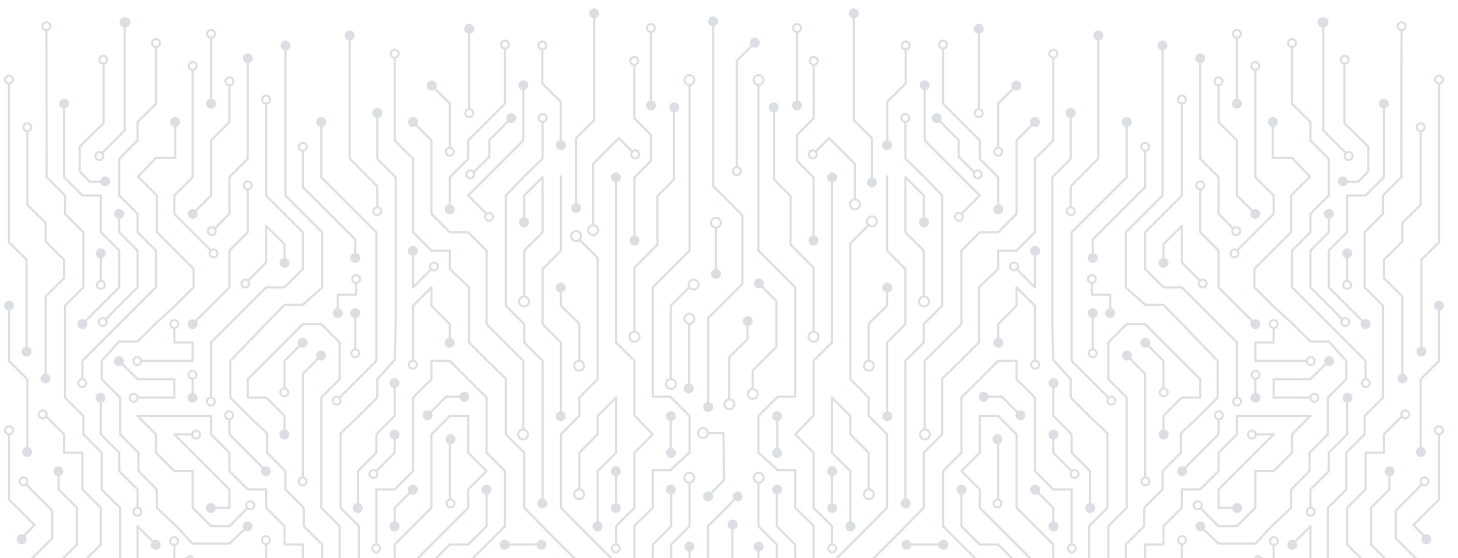




RESOLVE EVERY ALERT. **STOP BREACHES.**

When the stakes are high, organizations trust **CRITICALSTART™** – the Managed Detection & Response (MDR) experts that leave nothing to chance.





SECURITY IS ABOUT DEALING WITH RISK, BRINGING ORDER TO CHAOS.

Today, there is a critical and costly gap between security and the threats businesses face. Threats include insiders, nation-sponsored entities, and cyber criminals using constantly changing techniques such as zero-day and targeted malware, electronic espionage and fraud, and complex data exfiltration.

Security gaps exist for many reasons. Security teams are overwhelmed, fatigued and frustrated from alert overload. They do not have the headcount to fully investigate all security events, meaning they can't detect all attacks. Teams aren't properly deploying security tools, are ignoring tools, or increasing alert thresholds to reduce security event volume. As a result, analysts can't detect or contain breaches fast enough to reduce attacker dwell times.

The challenges are greater for organizations working with MSSP/MDR providers. Teams are forced to interact with their MSSP by email and through outdated web portals, with no knowledge or visibility into how alerts are triaged. Most find a one-size-fits-all approach that doesn't work with their unique business processes, requiring expensive, on-premise equipment. The result? Missed attacks, increases in attacker dwell time and remediation costs, and the inability to verify the effectiveness and quality of an MSSP/MDR due to their black box approach.

**THE RESULT? CUSTOMERS HAVE REDUCED
ALERTS THAT NEED INVESTIGATION BY**

99%

QUICK GUIDE

1

HOW DID WE GET HERE?

