

Mimecast SIEM Integration with Microsoft Azure Sentinel



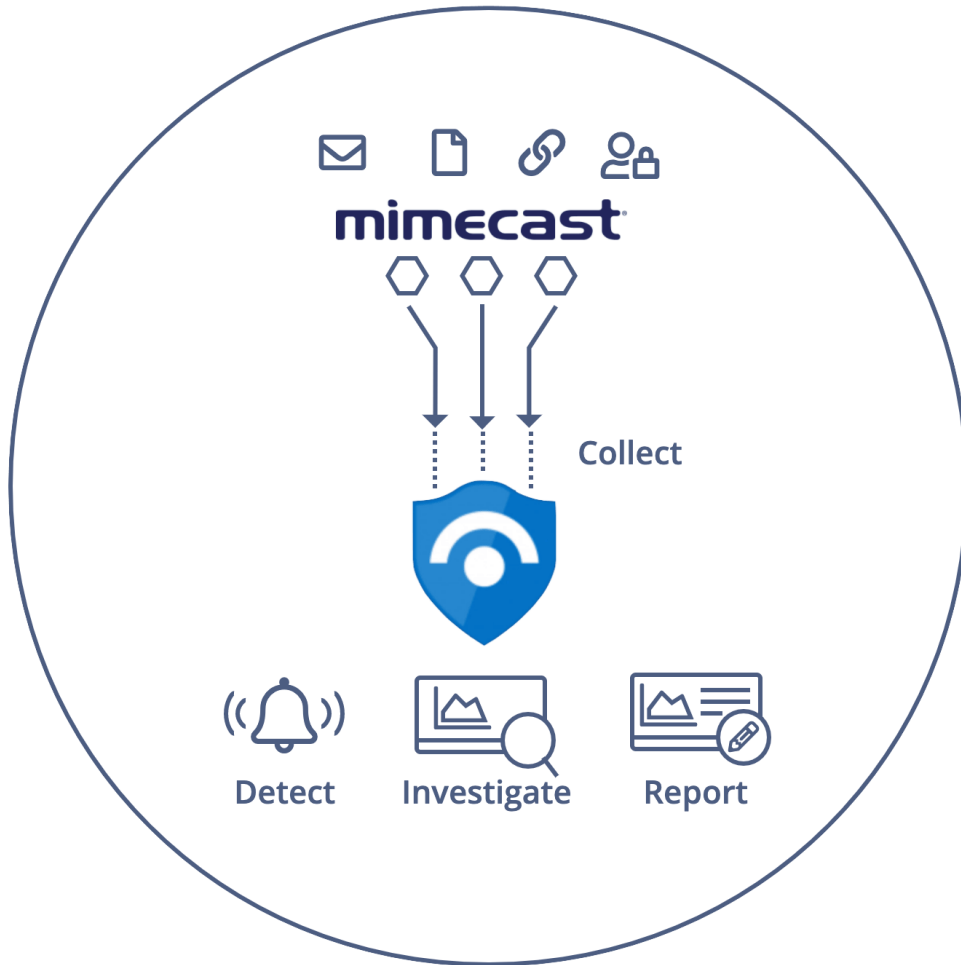
Identify Incidents & Respond Faster

Make your threat detection smarter and improve response times by fully integrating Mimecast's Threat Intelligence, Secure Email Gateway, Targeted Threat Protection, and Authentication / Audit logs into Microsoft Azure Sentinel.

- Utilize Sentinel's Log Analytics workspace to create custom queries for Mimecast's email security data
- Visualizations and tables showcasing the data available are provided as a Sentinel Workbook
- Enhance further with other technology solutions with an Open API

Key Benefits:

- A fully integrated threat environment with enhanced visibility of email born attacks
- Provides the ability to prioritize events and automate workflows and response, allowing a security analyst to address the most critical threats detected
- Decrease MTTR (Mean Time To Respond)
- Create custom reports and log analysis using Sentinel Workbooks



Key capabilities

Utilize Sentinel's Log Analytics workspace to create custom queries for Mimecast's email security data

View results quickly in a table or visualize as a chart

Export results to share with colleagues or create dashboards and alerts on the fly

Use the Mimecast Workbook to see what data is available

The screenshot shows the Microsoft Azure portal interface for Azure Sentinel Logs. The selected workspace is 'Mimecast-Azure-Sentinel-1'. A custom query is being executed, with the following KQL code:

```
Mimecast_mail_CL |  
extend mcast_json = parse_json(substring(RawData, 20)) |  
extend Category = mcast_json.category |  
extend URL = mcast_json.url |  
extend Result = mcast_json.scanResult |  
extend User = mcast_json.userEmailAddress |  
where RawData has "ttp_url" and Result has "malicious" |  
summarize count() by bin(TimeGenerated, 1d) |  
sort by TimeGenerated asc
```

The results are displayed as a line chart. The chart shows a peak in activity around the middle of the time range, with a count of approximately 750. The Y-axis is labeled 'count' and ranges from 500 to 800. The X-axis is labeled 'TimeGenerated' and shows a range of dates. The chart is titled 'Completed. Showing results from the custom time range.'

