
      add_field => { "Country" => "NL" }
      add_field => { "connector_host" => "hostname.domain.com" }
    }
    if ([host] == "17.93.180.49") or ([host] == "17.93.126.47") {
    mutate {
      add_field => { "sentinelTable" => "UX_rhlinux" }
    }
    }
    else if ([host] == "17.93.177.62") or ([host] == "17.93.178.219") or ([host] == "17.93.178.79") or ([host] == "17.93.126.92")
    or ([host] == "17.93.125.114") or ([host] == "17.93.125.126") or ([host] == "17.93.126.40") or ([host] == "17.93.178.204") or
    or ([host] == "17.93.180.43") or ([host] == "17.93.125.149") or ([host] == "17.93.125.124") or ([host] == "17.93.179.215") or
    or ([host] == "17.93.188.100") or ([host] == "17.93.178.31") {
    mutate {
      add_field => { "sentinelTable" => "UX_aix" }
```



DUTCH MICROSOFT SECURITY MEETUP

Logstash

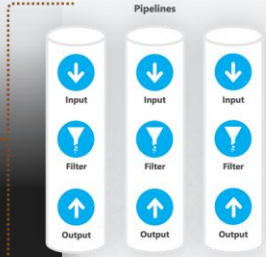
```
        else if ([host] == "10.16.128.30") {
            mutate {
                add_field => { "sentinelTable" => "AC_Aruba" }
            }
        }
        else {
        mutate {
            add_field => { "sentinelTable" => "New_SourcesAlert" }
        }
        }
        grok {
        keep_empty_captures => "true"
        match => { "@timestamp" => "%{YEAR:sys_year}-%{MONTHNUM:sys_month}-%{MONTHDAY:sys_day}%{GREEDYDATA}" }
        }
    }
}

output {
    if("gso_sentinel" in [tags]){
        if([sentinelTable] == "UX_rhlinux") {
            microsoft-logstash-output-azure-loganalytics {
                workspace_id => "${SENTINEL_ID}"
                workspace_key => "${SENTINEL_KEY}"
                proxy => "http://proxy.domain.com:8080"
