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.*

*Online Trust Alliance 2018.

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

Event & Flow Data

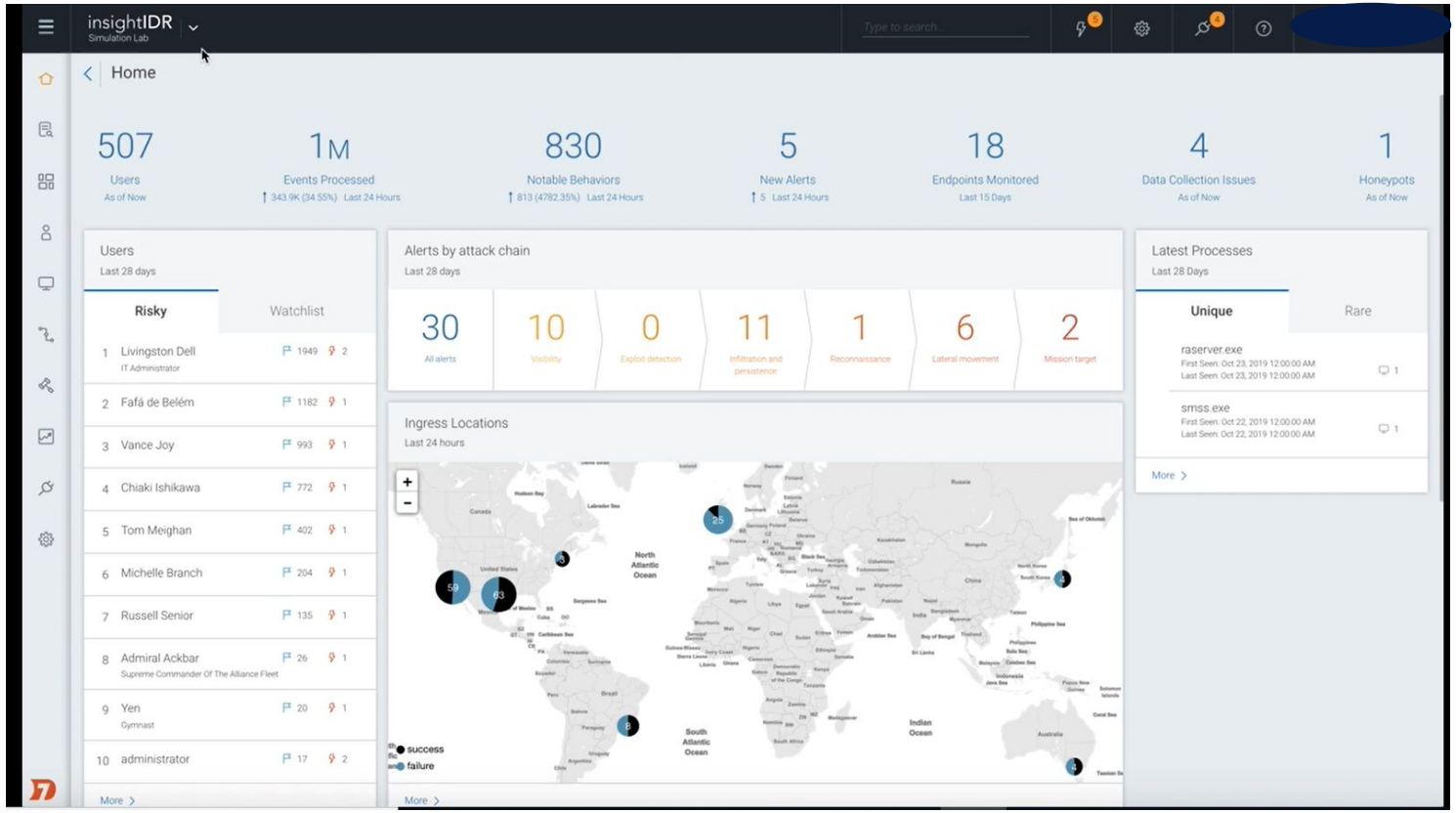
Collect and process data from various sources across the network