HOW CRITICAL**START** PROTECTS ORGANIZATIONS

OUR MDR SOAR PLATFORM

WHAT'S NEEDED: MOBILITY

NOTHING TO HIDE

WHAT TO ASK YOUR MDR PROVIDER



TODAY'S REALITY IS DAUNTING

The increase in cybersecurity alerts is a direct result of easier-to-launch attacks with more efficient methods to monetize them. While attacker tactics haven't changed, what has changed is:

CHEAPER to launch an attack

EASIER to monetize with cryptocurrency

FASTER to exploit vulnerabilities

This all leads to a tremendous increase in the number of attacks impacting companies every day. Is your organization equipped to manage an increase in cyber attacks?



THE COST TO DEFEND HAS SKYROCKETED

The costs of these gaps are staggering. Beyond the obvious theft of intellectual property and customer data, organizations are left with brand and reputation damage, the embarrassment of a public disclosure of an event, impacted shareholder value, and high turnover of security personnel, who quit out of frustration.

Average time to identify a breach: **197 days**

Average loss: **Approximately \$4.1M**

If a breach can be detected and contained in less than 30 days, then remediation costs **decrease by approximately \$1M**

Average time to contain a breach: **69 days**

87%

of respondents say they need up to 50% more cybersecurity budget

32%

of organizations experience a delay of over 6 months to fill a cybersecurity position with a qualified candidate

2.93M

global shortage of cybersecurity professionals

55%

of organizations expect an increase in cybersecurity budgets – down from 64% in 2018

500K

shortage of cybersecurity professionals in North America

89%

say their cybersecurity function doesn't fully meet their needs

60%

of organizations feel their cybersecurity budget is underfunded

69%

of cybersecurity pros say their teams are understaffed

12%

feel it is very likely they would detect a sophisticated cyberattack

34%

of security pros have a high degree of confidence in their team's ability to detect and respond to cyber threats

QUICK GUIDE

HOW DID WE GET HERE?

2

HOW CRITICALSTART PROTECTS ORGANIZATIONS

OUR MDR SOAR PLATFORM

WHAT'S NEEDED: MOBILITY

NOTHING TO HIDE

WHAT TO ASK YOUR MDR PROVIDER



RESOLVE EVERY ALERT TO DETECT ATTACKS

Organizations can't afford to ignore security events – even lower level security events, which is where many breaches and attacks occur. The goal is to quickly stop an attack before it becomes a breach. Nothing in the marketplace does this, which is why **CRITICALSTART** created its own platform.

CRITICALSTART is unique because we resolve 100% of security alerts. Our cloud-based Security Orchestration Automation and Response (SOAR) platform reviews every alert to determine a known good alert versus an unknown alert that needs to be investigated by our analysts. It's all baked right into our Zero-Trust Analytics Platform (ZTAP).

If you ignore or filter security alerts, you can't detect every attack and stop a breach from occurring. Organizations want the effectiveness and transparency of an in-house SOC, but without the cost. **CRITICALSTART** is the low risk option to replace or augment your SOC with an in-house, 24X7 SOC experience. **CRITICALSTART** adapts to your organization, provides complete transparency, and offers access to the analysts performing investigations.

**WE RESOLVE 100% OF
SECURITY ALERTS.**

OUR MDR PLATFORM

Managed Detection and Response (MDR) is all we do. Our MDR strategy is about building something that is effective and efficient, addresses the core problems of managed services, and can scale from small business to large enterprise with the same effectiveness.

Our cloud-based MDR SOAR platform is a multi-tenant system that provides a network effect, applying information learned from one customer to all other clients when applicable. Our platform augments this one-size-fits-all approach by adapting to each customer's unique business processes to resolve client specific software, administrative processes, and security tools. If **CRITICALSTART** is monitoring your network, you can be sure we're going to catch what attackers are trying to do.

CRITICALSTART'S MDR

ALL SECURITY EVENTS ARE UNKNOWN



Normalization & Aggregation

ZERO-TRUST ENGINE
(Resolve all alerts)

All Unknown Events investigated
by **CYBERSOC** analysts

QUICK GUIDE

HOW DID WE GET HERE?