                retransmission_time => 2
                plugin_flush_interval => 2
                custom_log_table_name => "UX_rhlinux"
            }
        }
    }
    else if([sentinelTable] == "UX_aix") {
        microsoft-logstash-output-azure-loganalytics {
            workspace_id => "${SENTINEL_ID}"
            workspace_key => "${SENTINEL_KEY}"
            proxy => "http://proxy.domain.com:8080"
            retransmission_time => 2
            plugin_flush_interval => 2
            custom_log_table_name => "UX_aix"
        }
    }
```



DUTCH MICROSOFT SECURITY MEETUP

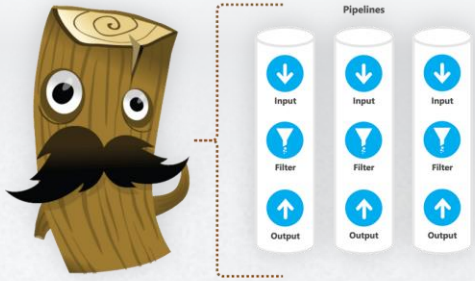
Logstash

```
            client_app_secret => "<client_app_secret>"
            tenant_id => "<tenant_id>"
            data_collection_endpoint => "https://dce-uri.westeurope-1.ingest.monitor.azure.com"
            dcr_immutable_id => "dcr-<id>"
            dcr_stream_name => "Custom-UX_Hpunix"
        }
    }
    else if([sentinelTable] == "UX_Solaris") {
        kusto {
            path => "/tmp/kusto/%{+YYYY-MM-dd-HH-mm-ss}.txt"
            ingest_url => "https://ingest-clustername.westeurope.kusto.windows.net"
            app_id => "<client_app_Id>"
            app_key=> "<client_app_secret>"
            app_tenant => "<tenant_id>"
            database => "logstash-archive"
            table => "Cisco_RO_CL"
            json_mapping => "UX_Solaris"
        }
    }
    else if([sentinelTable] == "AC_Aruba") {
        microsoft-sentinel-logstash-output-plugin {
            client_app_Id => "<client_app_Id>"
            client_app_secret => "<client_app_secret>"
