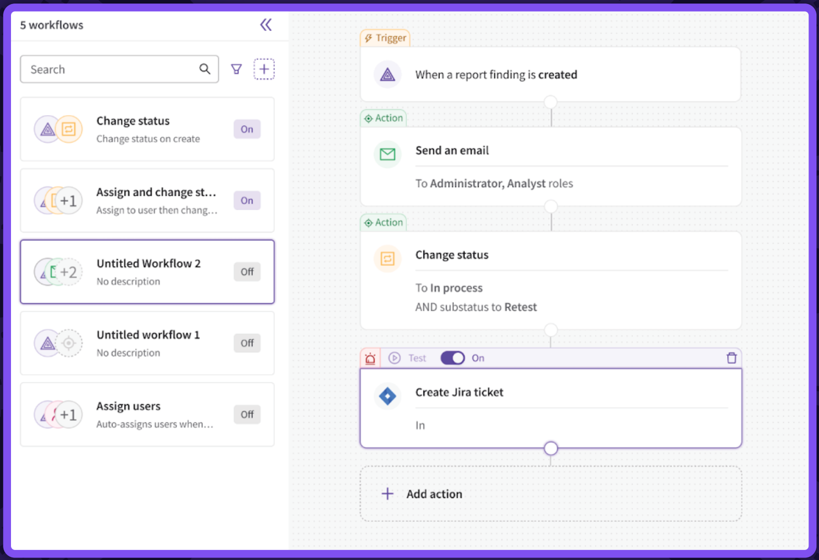
PlexTrac Workflow Automation Playbook

Save Time, Eliminate Bottlenecks, and Keep Security Teams Focused



5 workflows

Search

Change status — Change status on create — On

Assign and change st… — Assign to user then chang… — On

Untitled Workflow 2 — No description — Off

Untitled workflow 1 — No description — Off

Assign users — Auto-assigns users when… — Off

Trigger: When a report finding is created

Action: Send an email — To Administrator, Analyst roles

Action: Change status — To In process AND substatus to Retest

Test — On

Create Jira ticket — In

Add action

Why workflows matter:

Security work is too important to be slowed down by manual steps. Whether it's notifying the right people when a critical issue surfaces or assigning findings to the correct team, PlexTrac's workflow automation engine helps speed response time and drives consistency into established workflows.

This playbook highlights 7 key automated workflows to eliminate friction, reduce manual effort, and keep everyone aligned across your remediation process.

Create Tickets For Remediation When Findings Are Published

What it does:

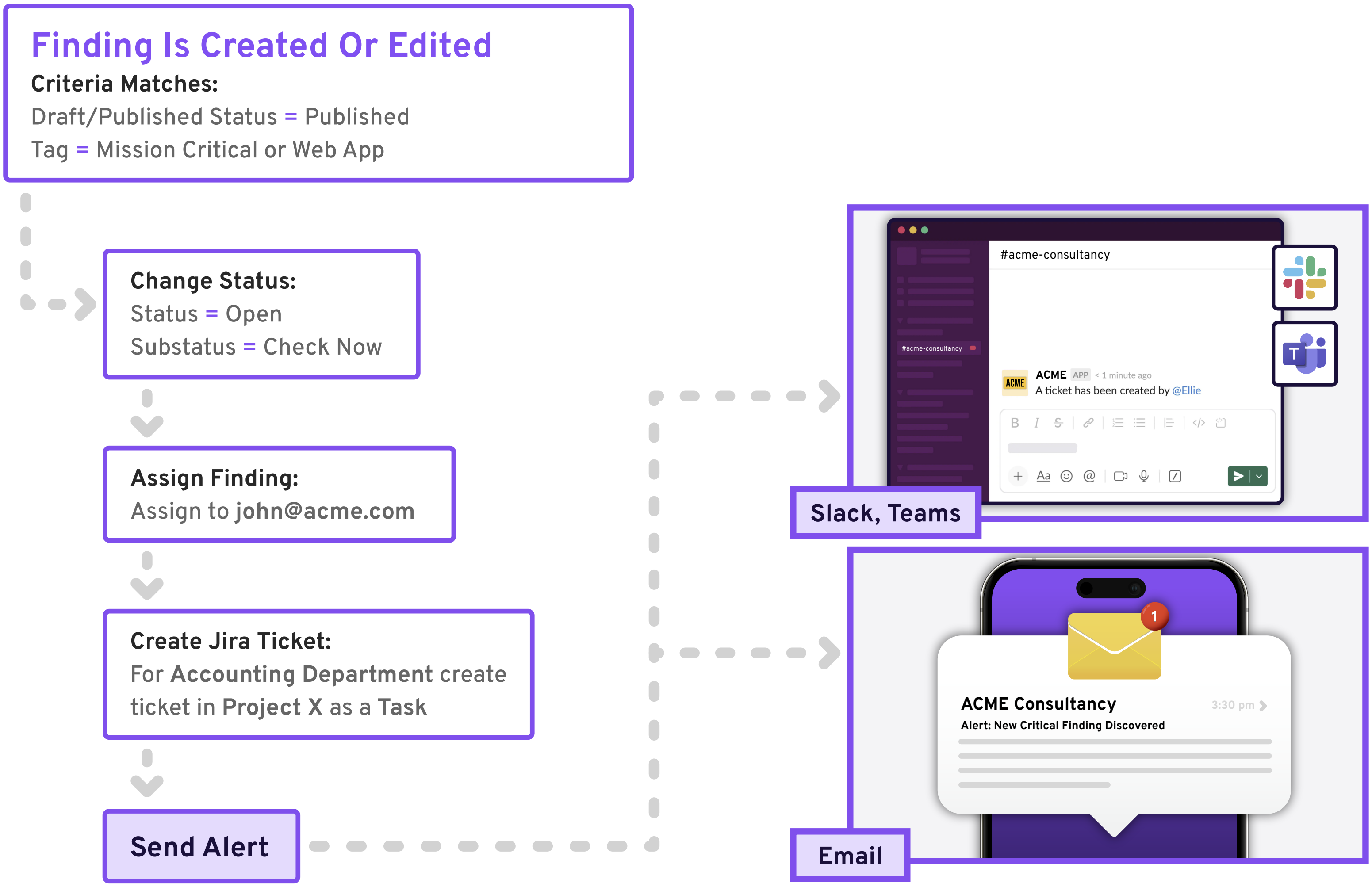
Automatically create a ticket in your issue-tracking system whenever a new finding is published. Control which project and issue types are used by identifying findings by their appropriate tags.

