

Detecting emerging threats with Fusion - info and TSG

Last updated by | Naser Mohammed | Mar 19, 2023 at 7:18 AM CDT

Please review the PM note made on this link: [PM notes](#) 

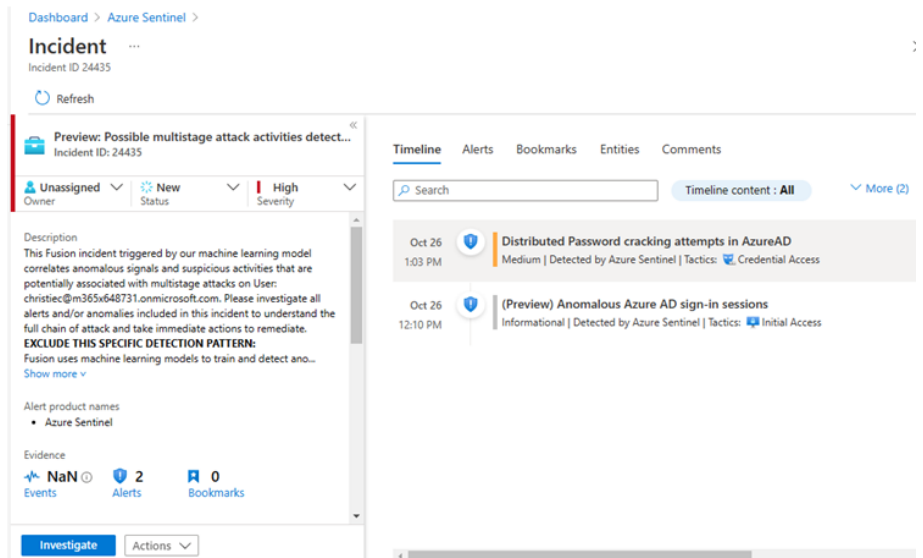
A new set of machine learning algorithms that detect emerging threat patterns automatically to stop attacks at an early stage.

Extended source signal coverage for all the assets monitored by the SOC team in an Azure Sentinel workspace by supporting custom scheduled rules, out-of-the box anomalies, and additional Microsoft products.

A new configuration UI that allows security analysts to configure source signals and to exclude specific detection patterns that may not be applicable to your environment from Fusion detection to further reduce alert fatigue.

Fusion for emerging threats

- Fusion for emerging threats detection will show up in the **incident** blade
- Incident title **“Possible multistage attack activities detected by Fusion”**
- Correlates **two or more** anomalous signals



Supported data sources

- [Out-of-the-box anomalies](#) **NEW**
- Alerts from Microsoft products
 - Azure Active Directory Identity Protection
 - Azure Defender
 - Azure Defender for IoT **NEW**
 - Microsoft 365 Defender **NEW**
 - Microsoft Cloud App Security
 - Microsoft Defender for Endpoint
 - Microsoft Defender for Identity **NEW**
 - Microsoft Defender for Office 365 **NEW**
- Alerts from scheduled analytics rules, both the [out-of-the-box rules](#) and the rules [created by your security analysts](#). Kill-chain (tactics) information and entity mapping information is required for the analytics rules to be leveraged by Fusion. **NEW**

Configuration UI

Analytics rule wizard - Edit existing Fusion rule

Advanced Multistage Attack Detection

General **Configure Fusion** Automated response Review and update

Fusion uses machine learning to automatically detect multistage attacks, by identifying combinations of anomalous behaviors and suspicious activities at various stages of the kill chain.

Configure source signals for Fusion detection

By design, Fusion incidents are low-volume, high-fidelity, and high-severity. We recommend that you include all the listed source signals, with all severity levels, for the best result. Excluding a particular source signal or an alert severity level means any Fusion detections that rely on signals from that source, or on alerts matching that severity level, will not be triggered. [Learn more](#)

Sources	Status	Severity
Anomalies	<input checked="" type="checkbox"/> Included	
Alert providers	<input checked="" type="checkbox"/> Included	
Azure Active Directory Identity Protection	<input checked="" type="checkbox"/> Included	4 selected
Azure Defender	<input checked="" type="checkbox"/> Included	4 selected
Azure Defender for IoT	<input checked="" type="checkbox"/> Included	4 selected
Microsoft 365 Defender	<input checked="" type="checkbox"/> Included	4 selected
Microsoft Cloud App Security	<input checked="" type="checkbox"/> Included	4 selected
Microsoft Defender for Endpoint	<input checked="" type="checkbox"/> Included	4 selected
Microsoft Defender for Identity	<input checked="" type="checkbox"/> Included	4 selected
Microsoft Defender for Office 365	<input checked="" type="checkbox"/> Included	4 selected
Azure Sentinel scheduled analytics rules	<input checked="" type="checkbox"/> Included	4 selected
Raw logs from other sources	<input checked="" type="checkbox"/> Included	
Palo Alto Network	<input checked="" type="checkbox"/> Included	Select all <input checked="" type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input checked="" type="checkbox"/> Low <input checked="" type="checkbox"/> Informational

