SOLUTION QUICK CARD

Benign True Positive and False Positive Alert Verdicts

Trust your alerts for precision cyber response

KEY BENEFITS

- ✓ **Detect and respond fast** to malware and malicious misuse before the threat escalates to a full-blown breach.
- ✓ **Run security testing**, including penetration tests, without escalating non-malicious activity to your response teams.
- ✓ **Automatically detect trusted behaviors** such as authorized activities that are misidentified as alerts.
- ✓ **Customize alert filters** to assign verdicts based on your organization's business context and desired operations.
- ✓ **Extend beyond EDR vendor capabilities** and reduce false alarms with granular analysis of alerts based on benign true positive criteria and filters.

When a cyber alert hits your queue, your team reacts. But when too many alerts turn out to be false alarms, you start to doubt your Managed Detection and Response (**MDR**) service. That lack of trust leads to frustration, alert fatigue, and ultimately – an increased risk of a breach.

CRITICAL**START**® provides three levels of alert verdict classification – True Positive, Benign True Positive, and False Positive – to help you filter out false alarms and respond only when warranted.

How it works

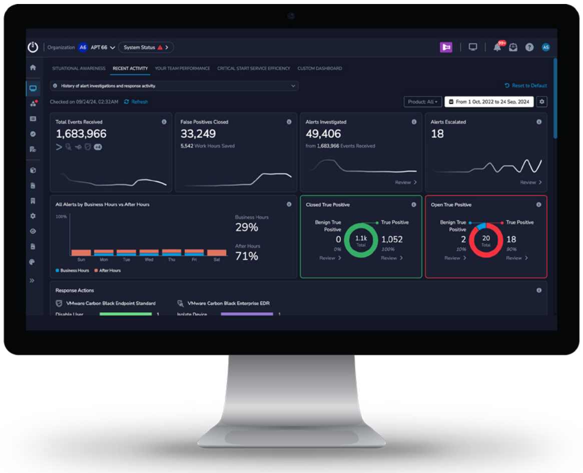
When any alert is raised by one of your security tools, it flows through a combination of automated and human-powered reviews to determine whether it requires escalation. These include Critical Start's curated Trusted Behavior Registry™ (**TBR**™), playbooks, filters, and investigation queues. Based on the findings, each alert is assigned one of three verdicts: True Positive, Benign True Positive, or False Positive.

Regardless of the alert verdict assigned, Critical Start MDR customers always have fully transparency and visibility into the triage, escalation, and resolution path of every alert – regardless of criticality. That means you can respond to the alerts that matter in the moment, and periodically review the alerts that are automatically closed to continually tune your playbooks, response authorizations, and filters.

True Positive: An alert that identifies a malicious action that requires attention and response to mitigate a real threat. For example, a true positive might be the detection of malware or account compromise.

Benign True Positive: An alert that is part of a known, authorized, or expected business process, but is identified by a security tool as malicious. Identifying these alerts is essential for regular security testing to show that critical security controls are functioning as expected.

False Positive: An alert where the detection incorrectly identifies non-malicious or known trusted behavior as malicious. This indicates that the detection mechanism is not working as expected. For example, a legitimate software update from a trusted vendor could be incorrectly flagged as a threat due to misconfiguration of detection rules.


Organization
A6 APT 66
System Status
SITUATIONAL AWARENESS
RECENT ACTIVITY
YOUR TEAM PERFORMANCE
CRITICAL START SERVICE EFFICIENCY
CUSTOM DASHBOARD
History of alert investigations and response activity.
Reset to Default
Checked on 09/24/24, 02:32AM
Refresh
Product: All
From 1 Oct, 2022 to 24 Sep, 2024
Total Events Received
1,683,966
False Positives Closed
33,249
5,542 Work Hours Saved
Alerts Investigated
49,406
from 1,683,966 Events Received
Review
Alerts Escalated
18
Review
All Alerts by Business Hours vs After Hours
100%
Sun
Mon
Tue
Wed
Thu
Fri
Sat
Business Hours
29%
After Hours
71%
Business Hours
After Hours
Closed True Positive
Benign True Positive
0
0%
Review
1.1k
Total
True Positive
1,052
100%
Review
Open True Positive
Benign True Positive
2
10%
Review
20
Total
True Positive
18
90%
Review
Response Actions
VMware Carbon Black Endpoint Standard
Disable User
1
VMware Carbon Black Enterprise EDR
Isolate Device
1