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

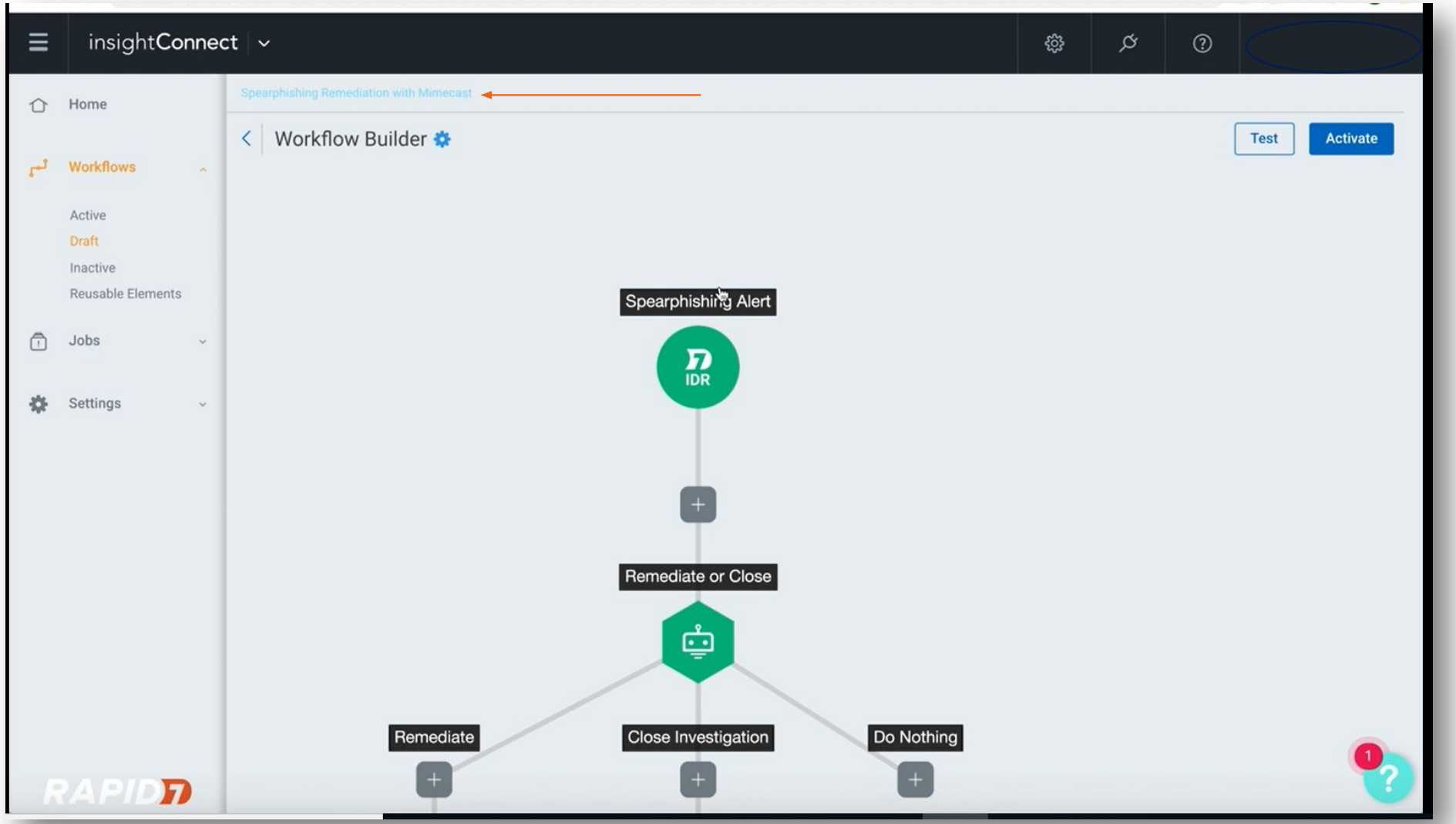
- Challenge:
  - Attackers targeted multiple users simultaneously across an organization, generating hundreds of alerts resulting in more work for a security analyst.
  - Repetitive and time consuming tasks, causing alert fatigue and stripping an analyst's time for actual problem-solving.
- Solution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

