

A fluffy black cat with yellow eyes is sitting on a desk next to a laptop. The cat is looking towards the camera. The background is a blurred office or home workspace with white shelves and a lamp.

Microsoft Sentinel for Developers

Laura Kokkarinen & Thomas Vochten

Who are we?



Thomas Vochten

Workplace Solution Lead, MVP

Sopra Steria, Belgium



Laura Kokkarinen

Software Architect, MVP

Sulava, Finland

Agenda

Why you should be interested

A quick tour around Microsoft Sentinel

Plugging in a custom app to Sentinel

Detecting incidents

Automating responses

```
import java.util.ArrayList;
import java.util.Scanner;
import java.io.File;
import java.io.IOException;
import java.util.Arrays;

public class AirlineProblem {

    public static void main(String[] args){
        Scanner scannerToReadAirlines = null;
        try{
            scannerToReadAirlines = new Scanner(new File("airlines.txt"));
        } catch(IOException e){
            System.out.println("Could not connect to file airlines.txt.");
            System.exit(0);
        }
        if(scannerToReadAirlines != null){
            ArrayList<Airline> airlinesPartnersNetwork = new ArrayList<Airline>();
            Airline newAirline;
            String lineFromFile;
            String[] airlineNames;
            while( scannerToReadAirlines.hasNext() ){
                lineFromFile = scannerToReadAirlines.nextLine();
                airlineNames = lineFromFile.split(",");
                newAirline = new Airline(airlineNames);
                airlinesPartnersNetwork.add( newAirline );
            }
            System.out.println(airlinesPartnersNetwork);
        }
    }
}
```

A fluffy grey cat with yellow eyes is sitting on a laptop keyboard. The cat is looking directly at the camera. The background is a blurred indoor setting with a white cabinet and a lamp.

Now what?

You deployed your app.
Do you really know what's going on?

Some Real-World Security Scenarios

- Compromised accounts
- API key misuse
- Brute-force login attempts
- Session hijacking
- Account abuse from unknown IPs
- Use of expired or forged JWT tokens
- Sudden spike in data exports or downloads
- Malicious actors misusing your app to get a foot in the door
- Access to production systems from unusual locations
- Chained low-severity vulnerabilities used for privilege escalation
- ...

```
import java.util.ArrayList;
import java.util.Scanner;
import java.io.File;
import java.io.IOException;
import java.util.Arrays;

public class airlineProblem {

    public static void main(String[] args) {
        Scanner scannerToReadAirlines = null;
        try {
            scannerToReadAirlines = new Scanner(new File("airlines.txt"));
        } catch (IOException e) {
            System.out.println("could not connect to file airlines.txt.");
            System.exit(0);
        }
        if (scannerToReadAirlines != null) {
            ArrayList<Airline> airlinesPartnersNetwork = new ArrayList<Airline>();
            Airline newAirline;
            String lineFromFile;
            String[] airlineNames;
            while (scannerToReadAirlines.hasNextLine()) {
                lineFromFile = scannerToReadAirlines.nextLine();
                airlineNames = lineFromFile.split(",");
                newAirline = new Airline(airlineNames);
                airlinesPartnersNetwork.add(newAirline);
            }
            System.out.println(airlinesPartnersNetwork);
            Scanner keyboard = new Scanner(System.in);
        }
    }
}
```


A fluffy grey cat is sitting on a laptop keyboard, which is placed on a wooden desk. The background is a blurred office environment with white shelves and a lamp. A semi-transparent white rectangle is overlaid on the image, containing the text.

But isn't that an operations problem?