Key capabilities

Utilize Sentinel's Log Analytics workspace to create custom queries for Mimecast's email security data

View results quickly in a table or simply visualize as a chart

Export results to share with colleagues or create dashboards and alerts on the fly

Use the Mimecast Workbook to see what data is available

The screenshot displays the Azure Sentinel Log Analytics interface. At the top, a Kusto query is shown: `extend Result = mcast_json.scanResult | extend User = mcast_json.userEmailAddress | where RawData has "ttp_url" and Result has "malicious"`. Below the query, the interface shows a table of results. The table has columns for TimeGenerated [UTC], Category, URL, Result, User, Computer, and RawData. The results are filtered to show malicious activity from March 31, 2020. The table includes 13 rows of data, with categories such as Malware, Phishing & Fraud, and Business. The interface also shows a status bar indicating 'Completed. Showing results from the custom time range.' and a total of 6,586 records.

TimeGenerated [UTC]	Category	URL	Result	User	Computer	RawData
3/31/2020, 7:54:11.000 PM	Malware	http://terrasnaya-doska.com/DocuSign/docusingn/	malicious	emoreno@twotoeight.com	azure-sentinel-agent	2020-03-31 19:54:11.000 PM
3/31/2020, 8:41:57.000 PM	Malware	http://jstqlobalpartners.com/hotoffice/cmd-login=4078f0e0de091e35...	malicious	pparker@twotoeight.com	azure-sentinel-agent	2020-03-31 20:41:57.000 PM
3/31/2020, 8:41:49.000 PM	Malware	http://jstqlobalpartners.com/hotoffice/cmd-login=4078f0e0de091e35...	malicious	pparker@twotoeight.com	azure-sentinel-agent	2020-03-31 20:41:49.000 PM
3/31/2020, 2:38:46.000 PM	Malware	http://jstqlobalpartners.com/hotoffice/cmd-login=4078f0e0de091e35...	malicious	pparker@twotoeight.com	azure-sentinel-agent	2020-03-31 14:38:46.000 PM
3/31/2020, 3:42:16.000 PM	Malware	http://gestionok.c/wp-admin/network/office/uodate/file/data/o/f/f/c/...	malicious	aorchard@twotoeight.com	azure-sentinel-agent	2020-03-31 15:42:16.000 PM
3/31/2020, 3:47:19.000 PM	Phishing & Fraud	http://mimecast.com/	malicious	nfrederiksen@twotoeight.com	azure-sentinel-agent	2020-03-31 15:47:19.000 PM
3/31/2020, 12:08:24.000 PM	Phishing & Fraud	http://mimecast.com/	malicious	aterblanche@twotoeight.com	azure-sentinel-agent	2020-03-31 12:08:24.000 PM
3/31/2020, 12:08:24.000 PM	Phishing & Fraud	http://mimecast.com/	malicious	nfrederiksen@twotoeight.com	azure-sentinel-agent	2020-03-31 12:08:24.000 PM
3/31/2020, 11:57:27.000 AM	Phishing & Fraud	http://mimecast.com/	malicious	aterblanche@twotoeight.com	azure-sentinel-agent	2020-03-31 11:57:27.000 AM
3/31/2020, 11:57:27.000 AM	Phishing & Fraud	http://mimecast.com/	malicious	nfrederiksen@twotoeight.com	azure-sentinel-agent	2020-03-31 11:57:27.000 AM
3/31/2020, 11:38:47.000 AM	Business	https://livelink.din.de/livelink/livelink.exe?func=ll&objId=70981578obj...	malicious	shofman@twotoeight.com	azure-sentinel-agent	2020-03-31 11:38:47.000 AM
3/31/2020, 8:27:37.000 AM	Phishing & Fraud	http://mimecast.com/	malicious	nfrederiksen@twotoeight.com	azure-sentinel-agent	2020-03-31 08:27:37.000 AM
3/31/2020, 7:08:31.000 AM	Phishing & Fraud	http://mimecast.com/	malicious	aterblanche@twotoeight.com	azure-sentinel-agent	2020-03-31 07:08:31.000 AM
3/31/2020, 7:08:31.000 AM	Phishing & Fraud	http://mimecast.com/	malicious	nfrederiksen@twotoeight.com	azure-sentinel-agent	2020-03-31 07:08:31.000 AM
3/31/2020, 7:04:07.000 AM	Phishing & Fraud	http://www.mimecast.com	malicious	nfrederiksen@twotoeight.com	azure-sentinel-agent	2020-03-31 07:04:07.000 AM
3/31/2020, 6:53:07.000 AM	Phishing & Fraud	http://www.mimecast.com	malicious	nfrederiksen@mimcast.com	azure-sentinel-agent	2020-03-31 06:53:07.000 AM
3/31/2020, 6:50:28.000 AM	Phishing & Fraud	http://www.mimecast.com	malicious	aterblanche@twotoeight.com	azure-sentinel-agent	2020-03-31 06:50:28.000 AM
3/31/2020, 2:42:47.000 PM	Phishing & Fraud	http://mimecast.com/	malicious	aterblanche@twotoeight.com	azure-sentinel-agent	2020-03-31 14:42:47.000 PM