Let's Take A Look

Rapid7 – Mimecast Workflow



Mimecast Functions

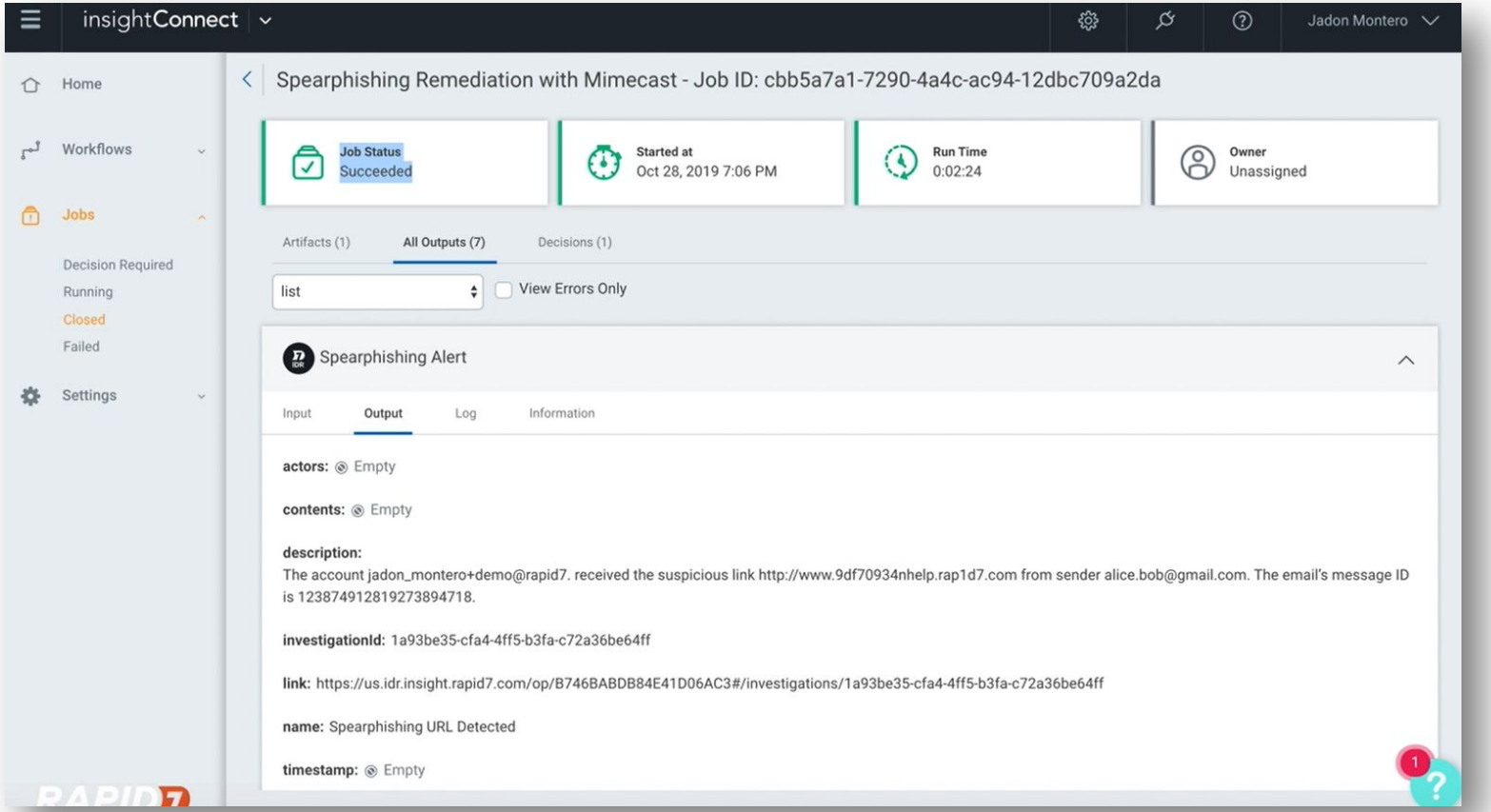
Block Sender
Prevent email delivery from malicious senders.