What do you need to know as a
developer and why

Security Logging and Monitoring

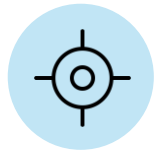
- Monitoring depends on quality logging!
- OWASP Top 10: Security Logging and Monitoring Failures
- “Shift Left”
“Defense in depth”
- Sentinel helps us adhere to the security requirements

- *Events, such as logins, failed logins, and high-value transactions, are not logged.*
- *Warnings and errors generate no, inadequate, or unclear log messages.*
- *Logs are only stored locally.*
- *Logs of applications and APIs are not **monitored for suspicious activity**.*
- *No **alerting thresholds** and **response escalation processes** are in place.*
- *Penetration testing and DAST scanning do not trigger alerts.*
- *The application cannot detect, escalate, or alert for active attacks in **real-time**.*



[https://owasp.org/
Top10](https://owasp.org/Top10)

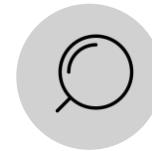
Microsoft Sentinel to the Rescue



Unified SIEM + SOAR



Built on Azure
Monitor and Log
Analytics



Correlates logs and
detects threats



Automates incident
response



Scalable and cloud-
native

Key Components & Capabilities



Data connectors and ingestion



Analytics and detection rules



Investigation tools and dashboards
















Response automation (Logic Apps, Functions)



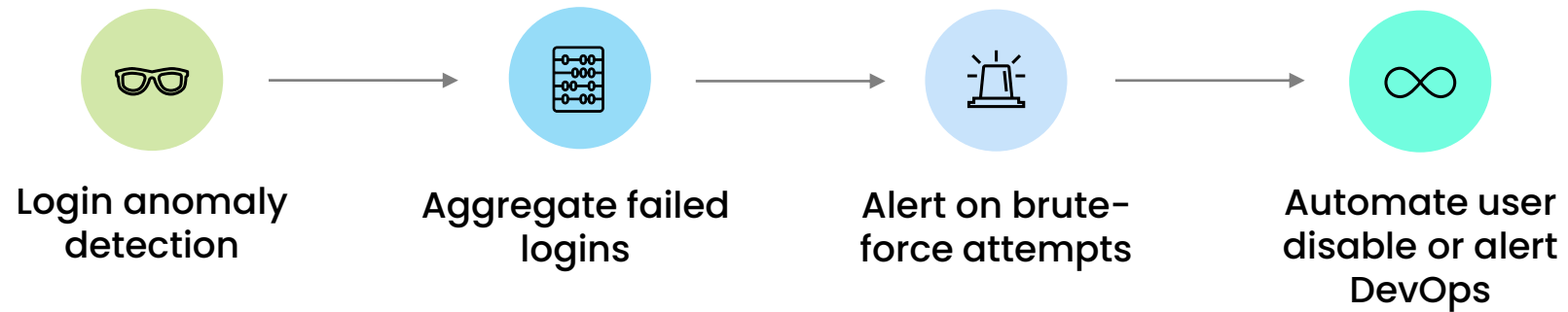
Built-in AI: Fusion, UEBA, anomaly detection

Data connectors

- 100+ built-in connectors
- Native support for most Microsoft services
- Templates for rules and workbooks
- Custom ingestion through an API, CEF or Syslog

	Microsoft 365 (formerly, Office 365) Microsoft
	Microsoft 365 Insider Risk Management (Preview) Microsoft
	Microsoft Defender for Cloud Apps Microsoft
	Microsoft Defender for Endpoint Microsoft
	Microsoft Defender for Identity Microsoft
	Microsoft Defender for Office 365 (Preview) Microsoft
	Microsoft Defender Threat Intelligence Microsoft
	Microsoft Defender XDR Microsoft
	Microsoft Entra ID Microsoft
	Microsoft Entra ID Protection Microsoft
	Microsoft Purview Information Protection (Preview) Microsoft
	Subscription-based Microsoft Defender for Cloud (Legacy) Microsoft
	Tenant-based Microsoft Defender for Cloud (Preview) Microsoft

Example: Typical Detection & Response Flow



Which events to log?

- Use threat modeling to identify what events to log for your specific application and business case
- Log enough but not too much



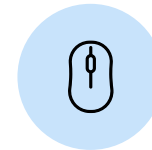
Authentication and authorization failures

Accessing resources, performing operations



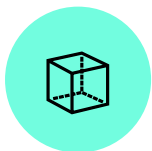
Session management failures

Invalid session token, JWT validation failures



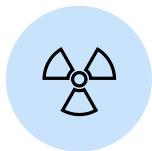
Input validation failures

Invalid params/values, payloads, outputs from external services



Deserialization failures

Invalid or unexpected serialized data



Use of higher-risk functionality

All admin actions, sensitive data, user-generated content, legal etc.



