

A background image showing two men in business attire. One man is pointing at a laptop screen while the other looks on. The image is overlaid with a dark blue semi-transparent filter.

mimecast®

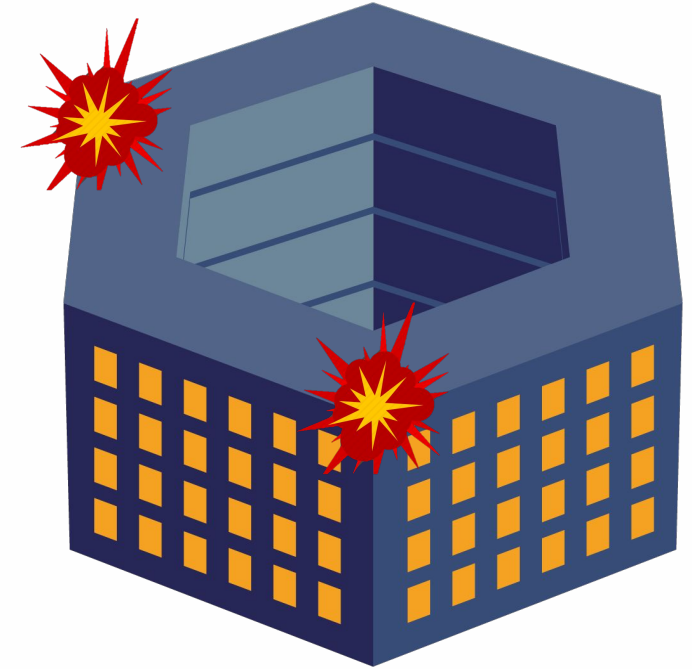
Mimecast for Rapid7

The Front Line of Incident Response

Email is a primary attack vector.

As threats are identified, Security teams' triage and investigate with a vast array of tools. This can rack up time and costs.

You're not realizing the full benefit of a **SOAR** investment without an integrated connection into email.



*94% of Malware delivery leverages email.**

SOAR + Email

Security Orchestration, Automation and Response

Benefits of Integration

Rapidly collects and organize ingested threat intel

Improve response time through automated workflows

Respond faster to contain and limit attack impact



Mimecast's open API integrates with SOAR platforms.

Mimecast for Rapid7 Insight Connect

Gives joint customers a single space to set up automated responses to security threats