Scenarios where this helps:

- Engineering or IT teams work with tools like Jira
- Clients use tools like Jira and want findings delivered directly into their issue-tracking system
- Findings need to be tracked and resolved across functions
- Specific findings or assets should be shared with different teams across the enterprise

How it helps:

- Eliminate handoff delays to ensure nothing is missed
- Eliminate need for manual ticket entry
- Maintain existing, established workflows with bi-directional visibility between systems
- Ensure findings get to the right teams the first time



Finding Is Created Or Edited

Criteria Matches:

Draft/Published Status = Published

Tag = Mission Critical or Web App

Change Status:

Status = Open

Substatus = Check Now

Assign Finding:

Assign to **john@acme.com**

Create Jira Ticket:

For **Accounting Department** create ticket in **Project X** as a **Task**

Send Alert

#acme-consultancy

ACME APP 1 minute ago

A ticket has been created by @Ellie

Slack, Teams

ACME Consultancy 3:30 pm

Alert: New Critical Finding Discovered

Email

Auto-Close Informational Findings Ingested From Security Tools

What it does:

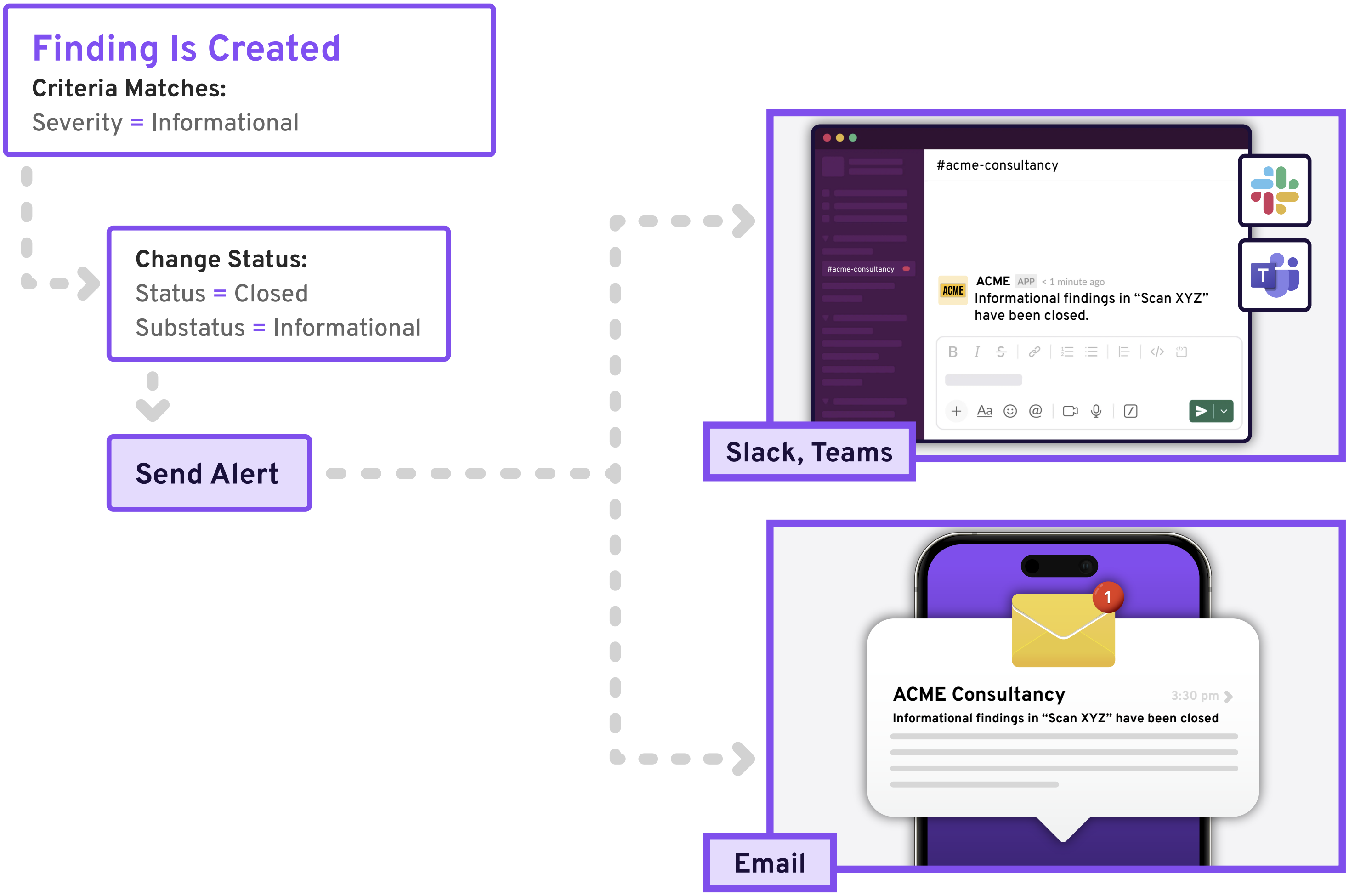
When a new scan is ingested, automatically close findings marked as “informational” so they don’t clog up dashboards or queues.

Scenarios where this helps:

- After a scan discovers findings with non-severity results
- When you need your team to stay focused on higher-risk issues, but don’t want to lose historical results

How it helps:

- Reduces triage time
- Keeps dashboards and workflows uncluttered
- Focuses attention on higher-risk issue



Finding Is Created
Criteria Matches:
Severity = Informational

Change Status:
Status = Closed
Substatus = Informational

Send Alert

Slack, Teams

#acme-consultancy

ACME APP < 1 minute ago
Informational findings in “Scan XYZ” have been closed.

Email

ACME Consultancy 3:30 pm
Informational findings in “Scan XYZ” have been closed

Send Real-Time Alerts When Critical Findings Are Discovered

What it does:

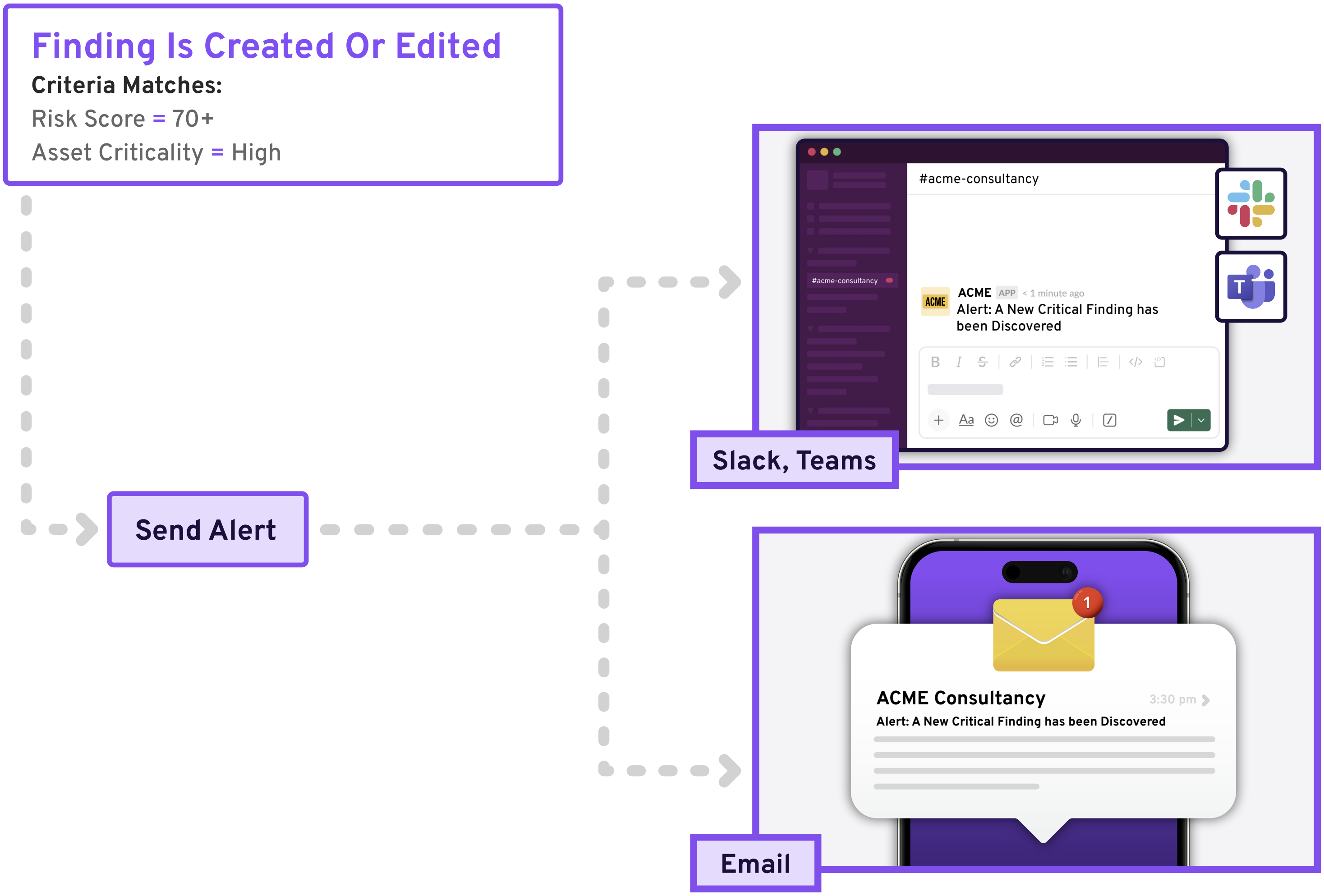
Send a real-time alert (Email, Slack, Teams, via webhook, etc.) when critical vulnerabilities are discovered.

Scenarios where this helps:

- During red team assessments, penetration tests, adversarial emulation, or any other type of testing
- Ensure high-severity issues are immediately addressed, even if testing has not yet been completed

How it helps:

- Speeds handoff and response time
- Reduces time to escalation
- Keeps stakeholders updated in real-time



Finding Is Created Or Edited

Criteria Matches:

Risk Score = 70+

Asset Criticality = High

Send Alert

#acme-consultancy

ACME APP < 1 minute ago

Alert: A New Critical Finding has been Discovered

Slack, Teams

ACME Consultancy 3:30 pm

Alert: A New Critical Finding has been Discovered

Email

Bonus Option: You can pair this workflow with the **Create Tickets For Remediation When Findings Are Published** on page 1, to auto create remediation tickets so that findings are immediately sent to the appropriate internal teams or customers for triaging.

Request Proofreading Of A Draft Finding

What it does:

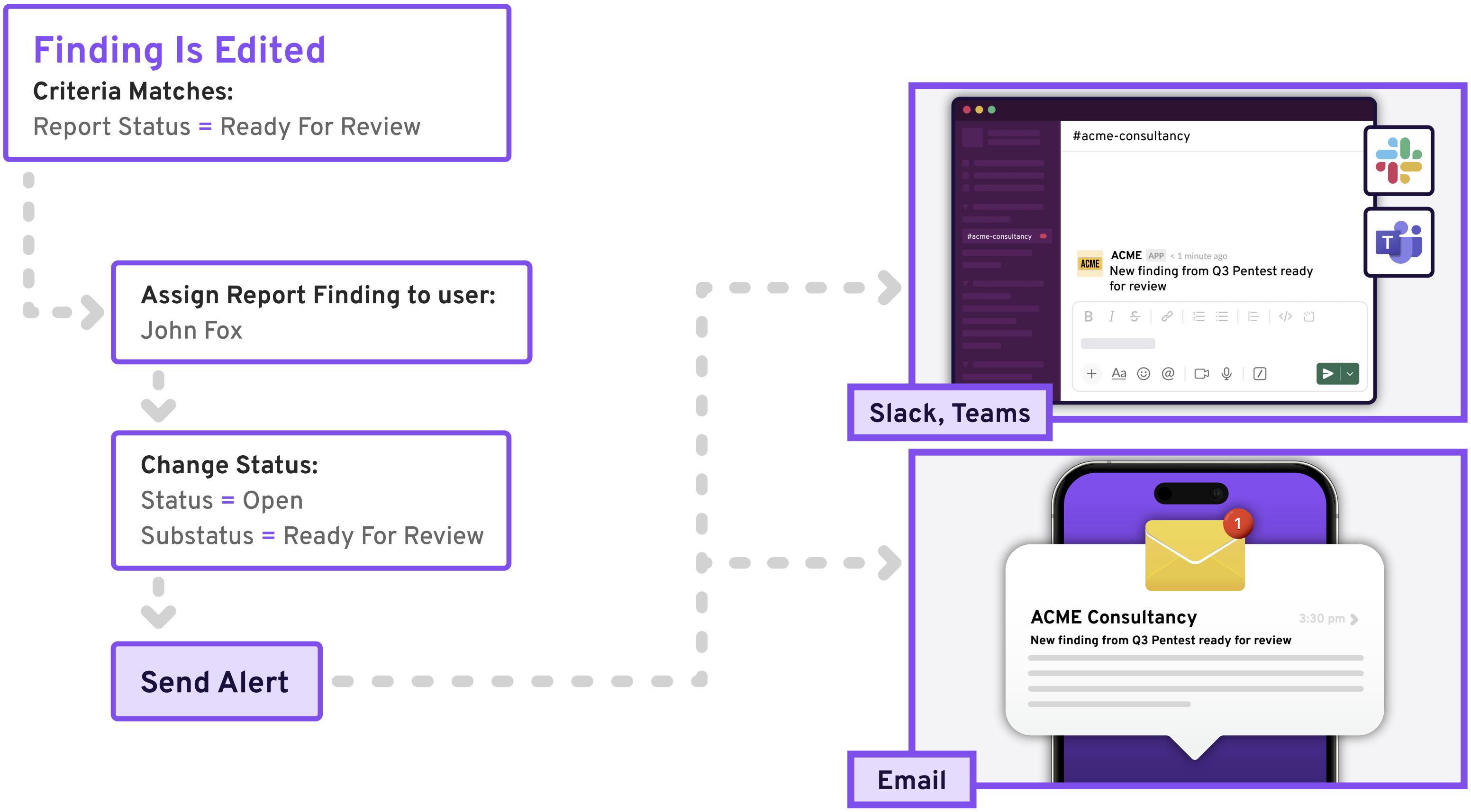
Send a real-time notification to a teammate when a finding is ready for review or needs to be edited.

Scenarios where this helps:

- During report writing or QA review
- When teams want multiple review levels prior to publishing

How it helps:

- Supports better quality deliverables
- Reduces communication overhead
- Encourages collaboration in the reporting process
- Supports more junior-level team members



Finding Is Edited

Criteria Matches:
Report Status = Ready For Review

Assign Report Finding to user:
John Fox

Change Status:
Status = Open
Substatus = Ready For Review

Send Alert

#acme-consultancy

ACME APP < 1 minute ago
New finding from Q3 Pentest ready for review

Slack, Teams

ACME Consultancy 3:30 pm
New finding from Q3 Pentest ready for review

Email

Alert When Findings Are Ready For Retest

What it does:

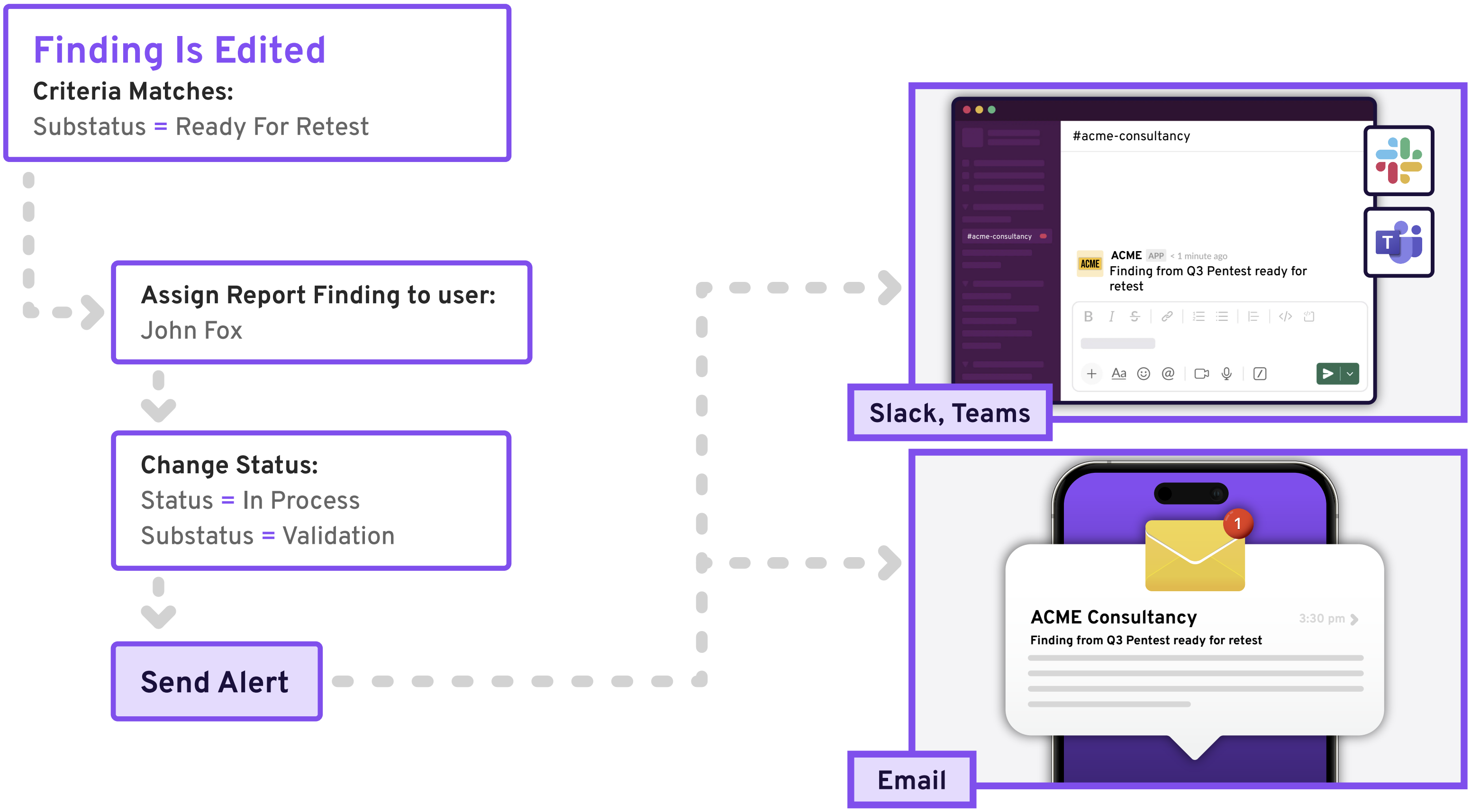
Automatically notify the right people when a finding is ready to be retested.

Scenarios where this helps:

- Retesting is managed by a different team or phase
- Timely follow-up is needed to close the loop

How it helps:

- Prevents retest delays
- Improves SLA compliance
- Bridges communication between team



Finding Is Edited

Criteria Matches:
Substatus = Ready For Retest

Assign Report Finding to user:
John Fox

Change Status:
Status = In Process
Substatus = Validation

Send Alert

#acme-consultancy

ACME APP < 1 minute ago
Finding from Q3 Pentest ready for retest

Slack, Teams

ACME Consultancy 3:30 pm
Finding from Q3 Pentest ready for retest

Email

Auto-Assign Findings To Users Based On Asset Type, Team, Role, Etc.

What it does:

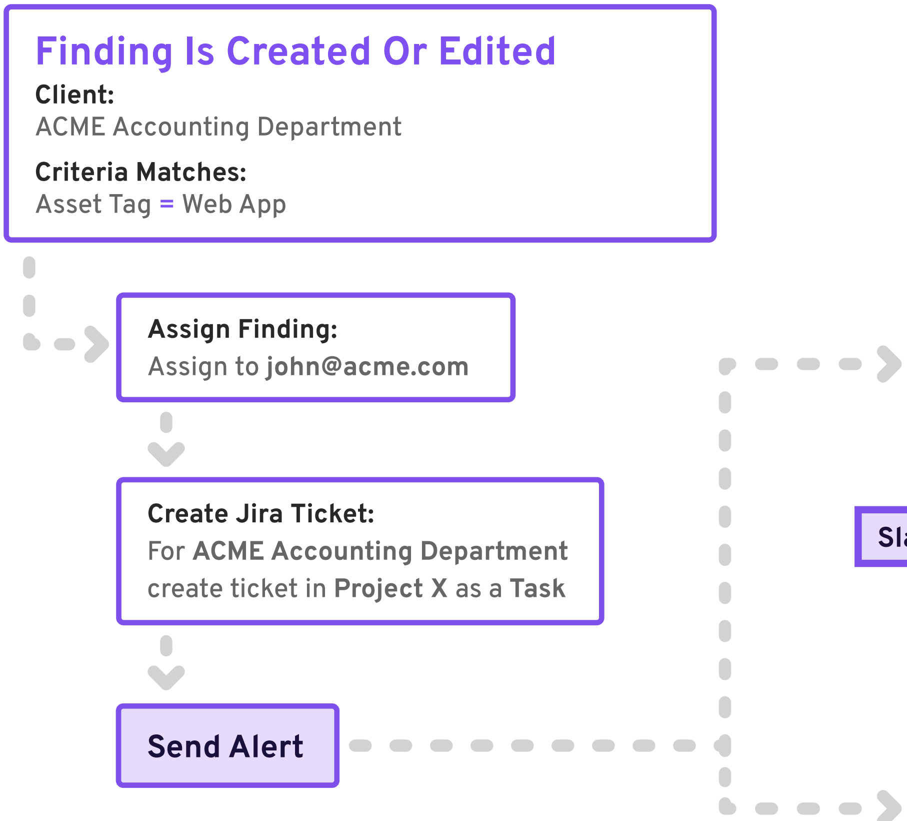
Auto-assign findings to specific users or teams based on role, department, asset type, criticality, vulnerability category, and more.

Scenarios where this helps:

- When findings should go to subject matter experts
- When teams are divided by domain, system, geography, or department

How it helps:

- Speeds up triage
- Reduces reassignment and confusion
- Eliminates manual efforts and human error



Finding Is Created Or Edited

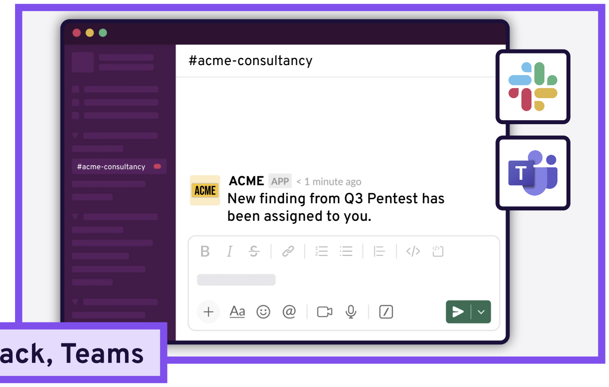
Client:
ACME Accounting Department

Criteria Matches:
Asset Tag = Web App

Assign Finding:
Assign to **john@acme.com**

Create Jira Ticket:
For **ACME Accounting Department** create ticket in **Project X** as a **Task**

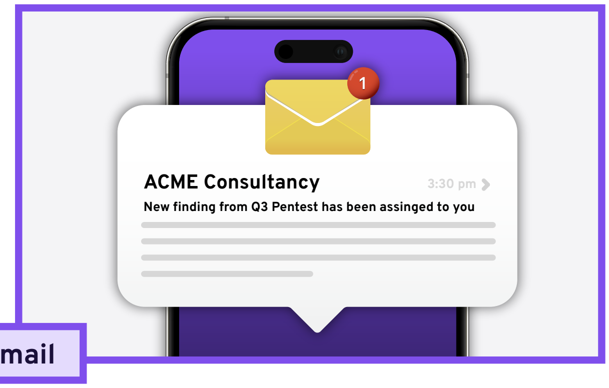
Send Alert



#acme-consultancy

ACME APP < 1 minute ago
New finding from Q3 Pentest has been assigned to you.