Suspicious activity

Attempts to bypass control flow, excessive usage

What information to log?

- Data to exclude or handle carefully: sensitive data, secrets, session identifiers, internal system information
- Log enough but not too much



When (UTC)

- 2020-05-27T14:30:00Z
- Consistency



Who (user or system)

- User type
- User ID
- Source IP address
- User agent
- Session ID (hashed!)



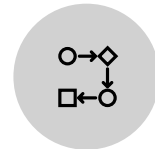
What (event details)

- Event type and severity
- Performed action
- Event description
- Affected resource
- Action outcome



Where (system location)

- App ID and address
- Client's geolocation
- Code location



How (technical details)

- Request details
- Response details
- Correlation ID

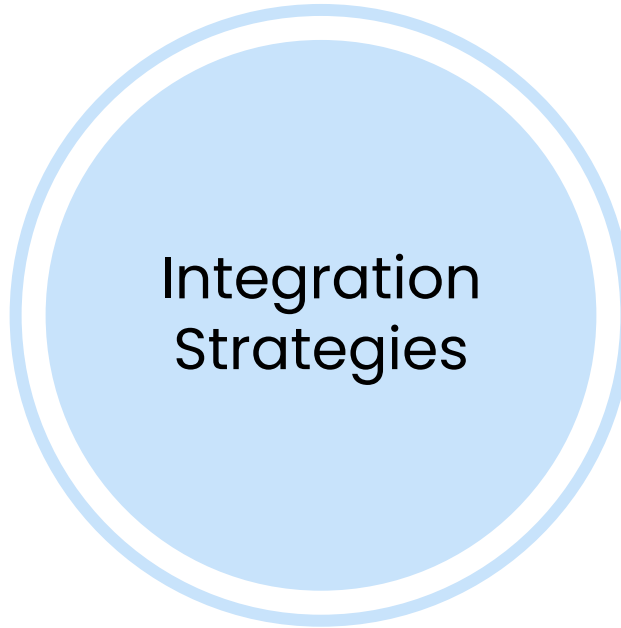
Log entry structure and best practices

- Log all events with a consistent structure (JSON schema)
- Validate and sanitize all data originating from clients and external applications before processing and logging
- Ensure proper encoding (e.g., UTF-8) to avoid log corruption

```
{  "datetime": "2025-05-10T14:30:00Z",
  "event_timestamp": "2025-05-10T14:29:55Z",
  "appid": "myapp-v1.2.3",
  "event": "AUTHN_login_fail",
  "severity": "WARN",
  "description": "User login failed due to incorrect password",
  "user_id": "9ed6e181-c4e5-4c9f-b7a6-6344f39a77bb",
  "user_type": "authenticated_user",
  "source_ip": "192.168.1.1",
  "useragent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64)",
  "host_ip": "10.0.0.1",
  "hostname": "auth.myapp.com",
  "protocol": "HTTPS",
  "port": 443,
  "request_uri": "/login",
  "request_method": "POST",
  "result_status": "FAILED",
  "reason": "Incorrect credentials",
  "http_status_code": 401,
  "region": "West Europe",
  "geo": "Europe",
  "correlation_id": "bf3e8dc2-cabe-443f-89c2-a2191f2ca112",
}
```