mimecast®

Secure Email Gateway

Threat Intelligence

Attachment Logs

Sender Policies

Network Security

Other log, security & machine data – e.g. network, endpoint



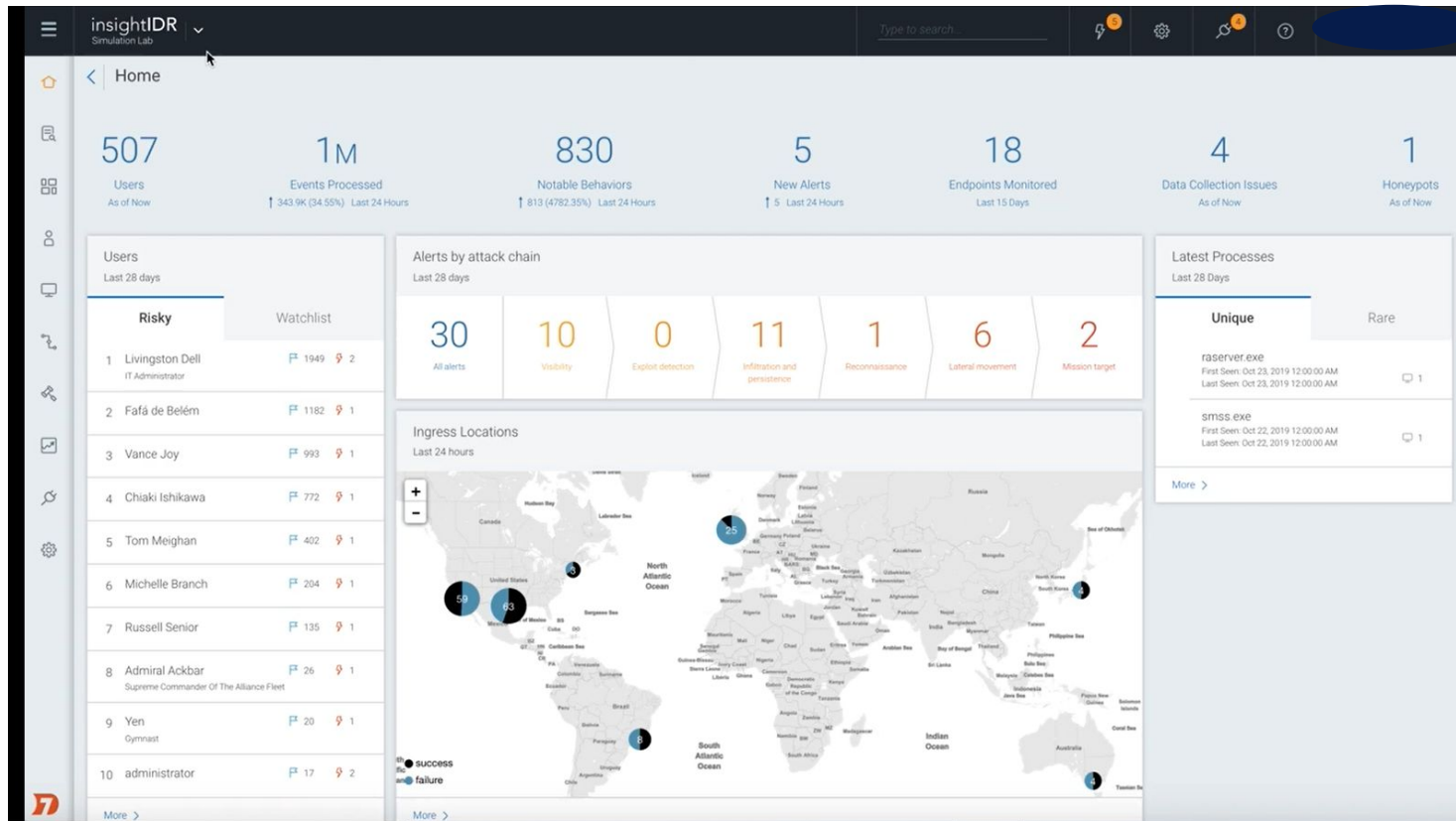
Collect and process data from various sources across the network

RAPID7

Insight Connect

- Ingest rich Mimecast information
- Manage Policies
- Orchestrate via Automated workflows
- 360-degree view of Incidents
- Complete records of investigations

Rapid7 InsightConnect



Mimecast data is mapped directly into Rapid7's SOAR (InsightConnect) to allow security analysts to create custom workflows to address a plethora of attacks in minutes, through Mimecast

mimecast[®]

RAPID7

Use Cases

Use Case: Saving Time

- **Challenge:**

- Attackers targeted multiple users simultaneously across an organization, generating hundreds of alerts resulting in more work for a security analyst.
- Repetitive and time consuming tasks, causing alert fatigue and stripping an analyst's time for actual problem-solving.

- **Solution**

- Implement Rapid7 InsightConnect, integrated with Mimecast to orchestrate and automate a variety of repeatable actions during incident response.
- Integrated Mimecast email security and network data to automatically execute actions such as blocking a malicious sender

- **Benefit**

- Rapid7 and Mimecast can bridge a common customers attacks together for quicker and automated responses.
- Ensures standardized response and updates for the entire SOC.
- Reduced effort and time, allowing Security Analysts to work on more complex threats.

Use Case: Investigation Visibility

- **Challenge:**

- Attack investigations require an analyst to keep all the evidence of an ongoing or completed investigation.
- The analyst must also grab and archive evidence for full documentation once the investigation is complete.
- This results in manually taking down all relevant information such as the sender's address, domain or a URL identified.

- **Solution**

- Debrief your SOC and forward all the relevant information found within the InsightConnect Jobs section