Slack, Teams



ACME Consultancy 3:30 pm
New finding from Q3 Pentest has been assinged to you

Email

Send Finding Updates To An Internal Client Portal or Immediately Alert Clients

What it does:

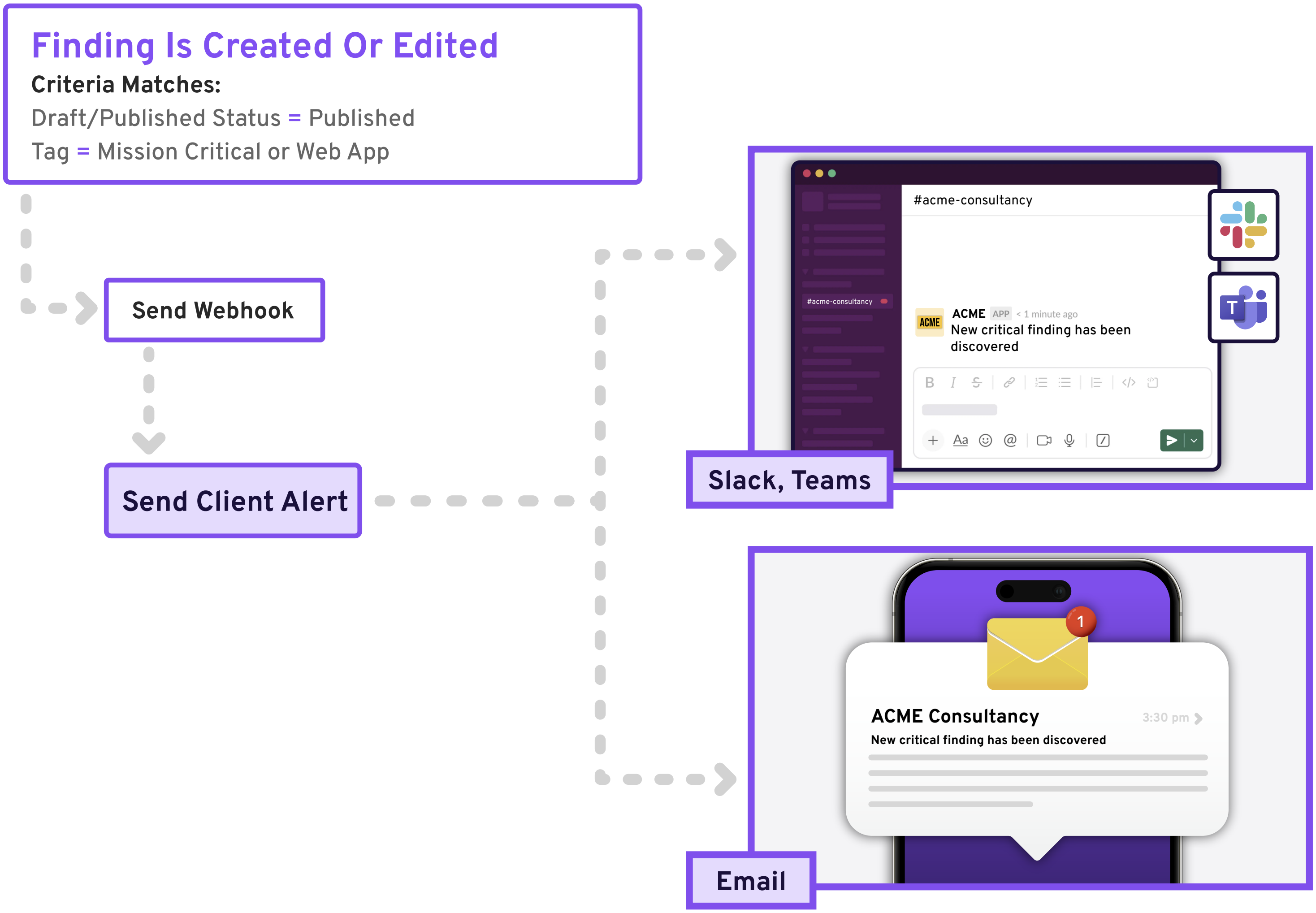
Send finding updates to a client-facing system via webhook and immediately alert the client.

Scenarios where this helps:

- Automating communication into client dashboards or systems
- Clients want real-time awareness of high-severity issues

How it helps:

- Strengthens client trust
- Reduces time to client response
- Enables seamless integration with client tools



Finding Is Created Or Edited

Criteria Matches:

Draft/Published Status = Published

Tag = Mission Critical or Web App

Send Webhook

Send Client Alert

Slack, Teams

#acme-consultancy

ACME APP < 1 minute ago
New critical finding has been discovered

Email

ACME Consultancy 3:30 pm
New critical finding has been discovered

PlexTrac is the leading AI-powered platform for pentest reporting and threat exposure management, trusted byFortune 500 companies and top security providers including Expedia, Mandiant, Deloitte, and KPMG. Built to help cybersecurity teams continuously manage and reduce threat exposure, PlexTrac centralizes security data, streamlines reporting, prioritizes risk, and automates remediation workflows—empoweringteams to drive measurable risk reduction.

Discover how PlexTrac can revolutionize your security operations at:

www.plextrac.com