● Application Insights

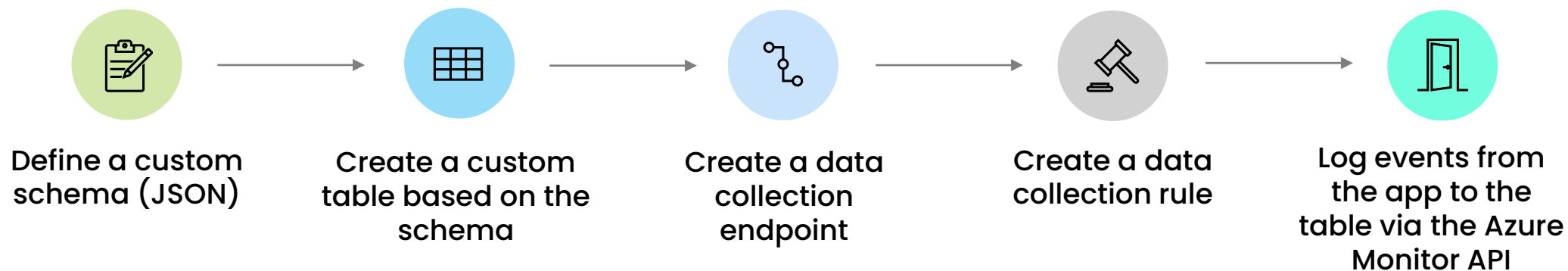
- Connect Application Insights to the Log Analytics Workspace used by Microsoft Sentinel
- **Pros:** Fast and easy
- **Cons:** Other than security events end up on the Sentinel workspace, resulting in higher cost



● Azure Monitor API

- Send log entries to the Log Analytics Workspace used by Microsoft Sentinel via Azure Monitor REST API
- **Pros:** Control what log entries to send to Sentinel, hence cost efficient to monitor
- **Cons:** Requires more effort to initially implement

Enable logging to Sentinel workspace via REST API



From schema to custom log analytics table

```
[
  {
    "timestamp": "2025-01-01T01:01:01.0000000Z",
    "appid": "00000000-0000-0000-0000-000000000000",
    "region": "West Europe",
    "geo": "Europe",
    "level": "Information",
    "event": "AUTHN_login_success:00000000-0000-0000-0000-000000000000",
    "description": "User 00000000-0000-0000-0000-000000000000 logged in successfully.",
    "host_ip": "127.0.0.1",
    "port": 1234,
    "request_method": "POST",
    "protocol": "https",
    "hostname": "azure.functions.com",
    "request_uri": "/api/LogEvent",
    "source_ip": "127.0.0.1",
    "useragent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36"
  }
]
```

AppSecurityEvents_CL

Schema Editor








> Azure Columns (6)

✓ Custom Columns (16)

Column name ↓	Description	Type
appid		String
description		String
event		String
geo		String
host_ip		String
hostname		String
...		...

Data collection endpoints & rules

- Needed when calling the Azure Monitor Logs Ingestion API
- DCE: Log Ingestion
- DCR: Access to custom table
- Important: Grant your app *"Monitoring Metrics Publisher"* permissions to the data collection rule.
- <https://github.com/LauraKokkarinen/FunctionApp.SentinelLogging>

<input type="checkbox"/>		demo-sentinellogging-asp	App Service plan
<input checked="" type="checkbox"/>		demo-sentinellogging-dce	Data collection endpoint
<input checked="" type="checkbox"/>		demo-sentinellogging-dcr	Data collection rule
<input type="checkbox"/>		demo-sentinellogging-func	Function App
<input type="checkbox"/>		demo-sentinellogging-func	Application Insights
<input type="checkbox"/>		demo-sentinellogging-log	Log Analytics workspace
<input type="checkbox"/>		demo-sentinelloggingst	Storage account

- DCE: Logs Ingestion URL
- DCR: Immutable ID
- DCR: Data Source (table name)

DEMO

Let's look at some sample code!

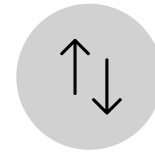
KQL Query Basics



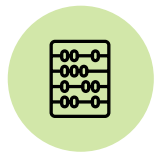
Querying



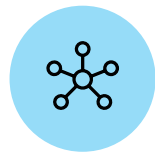
Filtering



Sorting



Aggregation



Summarization

KQL Query Basics

```
1 AppSecurityEvents_CL
2 | project TimeGenerated, event, level
```