Permit Sender
Allow email receipt from trusted senders.

Block Domain
Prevent email delivery from malicious domains.

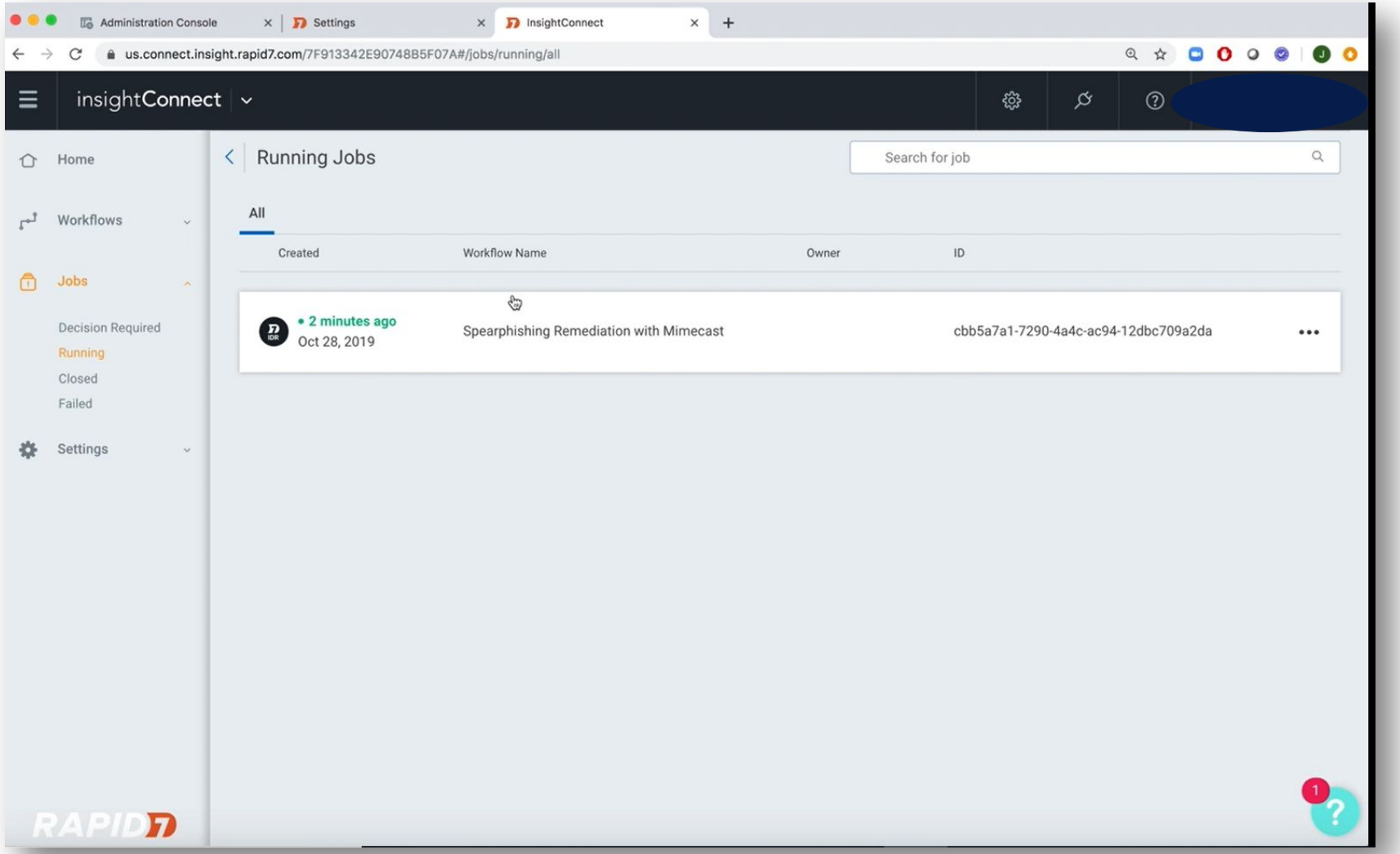
Permit Domain
Allow email receipt from trusted domains.