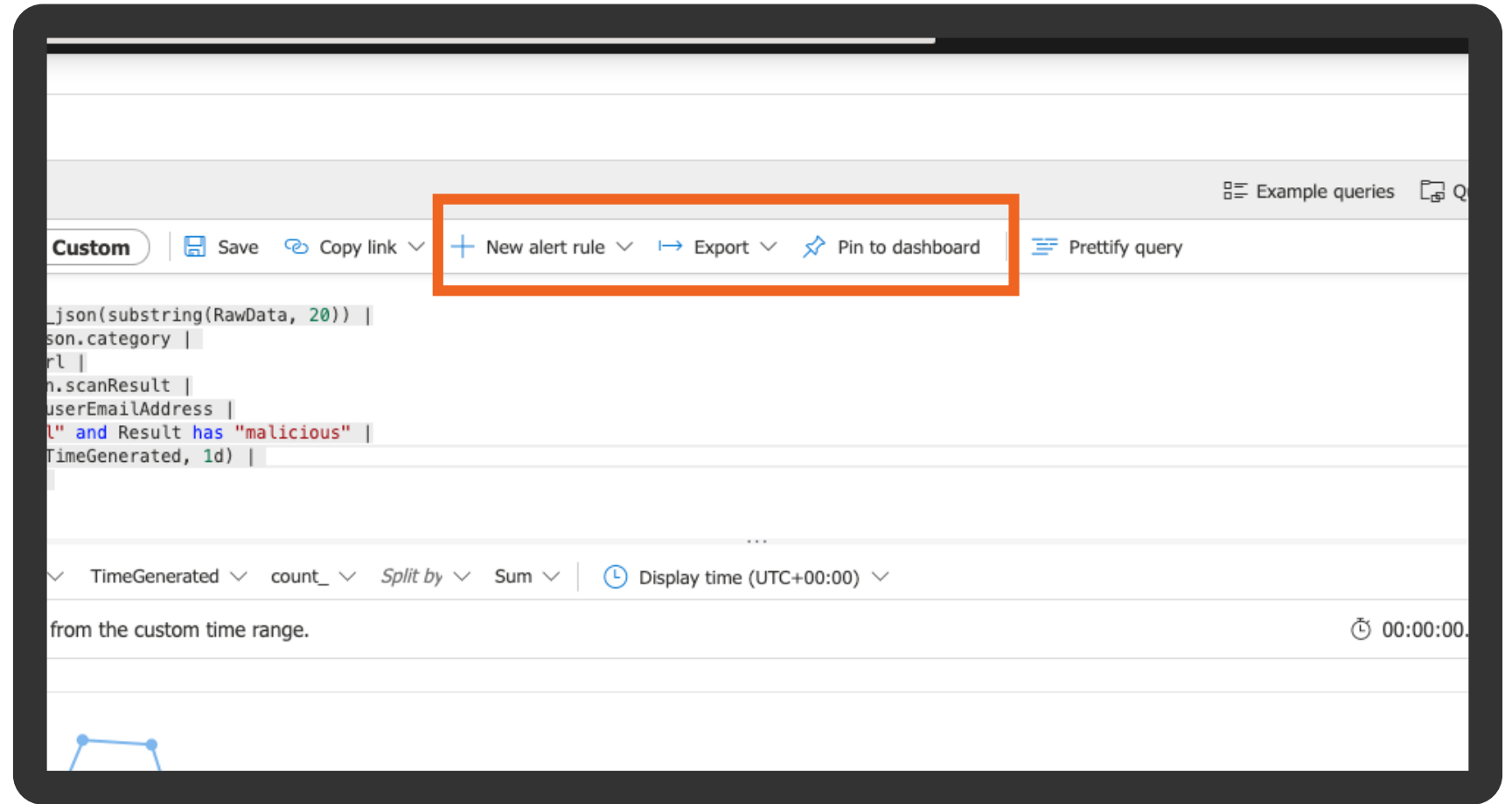
Key capabilities

Utilize Sentinel's Log Analytics workspace to create custom queries for Mimecast's email security data