Results | Chart | Add bookmark

<input type="checkbox"/> TimeGenerated [UTC] ↑↓	event	level
<input type="checkbox"/> > 5/6/2025, 1:30:53.163 PM	sequence_fail:00000000-0000-0000-0000-000000000000	Critical
<input type="checkbox"/> > 5/6/2025, 1:30:53.100 PM	privilege_permissions_changed:00000000-0000-0000-0000-000000000000	Warning
<input type="checkbox"/> > 5/6/2025, 1:30:53.059 PM	malicious_direct_reference:00000000-0000-0000-0000-000000000000	Critical
<input type="checkbox"/> > 5/6/2025, 1:30:52.951 PM	malicious_cors:00000000-0000-0000-0000-000000000000,illegal.origin.com	Critical
<input type="checkbox"/> > 5/6/2025, 1:30:52.901 PM	malicious_attack_tool:00000000-0000-0000-0000-000000000000,Nikto	Critical
<input type="checkbox"/> > 5/6/2025, 1:30:52.781 PM	malicious_extraneous:00000000-0000-0000-0000-000000000000,creditcardnum	Critical
<input type="checkbox"/> > 5/6/2025, 1:30:52.657 PM	malicious_excess_404:00000000-0000-0000-0000-000000000000	Warning
<input type="checkbox"/> > 5/6/2025, 1:30:52.607 PM	input_validation_fail:00000000-0000-0000-0000-000000000000,date_of_birth	Warning
<input type="checkbox"/> > 5/6/2025, 1:30:52.563 PM	upload_delete:00000000-0000-0000-0000-000000000000,1234567890	Information
<input type="checkbox"/> ∨ 5/6/2025, 1:30:52.509 PM	upload_validation:file.png,virusscan,FAILED	Critical
TimeGenerated [UTC]	2025-05-06T13:30:52.5090415Z	
event	upload_validation:file.png,virusscan,FAILED	
level	Critical	

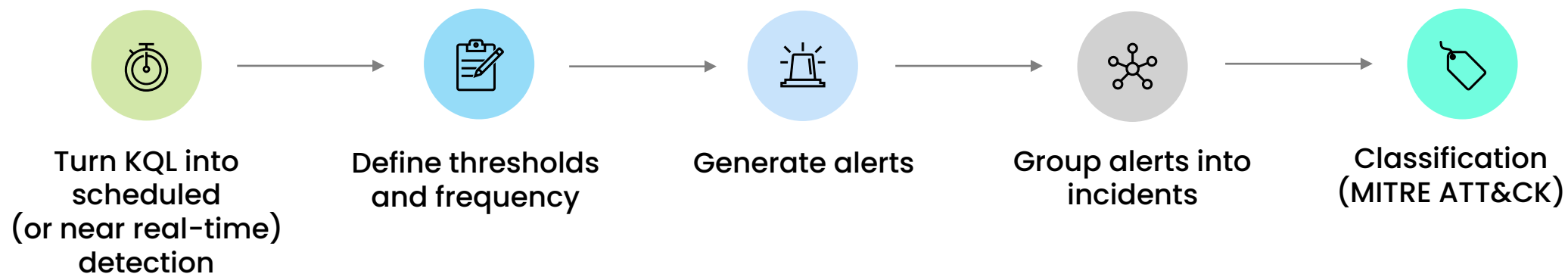
KQL to Detect Impossible Travel

```
AppSecurityEvents_CL
| where event startswith "AUTHN_login_success"
| extend user_id = tostring(split(event, ":")[1])
| summarize
    login_count = count(),
    countries = dcount(geo),
    regions = make_set(region),
    hosts = make_set(host_ip)
    by user_id, bin(timestamp, 1h)
| where login_count >= 2 and countries > 1
```

KQL with Threat Intelligence Integration

```
AppSecurityEvents_CL
| where timestamp > ago(1d)
| where isnotempty(source_ip)
| extend source_ip_str = tostring(source_ip)
| join kind=inner (
    ThreatIntelligenceIndicator
    | where TimeGenerated > ago(1d)
    | where isnotempty(NetworkIP)
    | extend ti_ip = tostring(NetworkIP)
)
on $left.source_ip_str == $right.ti_ip
| project
    timestamp,
    source_ip,
    event,
    description,
    ThreatType,
    ConfidenceScore,
    Description
```