            tenant_id => "<tenant_id>"
            data_collection_endpoint => "https://dce-uri.westeurope-1.ingest.monitor.azure.com"
            dcr_immutable_id => "dcr-<id>"
            dcr_stream_name => "Custom-AC_Aruba"
        }
    }
    else if([sentinelTable] == "New_SourcesAlert") {
        microsoft-logstash-output-azure-loganalytics {
            workspace_id => "${SENTINEL_ID}"
            workspace_key => "${SENTINEL_KEY}"
            proxy => "http://proxy.domain.com:8080"
            retransmission_time => 2
            plugin_flush_interval => 2
            custom_log_table_name => "New_SourcesAlert"
        }
    }
}
```



DUTCH MICROSOFT SECURITY MEETUP

Logstash

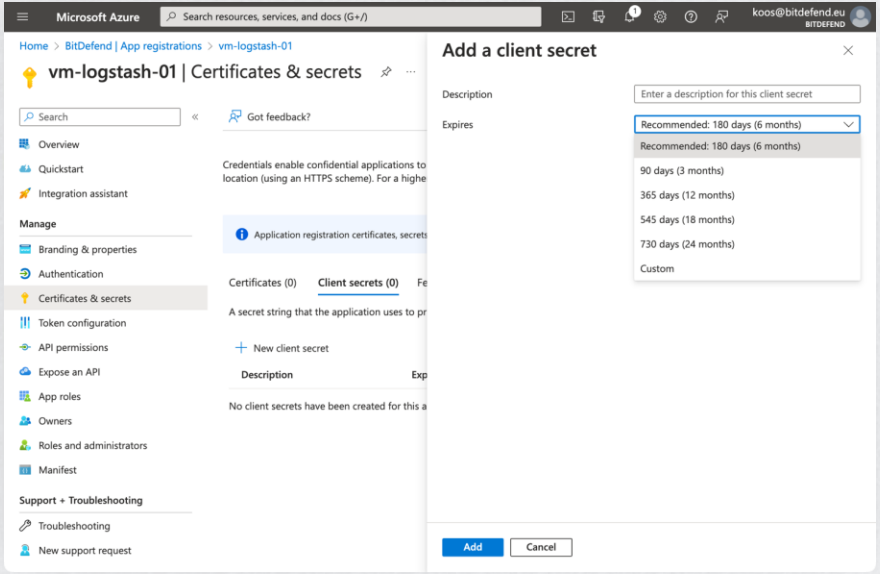


DUTCH MICROSOFT SECURITY MEETUP

Managing keys

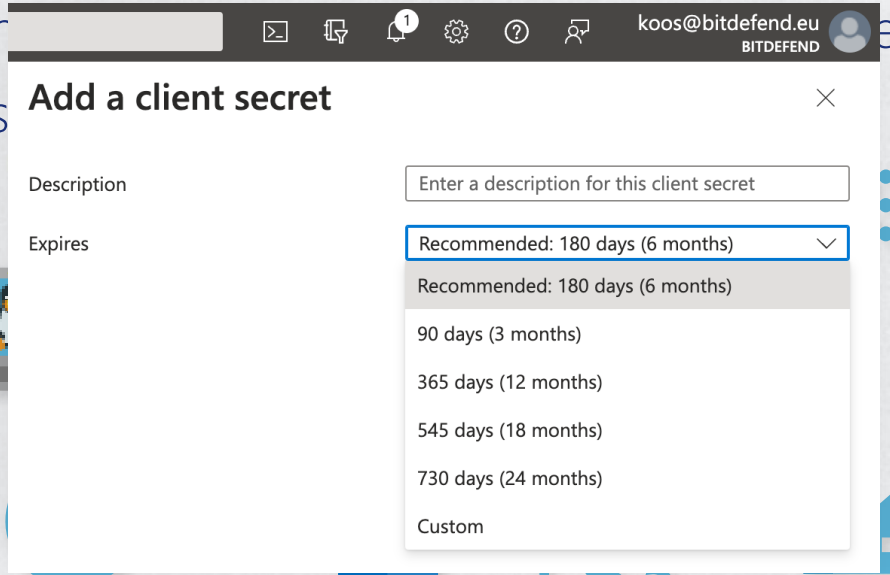
Managing keys

- (Enterprise) Applications secrets



Managing keys

- (Enterprise) Applications secrets
- Ch expire
- Us



DUTCH MICROSOFT SECURITY MEETUP

Managing keys

- (Enterprise) Applications secrets
- Check for older secrets which may never expire
- Use Managed-Identities if possible
- Implement key-rotation mechanism


LOGSTASH

Logstash **r0t8r**

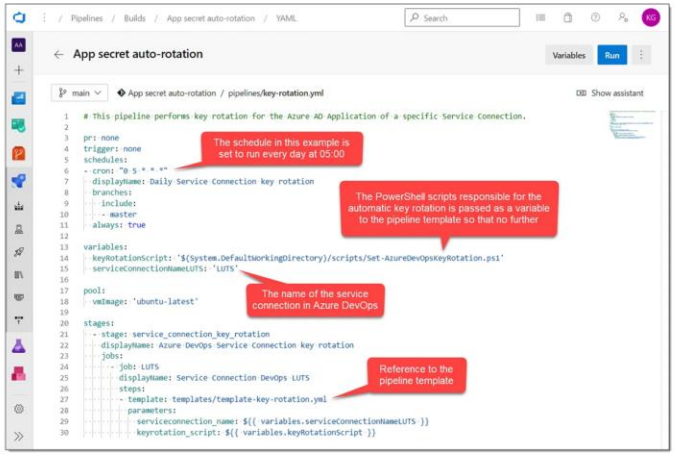
- Sequel to Azure DevOps "**r0t8r**"

Logstash **r0t8r**

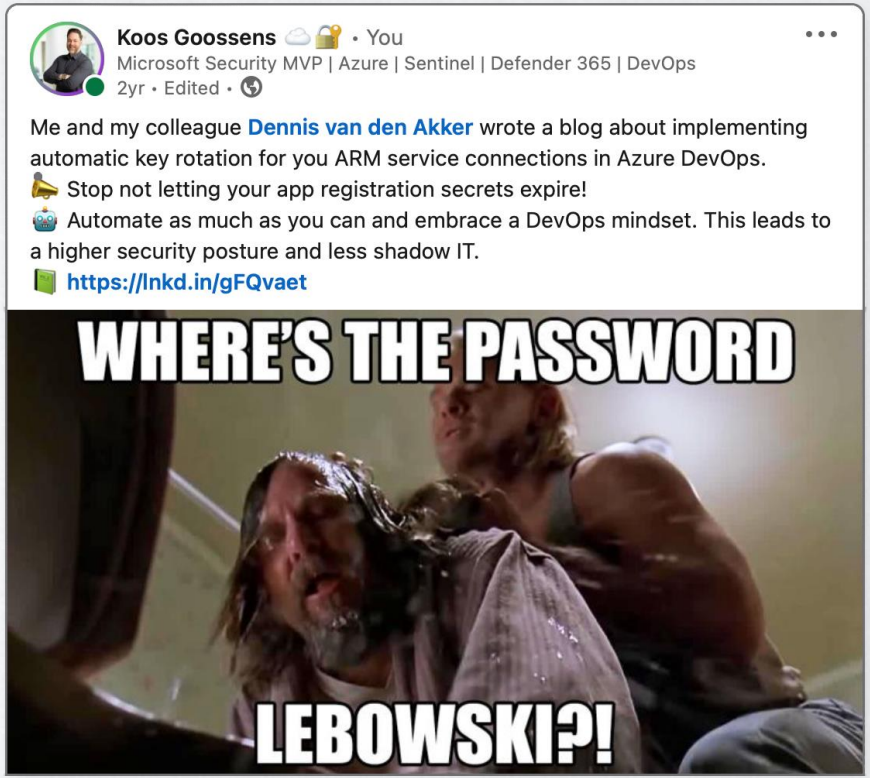
- Sequel to Azure DevOps "**r0t8r**"

Setting up the pipeline

> *A copy of all source code listed below can be found on my Github page here.*

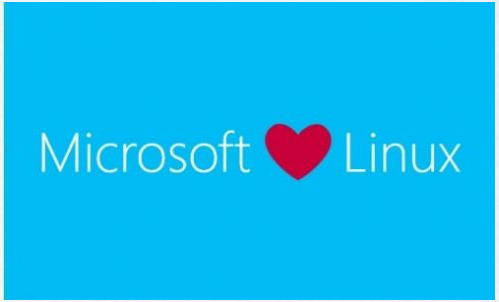


Note: the only changes you should make is the serviceConnectionName variable.



