mimecast | Data Sheet

Mimecast for Splunk

The Mimecast for Splunk Enterprise app helps joint customers identify threats more quickly and respond faster.

Protecting against the onslaught of cyber-attacks today is no easy task. There are likely attacks in progress inside most organizations, but seeing what's going on and having the intelligence to do something about it can be a challenge – especially with the vast amount of data generated by numerous business and security systems being used.

Email is the primary attack vector and holds a huge amount of data, that if harnessed in the right way, can help improve security defenses and response significantly. This is where SIEM tools can help, by correlating data from multiple sources, including email systems, to help identify priority threats and reduce investigation and resolution times. Using our open API, Mimecast has developed an integration to bring email security data into the Splunk Enterprise platform.

A single source of truth to help drive better, faster security decisions

Integrating Mimecast data into Splunk means it can be correlated against other data sources for better visibility and alerting to active and potential threats that may otherwise go unnoticed. Integrating email security data into Splunk's Common Information Model (CIM) makes it faster and easier to correlate, monitor, query and extract actionable intelligence from.

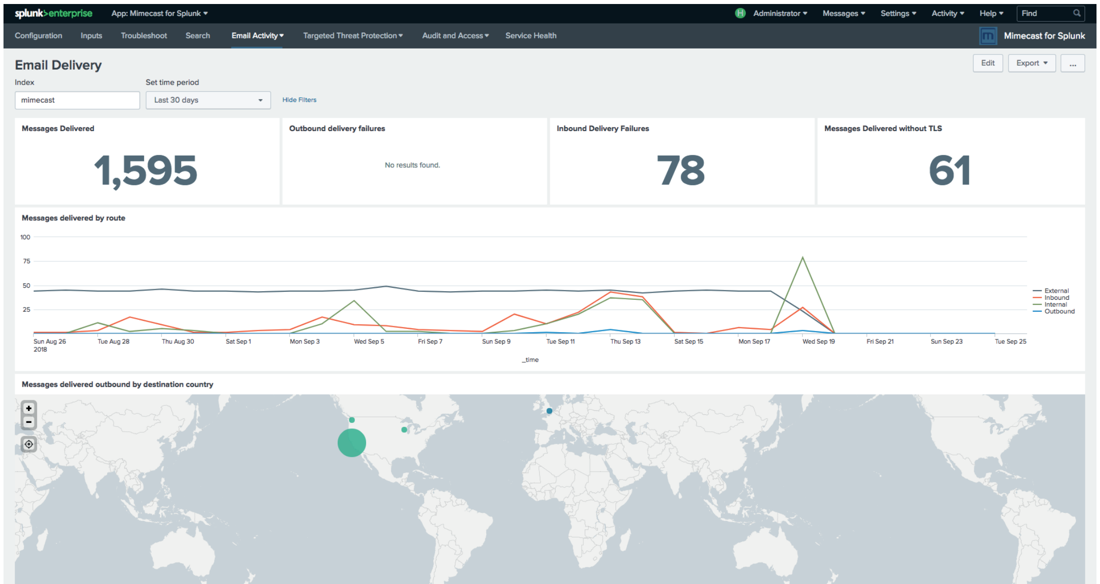
The app supports multiple input sources including email, directory, journal, and audit data for more comprehensive insights. Deeper Targeted Threat Protection URL data is also included for greater visibility into link activity including user clicks and outcomes. Pre-built dashboards help visualize the data for easier interpretation and action.

Find more information at Mimecast.com/developer and download Mimecast for Splunk app on Splunkbase.

Key Highlights:

- Improve visibility and detection of potential and active attacks by adding email security data into Splunk.
- Find high-priority incidents among a sea of data points through anomaly detection and machine learning.
- Rapid time to value with fast install and setup, pre-build dashboards and support for Splunk's Common Information Model (CIM).
- Support for multiple Mimecast data input sources - SIEM, Email, Directory, Journal, Audit and Targeted Threat Protection URL logs.
- Consolidate threat intelligence and response into a single system.
- Improve regulatory compliance.
- Support for the latest versions of Splunk Enterprise.

splunk>



splunk>enterprise App: Mimecast for Splunk ▾ | Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Configuration | Inputs | Troubleshoot | Search | Email Activity ▾ | Targeted Threat Protection ▾ | Audit and Access ▾ | Service Health | Mimecast for Splunk

Email Delivery

Index: mimecast

Set time period: Last 30 days ▾

Hide Filters

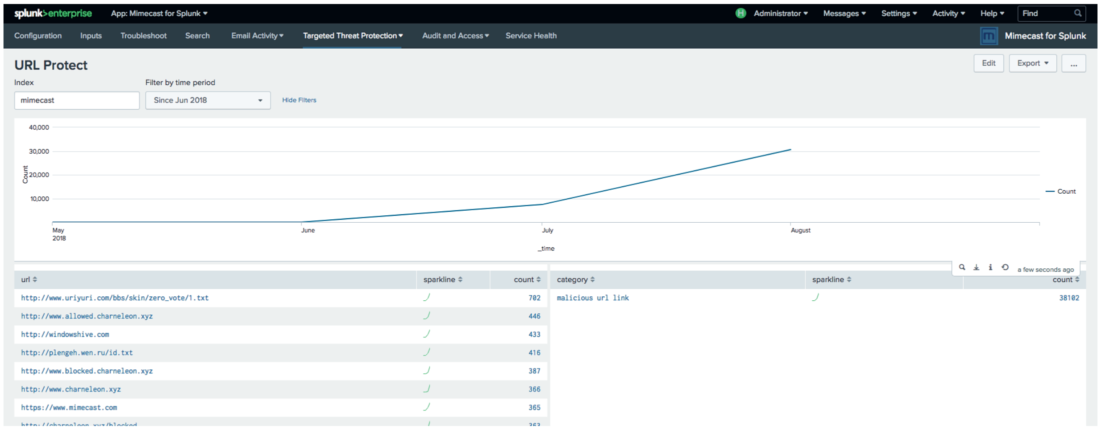
Edit | Export ▾ | ...