Detecting and alerting on events



Creating an analytics rule

AppSec - VIRUS DETECTED

Medium
Severity

 Custom
Content Source

 Enabled
Status

Info Insights

ID

dd812b4f-ff81-4193-a175-15c98ce69539



Description

--

MITRE ATT&CK

✓  Resource Development (2)

✓ T1608 - Stage Capabilities (1)

T1608.001 - Upload Malware

Rule query

```
AppSecurityEvents_CL  
| where event contains "virusscan,FAILED"
```

Rule frequency

Run query every **5 hours**

Rule period

Last **5 hours** data

Rule threshold

Trigger alert if query returns **more than 0** results


Event grouping

Group all events into a single alert


Suppression

Not configured

Create incidents from this rule

 Enabled

Alert grouping

 Disabled

Managing Incidents

AppSec - VIRUS DETECTED
Incident number 33

[Refresh](#)
[Logs](#)
[Tasks](#)
[Activity log](#)

This is the new, improved incident page - Now generally available. You can use the toggle to switch back.

Medium
Severity

New
Status

Unassigned
Owner

[Investigate in Microsoft Defender XDR](#)

Workspace name
loganalytics

Description
--

Alert product names

- Microsoft Sentinel

Evidence

10
Events

1
Alerts

0
Bookmarks

Last update time
6/5/2025, 15:37:43

Creation time
6/5/2025, 15:37:42

Entities (0)
-

Tactics and techniques
-

Incident workbook
[Incident Overview](#)

Analytics rule
[AppSec - VIRUS DETECTED](#)

Incident Team
-

Tags

+

Incident link
https://portal.azure.com/#asset/Microsoft_Azure_Security_Insight...

Last comment

(Total: 0)

Write a comment...

➤

Overview

Entities

Incident timeline

Search

Add filter

May 6
12:02:04

AppSec - VIRUS DETECTED

Med... Detected by Microsoft... Tacti...

Entities

AppSec - VIRUS DETECTED

Description

Severity
 Medium

Events
[Link to LA](#)

Entities (0)
-

Tactics and techniques

>

Resource Development (1)

System alert ID
e3cfad79-77d2-8584-74a0-e...

Rule name
[AppSec - VIRUS DETECTED](#)

Last update time
5/6/2025, 03:37 PM

Updates
0

Start time
5/6/2025, 12:02 PM

End time
5/6/2025, 03:30 PM

Alert link
-

Remediation steps
-

Similar incidents

Severity	Incident number	Title	Last update time	Status	Similarity
Medium	31	AppSec - VIRUS DETECTED	5/6/2025, 12:20 PM	New	Simi
Medium	30	AppSec - VIRUS DETECTED	5/6/2025, 02:20 AM	New	Simi