- **Benefit**

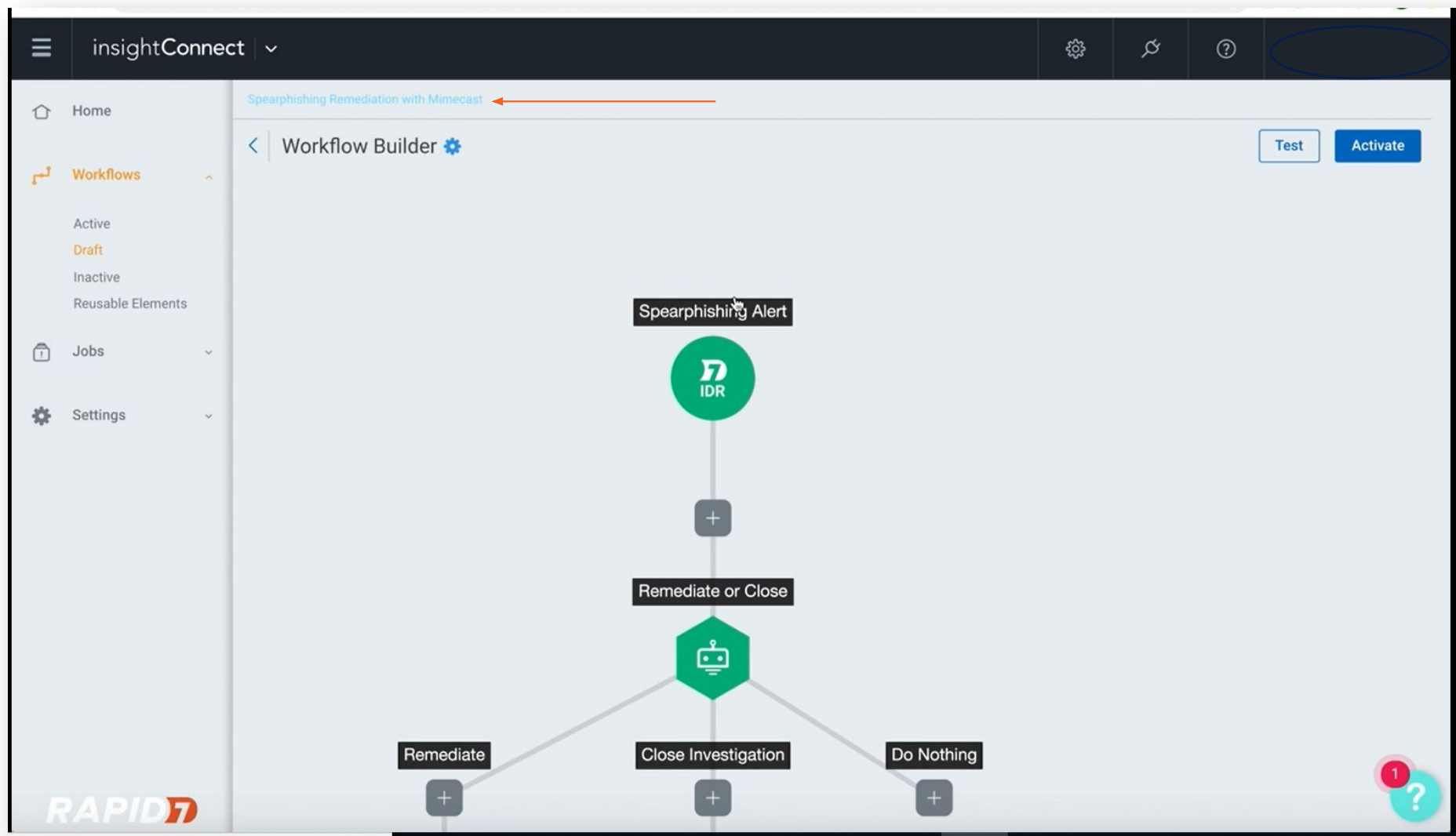
- The Rapid7 Job tab allows analysts to be fully informed on an investigation with complete visibility into an incident
- Prevent the need for collecting information from multiple sources for documentation.

mimecast[®]

RAPID7

Let's Take A Look

Rapid7 – Mimecast Workflow



Block Sender

Prevent email delivery from malicious senders.

Permit Sender

Allow email receipt from trusted senders.