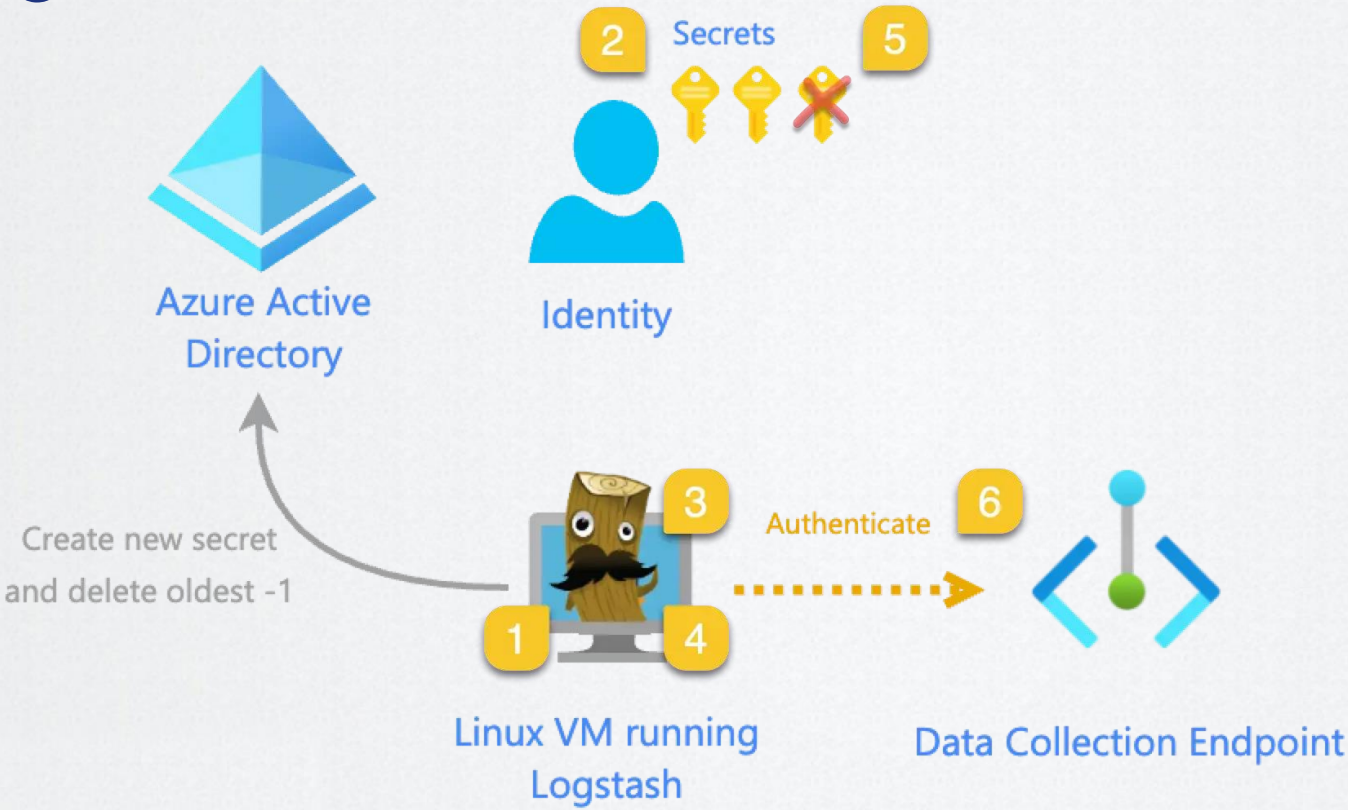
DUTCH MICROSOFT SECURITY MEETUP

Logstash **r0t8r**



- Sequel to Azure DevOps "**r0t8r**"
- We can run PowerShell on Linux too!

Logstash **r0t8r**



DUTCH MICROSOFT SECURITY MEETUP

Logstash **r0t8r**

- PowerShell Credentials
  - appId.CRED file containing System.Security.SecureString
  - Avoids storing sensitive strings in memory as plain text
  - The value is automatically protected when the instance is initialized or when the value is modified.

Logstash **r0t8r**

- One more thing: minor preparations
  - Application needs to be **owner** of itself
  - Application has **Application.ReadWrite.OwnedBy** **Microsoft.Graph** permissions
- Use my script **Add-AppOwner.ps1** *(one time only)*

Logstash r0t8r

- One more th… …parations
  - o… …lf
    - …nly)

DUTCH MICROSOFT SECURITY MEETUP

Logstash **r0t8r**

Logstash **r0t8r**

- How to run **r0t8r**?