Custom Workbooks

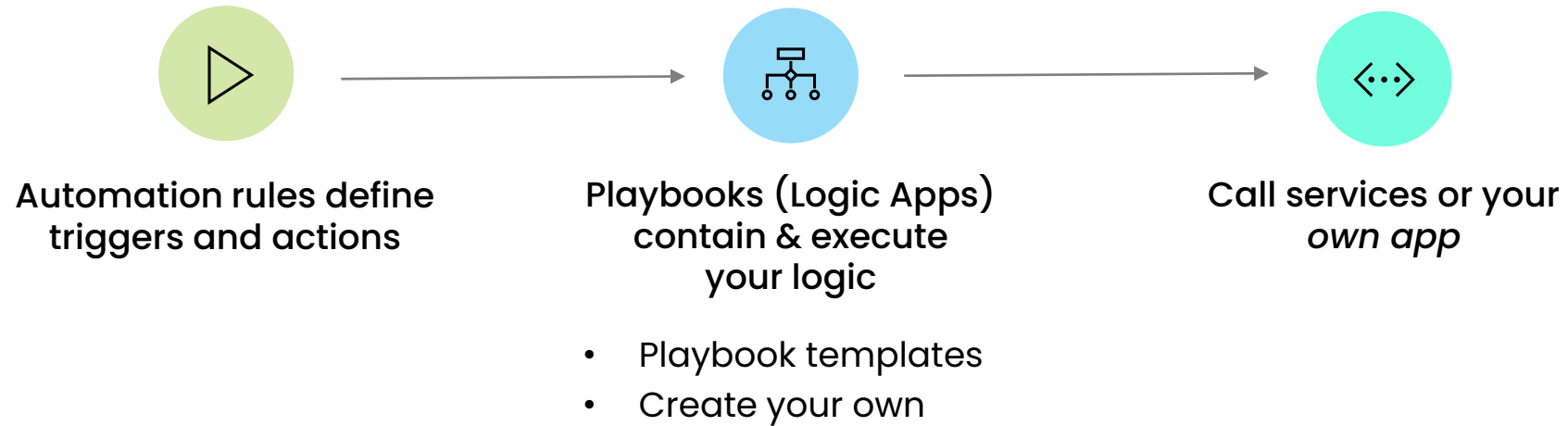
AppSecurityEvents

loganalytics

Edit Open Save Refresh Alerts Pins Groups ? Help Auto refresh: Off

user_updated 16	sys_restart 67	sys_monitor_disabled 38	user_created 24	malicious_excess_404 23	privilege_permissions_c... 23	authn_password_chang... 23	malicious_direct_referen... 23
session_use_after_expire 23	upload_stored:file.png,C... 23	sys_startup 23	authn_login_success 23	sys_crash 23	sys_shutdown 23	authn_password_change 23	session_renewed 23
user_disabled 23	authn_login_fail 23	upload_validation:file.p... 23	sys_monitor_enabled 23	sequence_fail 23	session_expired 23	session_created 23	user_deleted 23
malicious_cors,illegal.ori... 20	authn_impossible_travel... 20	authn_login_fail_max,5 20	authz_admin,user_privil... 20	sensitive_delete,C:\temp... 20	authn_token_delete,api... 20	authz_change,user,admin 20	sensitive_update,C:\tem... 20
authn_token_created,ap... 20	upload_delete,1234567... 20	authn_login_successafte... 20	authn_login_lock,maxret... 20	authn_token_revoked,a... 20	malicious_extraneous,cr... 20	authn_token_reuse,api.a... 20	input_validation_fail,d... 20
malicious_attack_tool,Ni... 20	upload_complete,file.pn... 20	sensitive_create,C:\temp... 20	sensitive_read,C:\temp\... 20	authz_fail,file.docx 20	excess_rate_limit_excee... 20	excess_rate_limit_excee... 3	authn_token_delete:api... 3

Automating a response



Automation Rules

Automation rule name *

AlertTheTeam

Trigger

When incident is created

Conditions

If

Analytic rule name


Contains

AppSec - VIRUS DETECTED

+ Add

Actions ⓘ

Run playbook

 AlertTheTeam
thomasvochten.com / monitoring

+ Add action

Rule expiration ⓘ

Indefinite



Time

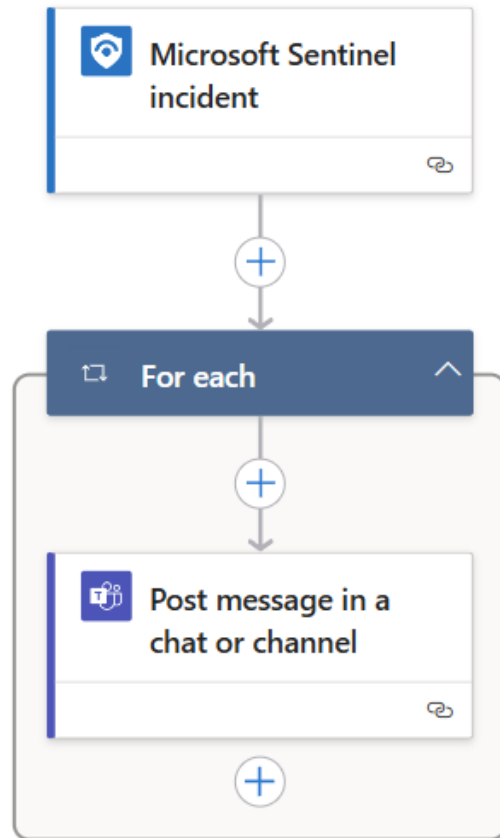
Order ⓘ

1

Status

 Enabled

Playbook Example: Posting in Teams



Thomas Vochten via Workflows 19:59 New

🔔 Sentinel incident created

AppSec - VIRUS DETECTED
[view incident details](#)

