

# CrowdStrike Alerts

## Generic help for the platform and be able to respond to basic alerts

- We receive pings in Channel "Technical - All" for CrowdStrike Alerts.
- Look for Hostname
- Reply to the post to say you are investigating
- or ping Matt for the associated ticket to assign to me

\*Escalate to Liam for assistance\*

- Log into CrowdStrike
- Click on New Detections (default filters to new)
- Find the alert with the associated hostname
- Status > Edit Status > In Progress > Assign to Yourself > Update Status
  - it will then move to the in progress filter
- Click on severity to pop out more information
  - click on network contain if it is a threat to other machines
  - once resolved click edit status, set the tag, and a comment, change status to closed, and update
- If true positive, escalate and advise the customer
- do not create any exclusions, escalate to Liam if you believe it is recurring

---

Revision #2

Created 2026-08-27 23:47:45 UTC by Admin

Updated 2026-09-07 22:14:21 UTC by Admin