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

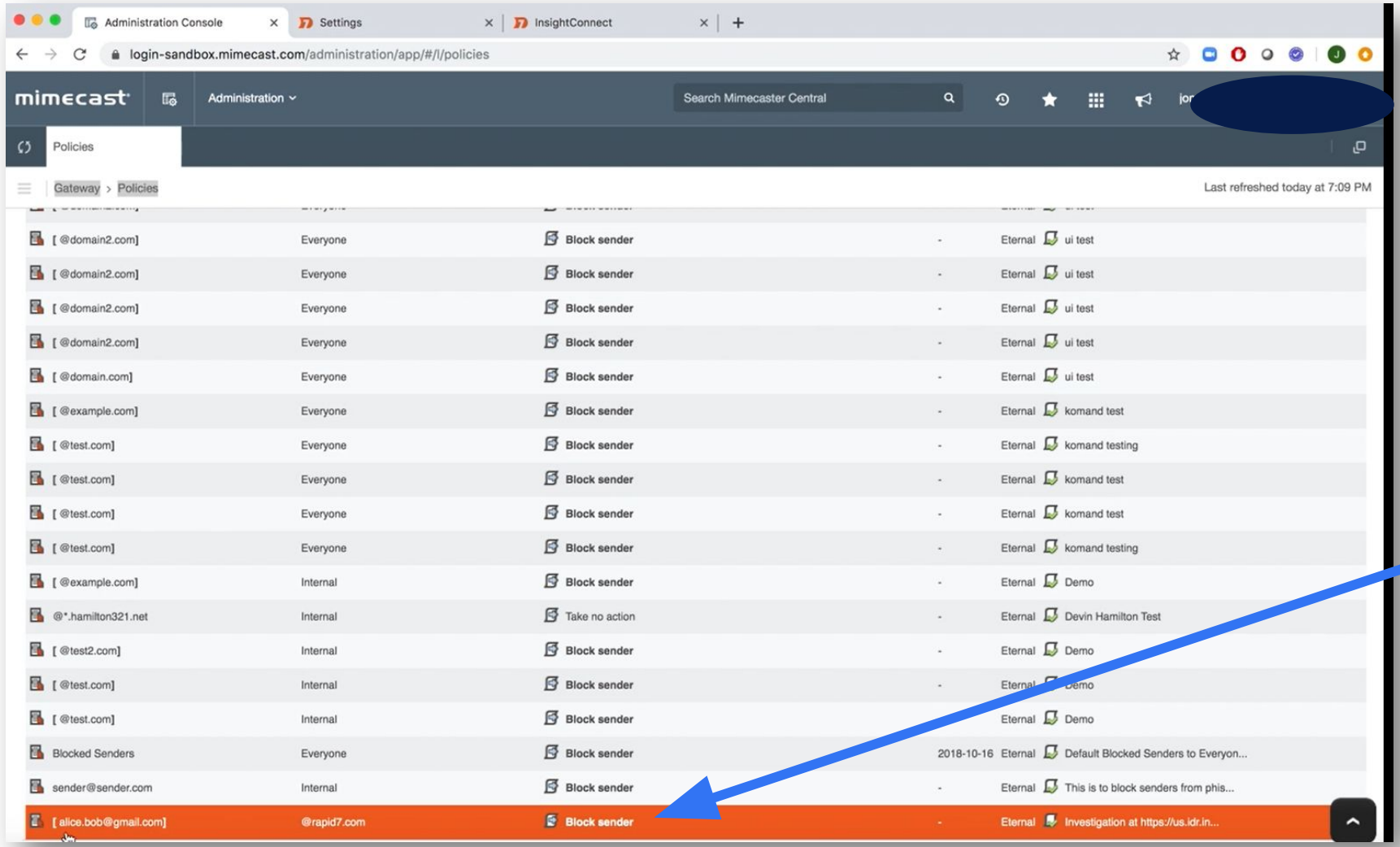


Successfully remediating against a malicious URL

Running a Job through Rapid7



Completing a Job through Mimecast



Blocked Sender