```
sudo pwsh \
    -file logstash-rot8r.ps1 \
    -tenantId <tenantId> \
    -applicationId <appId> \
    -logstashConfigLocation /etc/../example.conf
```

Logstash **r0t8r**

- Schedule with cronjob

sudo crontab -e

```
# ┌──────────── minute [ 0 – 59 ]
# │ ┌──────────── hour [ 0 – 23 ]
# │ │ ┌──────────── day of the month [ 1 – 31 ]
# │ │ │ ┌──────────── month [ 1 – 12 ]
# │ │ │ │ ┌──────────── day of the week [ 0 – 6 ] (Sunday - Saturday)
# │ │ │ │ │
# │ │ │ │ │
# │ │ │ │ │
# * * * * * command or script
```

Logstash r0t8r

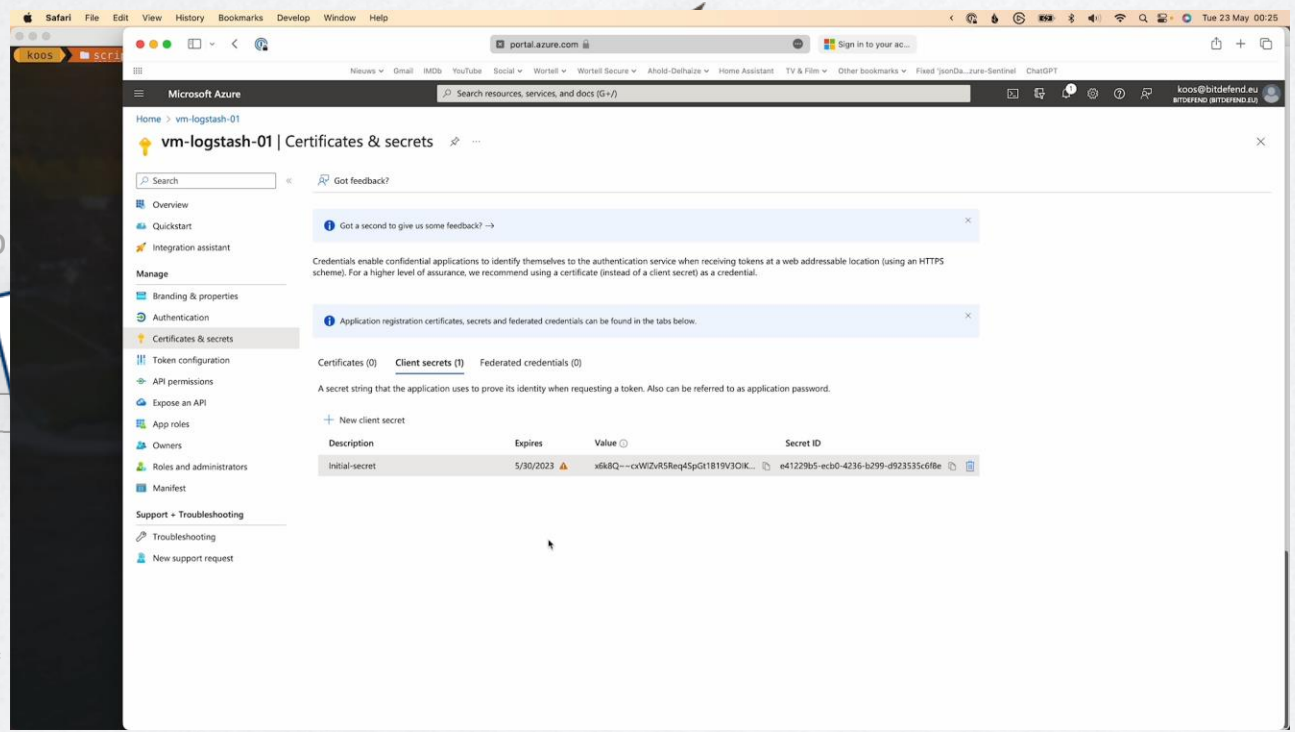
- Schedule with c

sudo crontab -e

```
#
#
#
#
#
#
#
#
# * * * * * com
```