Block Domain

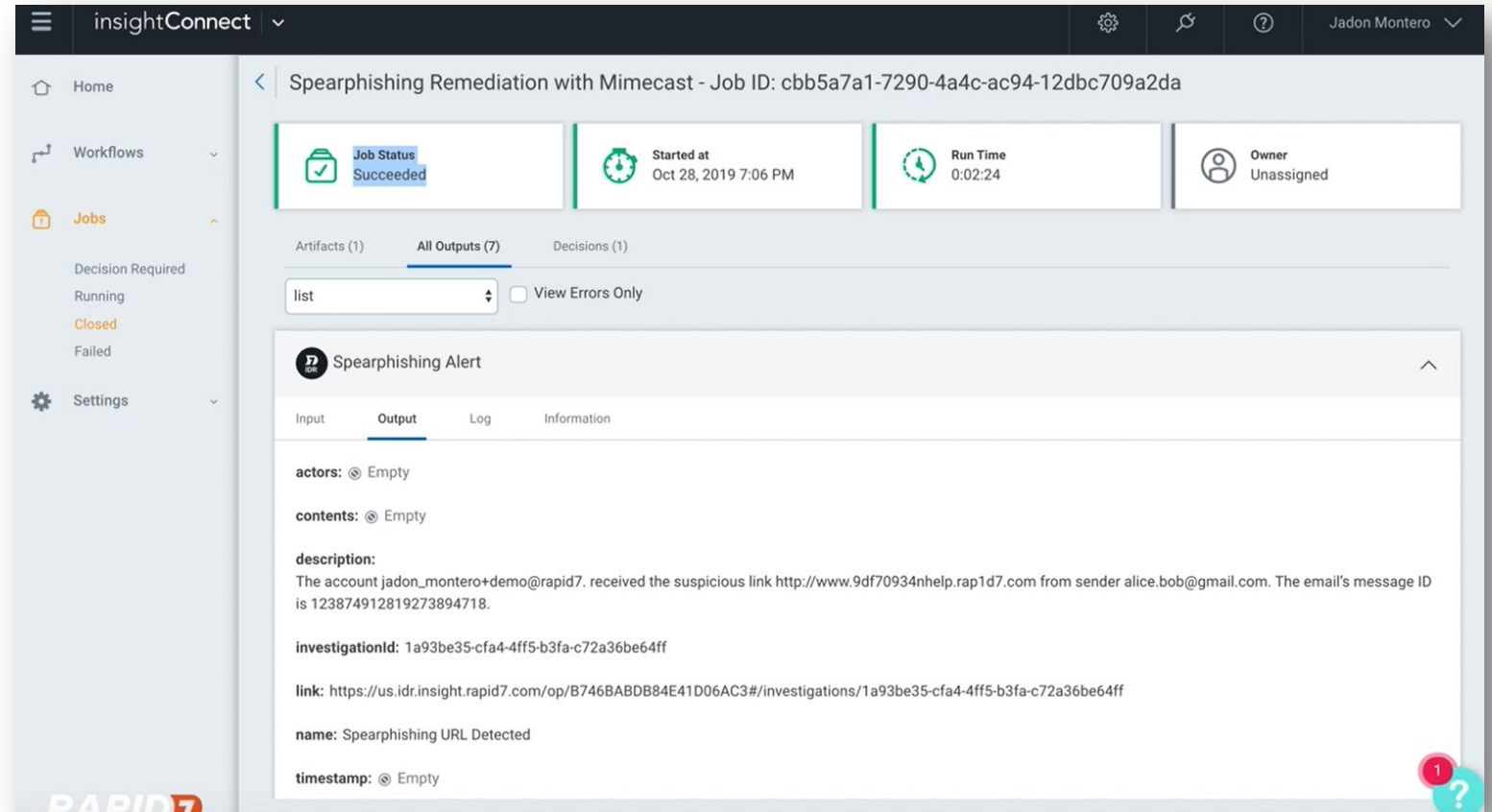
Prevent email delivery from malicious domains.

Permit Domain

Allow email receipt from trusted domains.