🗨️

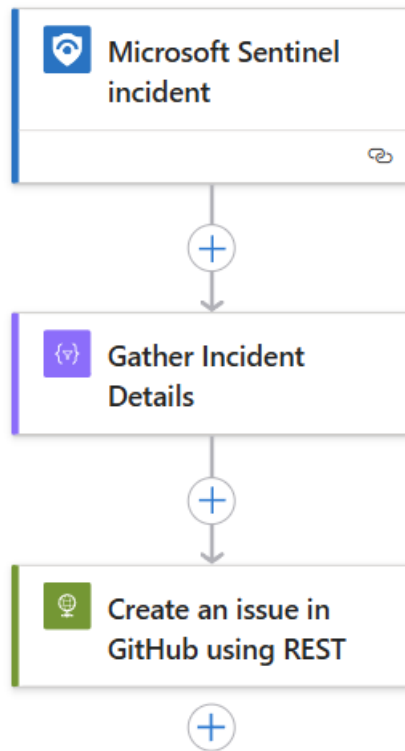
👤 Reply

AppSec - VIRUS DETECTED

🔔 Something might be a bit fishy... Better check it out ASAP!

[I'll take this one](#) [Nope, not me](#) [View](#)

Playbook Example: Creating a GitHub Issue



Sentinel Security Incident #6

Open



thomasvochten opened now

Security Incident Detected

Timestamp: 2025-05-07T09:37:52.69Z

Severity: Medium

Error: AppSec - VIRUS DETECTED

Details:

No details available.

Entities:

This issue was automatically generated by Microsoft Sentinel.

Create sub-issue



thomasvochten added

runtime-attack

security-log

autogenerated

now

Possibilities are endless

- Enrich IPs with Threat Intelligence
- Enrich incidents with geolocation or tags
- Send adaptive cards to Teams for interactivity
- Auto-close low-risk incidents
- Add a comment & assign to a specific developer
- Block IP or domain in your (web application) firewall
- Switch a feature flag based on certain abuse
- Generate a summary PDF and save to SharePoint
- Tag the application version that was live during the attack
- Annotate code in GitHub
- ...

```
import java.util.ArrayList;
import java.util.Scanner;
import java.io.File;
import java.io.IOException;
import java.util.Arrays;

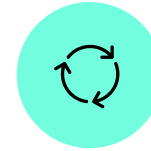
public class AirlineProblem {

    public static void main(String[] args) {
        Scanner scannerToHeadAirlines = null;
        try {
            scannerToHeadAirlines = new Scanner(new File("airlines.txt"));
        } catch (IOException e) {
            System.out.println("could not connect to file airlines.txt.");
            System.exit(0);
        }
        if (scannerToHeadAirlines != null) {
            ArrayList<Airline> airlinesPartnersNetwork = new ArrayList<Airline>();
            Airline newAirline;
            String lineFromFile;
            String[] airlineNames;
            while (scannerToHeadAirlines.hasNextLine()) {
                lineFromFile = scannerToHeadAirlines.nextLine();
                airlineNames = lineFromFile.split(",");
                newAirline = new Airline(airlineNames);
                airlinesPartnersNetwork.add(newAirline);
            }
            System.out.println(airlinesPartnersNetwork);
            Scanner keyboard = new Scanner(System.in);
        }
    }
}
```

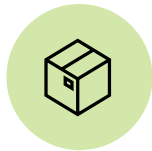
What about the costs?



Balancing insights
versus cost and noise



Managing data
ingestion effectively



Optimizing log
retention policies



Pay-as-you-go vs
commitment tier pricing

Key takeaways



Developers play a vital role in modern security operations

Instrument your app for security-relevant logging

Use Sentinel to detect and respond in near real-time

Integrate the intelligence that Sentinel provides back in your development cycle (SDL)

Start small: log smart, query smarter, automate what matters