DUTCH MICROSOFT SECURITY MEETUP

Logstash **r0t8r**



Logstash **r0t8r**

- Using Logstash Keystore 

client_app_secret => "pg%lecateMnsr&@p"

Logstash **r0t8r**

- Using Logstash Keystore 

```
client_app_secret => "${app_secret}"
```

Logstash **r0t8r**

- Using Logstash Keystore

logstash.keystore

client_app_secret => "${app_secret}"

DUTCH MICROSOFT SECURITY MEETUP

Logstash r0t8r

- Using Logstash Keystore

logstash.keystore

LOGSTASH_KEYSTORE_PASS

client_app_secret => "${app_secret}"

DUTCH MICROSOFT SECURITY MEETUP

Logstash **r0t8r**

- Using Logstash Keystore

LOGSTASH_KEYSTORE_PASS

logstash.keystore

client_app_secret => "${app_secret}"

DUTCH MICROSOFT SECURITY MEETUP

Logstash **r0t8r**

- Using Logstash Keystore

LOGSTASH_KEYSTORE_PASS

logstash.keystore

client_app_secret => "pg%lecateMnsr&@p"

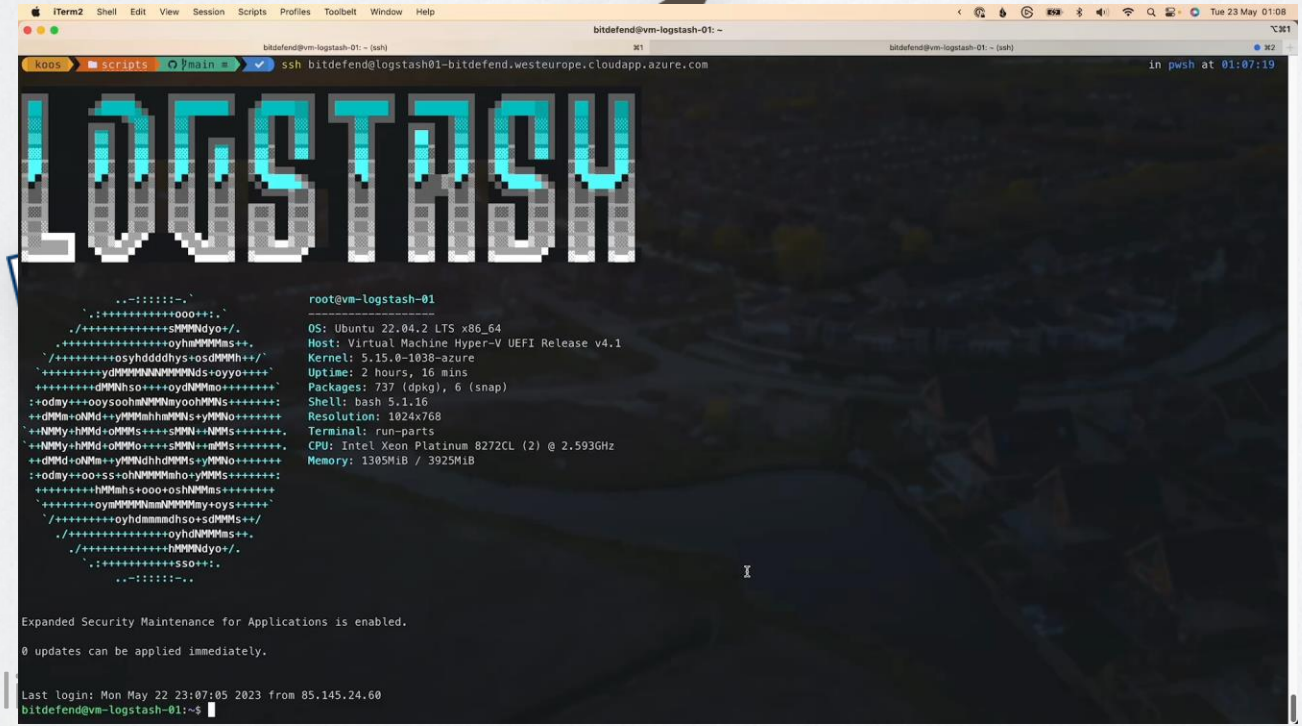
Logstash **r0t8r**

- Using Logstash

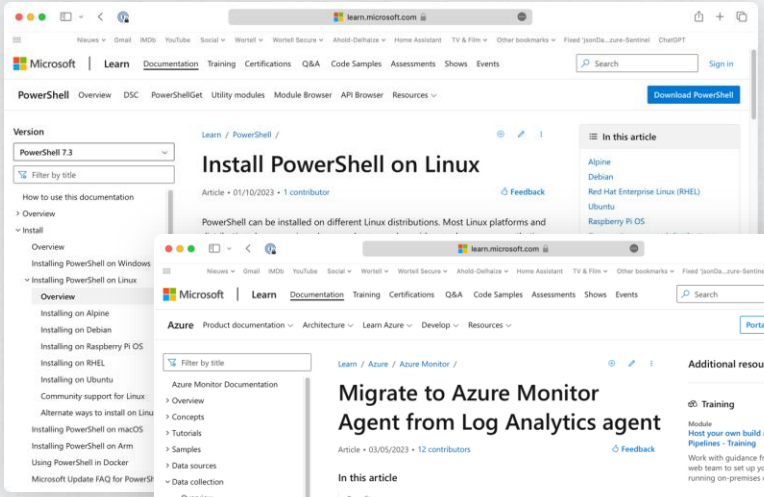
client_app_secret => "pg%lecateMnsr&@p"

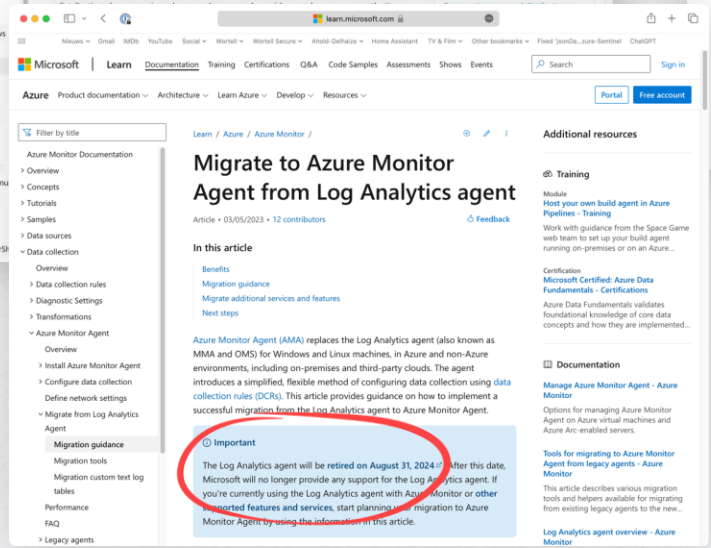
DUTCH MICROSOFT SECURITY MEETUP

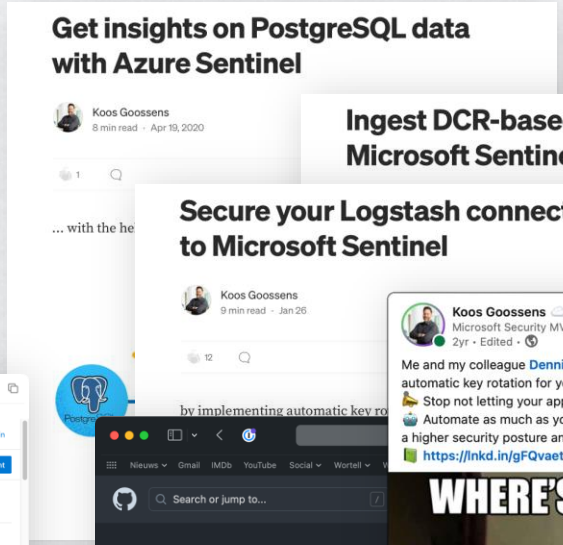
Logstash **r0t8r**

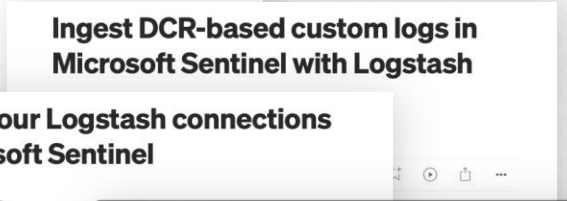


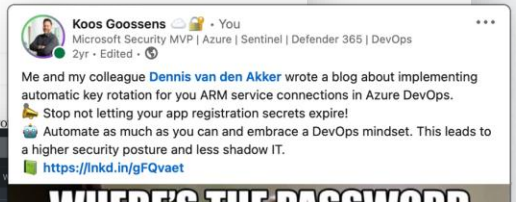
References











DUTCH MICROSOFT SECURITY MEETUP


DUTCH
MICROSOFT SECURITY
MEETUP

Are there any questions?_