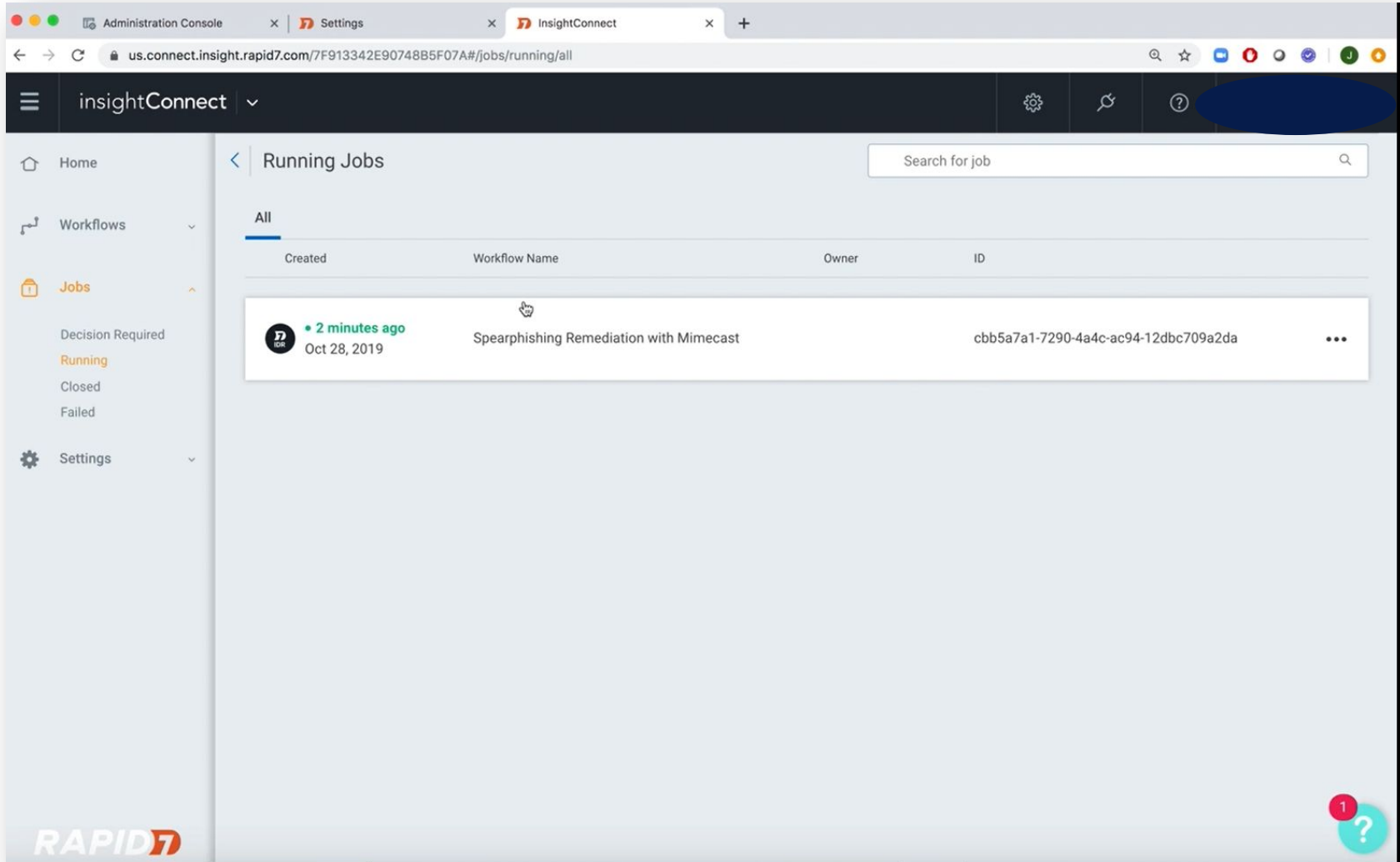
Get Managed URLs

Retrieve a list of all the currently managed URLs in the system.



Successfully remediating against a malicious URL

Running a Job through Rapid7



Completing a Job through Mimecast

The screenshot shows the Mimecast Administration Console interface. The browser address bar indicates the URL is `login-sandbox.mimecast.com/administration/app/#/policies`. The page title is "Policies" and it shows a list of policies. A blue arrow points to the policy for "alice.bob@gmail.com".

Sender	Policy	Action	Created	Owner
[@domain2.com]	Everyone	Block sender	-	Eternal ui test
[@domain2.com]	Everyone	Block sender	-	Eternal ui test
[@domain2.com]	Everyone	Block sender	-	Eternal ui test
[@domain2.com]	Everyone	Block sender	-	Eternal ui test
[@domain.com]	Everyone	Block sender	-	Eternal ui test
[@example.com]	Everyone	Block sender	-	Eternal komand test
[@test.com]	Everyone	Block sender	-	Eternal komand testing
[@test.com]	Everyone	Block sender	-	Eternal komand test
[@test.com]	Everyone	Block sender	-	Eternal komand test
[@test.com]	Everyone	Block sender	-	Eternal komand testing
[@example.com]	Internal	Block sender	-	Eternal Demo
@*.hamilton321.net	Internal	Take no action	-	Eternal Devin Hamilton Test
[@test2.com]	Internal	Block sender	-	Eternal Demo
[@test.com]	Internal	Block sender	-	Eternal Demo
[@test.com]	Internal	Block sender	-	Eternal Demo
Blocked Senders	Everyone	Block sender	2018-10-16	Eternal Default Blocked Senders to Everyon...
sender@sender.com	Internal	Block sender	-	Eternal This is to block senders fromphis...
[alice.bob@gmail.com]	@rapid7.com	Block sender	-	Eternal Investigation at https://us.idr.in...

Blocked Sender