Exclude specific detection patterns from Fusion detection

The following detection patterns are currently excluded from Fusion. Excluding a detection pattern means any Fusion detections matching the combination of anomalous signals (e.g. alerts and anomalies) in the pattern will not show up in your active incident queue. Incidents that match the excluded detection pattern will still be generated, but with a "closed" status. To exclude a detection pattern, follow the exclusion link in the description of the relevant Fusion incident. [Learn more](#)

Exclusion pattern	Time added (dd/mm/yy)	Remove
Alert providers:Azure Defender:Connection to web page from anomalous IP address detected:Alert providers:Azure Defender:Crypto-mining activity:Alert provider...	10/20/21, 03:28 PM	
Alert providers:Azure Defender:Network intrusion detection signature activation [seen multiple times]:Alert providers:Microsoft Defender for Endpoint:Malicious U...	10/20/21, 03:24 PM	

- All the source signals and severity levels are **included** by default.
- Excluding a particular source signal or an alert severity level means any Fusion detections that rely on signals from that source, or on alerts matching that severity level, will not be triggered.

- Excluding a detection pattern means any Fusion detections matching the combination of anomalous signals (e.g. alerts and anomalies) in the pattern will not show up in your active incident queue. Incidents that match the excluded detection pattern will still be generated, but with a "closed" status.
- To exclude a detection pattern, follow the exclusion link in the description of the relevant Fusion incident.

Know limitations

- For source signal configuration, the list shown reflects all the sources signals supported by Fusion but not the actual data connector status. This UI only controls whether the source signals are included or excluded for Fusion.
- API documentation for UI will not release during Ignite. The Sentinel API swagger will likely go out in November.
- Customers won't be able to save the rule if there are duplicated exclusion pattern. Manual removal of the duplicated exclusion pattern is need.
 - *Error message: Failed to save analytics rule. One or more alert validation have failed. [Scenario exclusion pattern has duplicates]*



Investigating Incidents


Fusion Incidents will be named "Preview: Possible multistage attack activities detected by Fusion" which correlated multiple anomalies into an incident based on a joined entity.

1. In the Fusion incident, anomalies were promoted into alerts so customers can always go to the Anomalies table to find additional information. After clicking on the SystemAlertID in the alert, the customer can see it's an anomaly (Alert Type = Anomaly) and can view more details in the anomaly table using the OriginalSystemAlertId.

```

1 SecurityAlert
2 | summarize arg_max(TimeGenerated, *) by SystemAlertId
3 | where SystemAlertId in("b8f6f65d-")

```

Results | Chart |  Add bookmark

<input type="checkbox"/> SystemAlertId	TimeGenerated [UTC]	DisplayName
VendorName	Microsoft	
VendorOriginalId	b8f6f65d-	
AlertType	Anomaly	
IsIncident	false	
StartTime [UTC]	2022-08-08T11:20:30.058Z	
EndTime [UTC]	2022-08-08T11:58:00Z	
ProcessingEndTime [UTC]	2022-08-08T20:24:49.55Z	
ExtendedProperties	{ "TenantId": "", "RuleId": "" }	
Alert generation status	Full alert created	
FusionSyntheticAlert	true	
IpAddress	170.99.8.133	
OriginalSystemAlertId	df1b57a5-	

Anomalies | where Id contains "OriginalSystemAlertId"

Delay on Fusion Incidents

See [This ICM 315378181](#) for more information, or case 2209120010001710.

According to the ICM above, the delay between the first alerts and the Incident is normally seen between 0-2 days. But, it can be up to 7 days the max delay.

The following is an explanation given by Sylvie Liu, PM of Fusion, that assisted on the case shown above. The alerts came on 8/31 and the incident was seen until 4 days later on 9/4. 2 alerts were shown per incident only:

Fusion works by giving the events/alerts a score. When the score reaches a certain value, the Incident will be created and posted. When the alerts were triggered, the scoring was not high enough to raise them in an incident. Later on, additional alerts influenced the Fusion scoring for the incident, which raised the score to meet the bar for publishing. Yet, you may ask why there are only 2 alerts shown per incident. Currently Fusion surfaces the mostly relevant alerts in an incident to keep the alert fatigue low. The new alerts added to the full graph might impacted the scoring but may not be considered as the most relevant alerts to show in the incident.

The PM added that they are exploring an option to show all the alerts (more alerts to investigate) vs. only the most relevant alerts.