Messages Delivered	Outbound delivery failures	Inbound Delivery Failures	Messages Delivered without TLS
1,595	No results found.	78	61

Messages delivered by route

Messages delivered outbound by destination country

Fig 1: Email delivery dashboard



splunk>enterprise App: Mimecast for Splunk ▾ | Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Configuration | Inputs | Troubleshoot | Search | Email Activity ▾ | Targeted Threat Protection ▾ | Audit and Access ▾ | Service Health | Mimecast for Splunk

URL Protect

Index: mimecast

Filter by time period: Since Jun 2018 ▾

Hide Filters

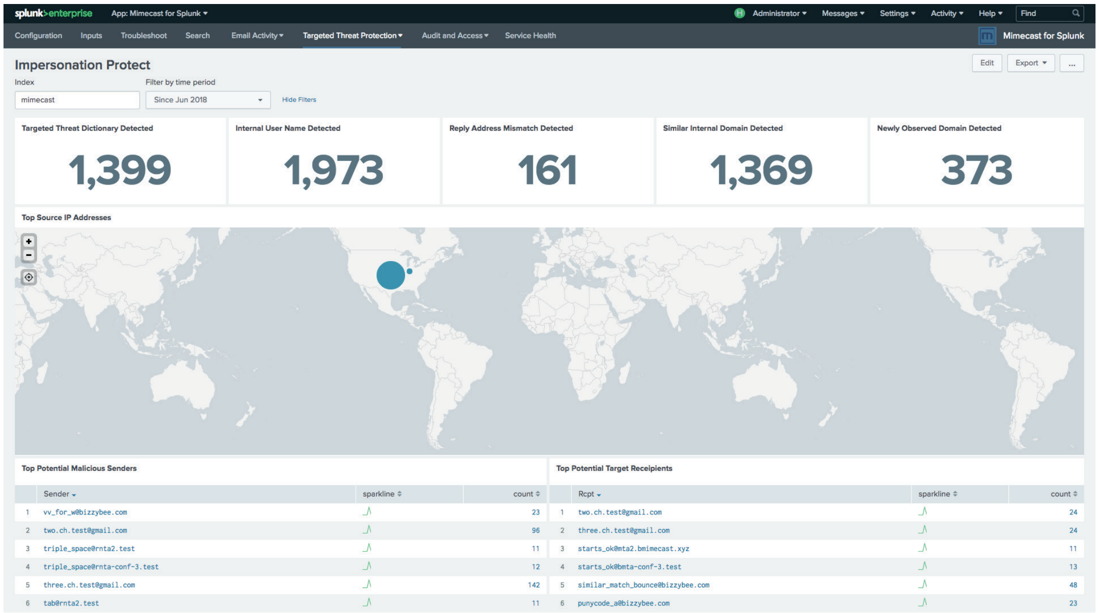
Edit | Export ▾ | ...

a few seconds ago

url ⇕	sparkline ⇕	count ⇕
http://www.uriyuri.com/bbs/skin/zero_vote/1.txt		702
http://www.allowed.charneleon.xyz		446
http://windowshive.com		433
http://plengeh.wen.ru/id.txt		416
http://www.blocked.charneleon.xyz		387
http://www.charneleon.xyz		366
https://www.mimecast.com		365
http://charneleon.xyz/blocked		363

category ⇕	sparkline ⇕	count ⇕
malicious url link		38102

Fig 2: Targeted Threat Protection URL Protect dashboard



splunk>enterprise App: Mimecast for Splunk ▾ | Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Configuration | Inputs | Troubleshoot | Search | Email Activity ▾ | Targeted Threat Protection ▾ | Audit and Access ▾ | Service Health | Mimecast for Splunk

Impersonation Protect

Index: mimecast

Filter by time period: Since Jun 2018 ▾

Hide Filters

Edit | Export ▾ | ...

Targeted Threat Dictionary Detected	Internal User Name Detected	Reply Address Mismatch Detected	Similar Internal Domain Detected	Newly Observed Domain Detected
1,399	1,973	161	1,369	373

Top Source IP Addresses

Top Potential Malicious Senders

	Sender ▾	sparkline ⇕	count ⇕
1	vv_for_w@bizzybee.com		23
2	two.ch.test@gmail.com		96
3	triple_space@rnta2.test		11
4	triple_space@rnta-conf-3.test		12
5	three.ch.test@gmail.com		142
6	tab@rnta2.test		11

Top Potential Target Receipients

	Rcpt ▾	sparkline ⇕	count ⇕
1	two.ch.test@gmail.com		24
2	three.ch.test@gmail.com		24
3	starts_ok@mta2.bmimecast.xyz		11
4	starts_ok@bmta-conf-3.test		13
5	similar_match_bounce@bizzybee.com		48
6	punycode_a@bizzybee.com		23

Fig 3: Targeted Threat Protection Impersonation Protect dashboard