View results quickly in a table or visualize as a chart

Export results to share with colleagues or create dashboards and alerts on the fly

Use the Mimecast Workbook to see what data is available



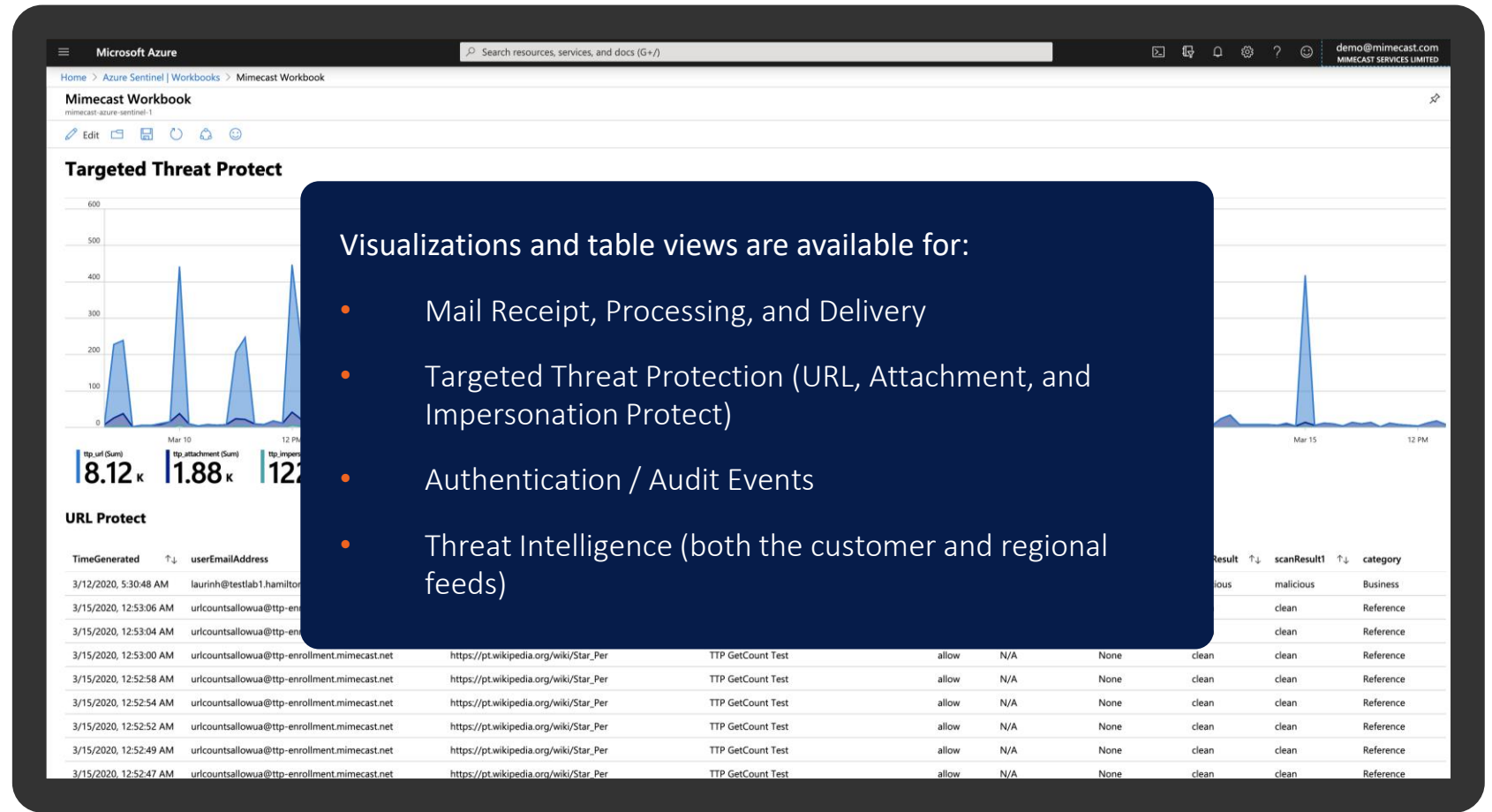
Key capabilities

Utilize Sentinel's Log Analytics workspace to create custom queries for Mimecast's email security data

View results quickly in a table or visualize as a chart

Export results to share with colleagues or create dashboards and alerts on the fly

Use the Mimecast Workbook to see what data is available



mimecast®