HOW CRITICAL**START** PROTECTS ORGANIZATIONS

3

OUR MDR SOAR PLATFORM

WHAT'S NEEDED: MOBILITY

NOTHING TO HIDE

WHAT TO ASK YOUR MDR PROVIDER



BUSINESS BENEFITS

We don't believe in playing the odds by ignoring and filtering lower priority security events that could be early indicators of an attack. Our MDR platform improves the in-house SOC experience by resolving every alert using a 100% transparent process that extends the one-size-fits-all approach by adapting to each customer's unique business processes.

Through our approach, customers will realize:

Lower likelihood of damaging losses from inevitable breaches

Increased time available for IT security personnel to focus on the business

SOC 2 Type II certified Security Operations Center (SOC)

Realized financial savings vs. building in-house SOC

24X7 security monitoring and response capability implemented in months vs. years

Reduction of risk exposure to advanced threats

Reduced or eliminated financial losses

Senior management receives definitive information (not guesses) about security events

Security staff is more effective and confident in battling and understanding events

Stability of security operations even with loss of key personnel

90%

COMMON SECURITY EVENTS

Why waste time investigating?

10%

SPECIFIC TO A CUSTOMER'S SECURITY EVENTS

99% of these can be classified as GOOD, so really...

ONLY 1%

NEED TO BE INVESTIGATED

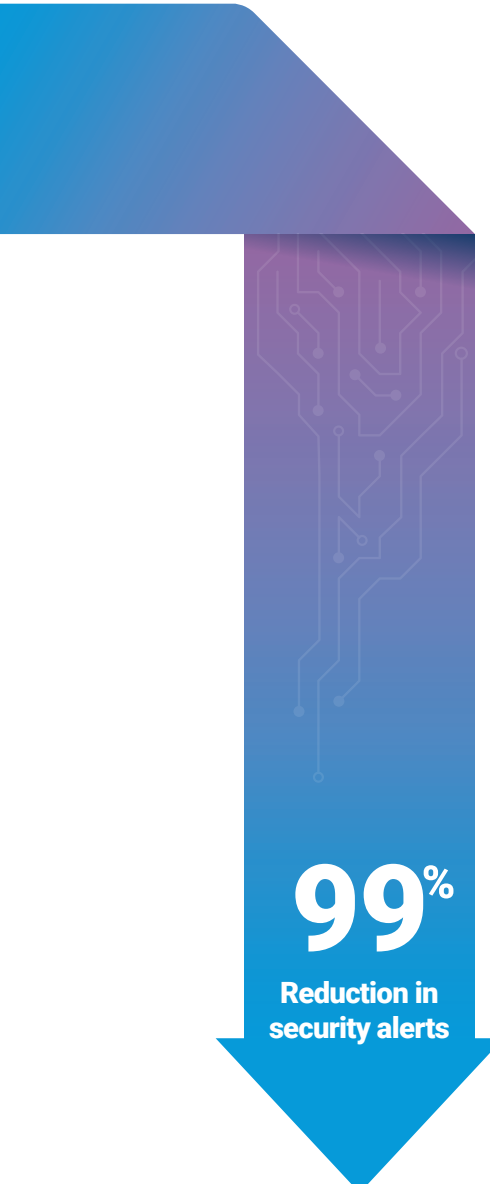
And that means...

ONLY .01%

NEED YOUR ATTENTION

HOW WE THINK ABOUT MANAGED CYBERSECURITY

Spending time managing too many security tools while investigating thousands of redundant alerts and false positives prevents security teams from adding value to the organization. The security team should spend their time on business issues that impact customers.



90% of security alerts are generic, meaning that an analyst doesn't need in-depth knowledge of the company to investigate and make triage decisions. These types of alerts can be handled more cost effectively by a quality MDR provider.

By resolving generic security alerts, **CRITICALSTART** frees up time for cybersecurity professionals to invest in the business and focus on the 10% of alerts that are unique to your organization and require expertise.

QUICK GUIDE

HOW DID WE GET HERE?

HOW **CRITICALSTART** PROTECTS ORGANIZATIONS

OUR MDR SOAR PLATFORM

4

WHAT'S NEEDED: MOBILITY

NOTHING TO HIDE

WHAT TO ASK YOUR MDR PROVIDER



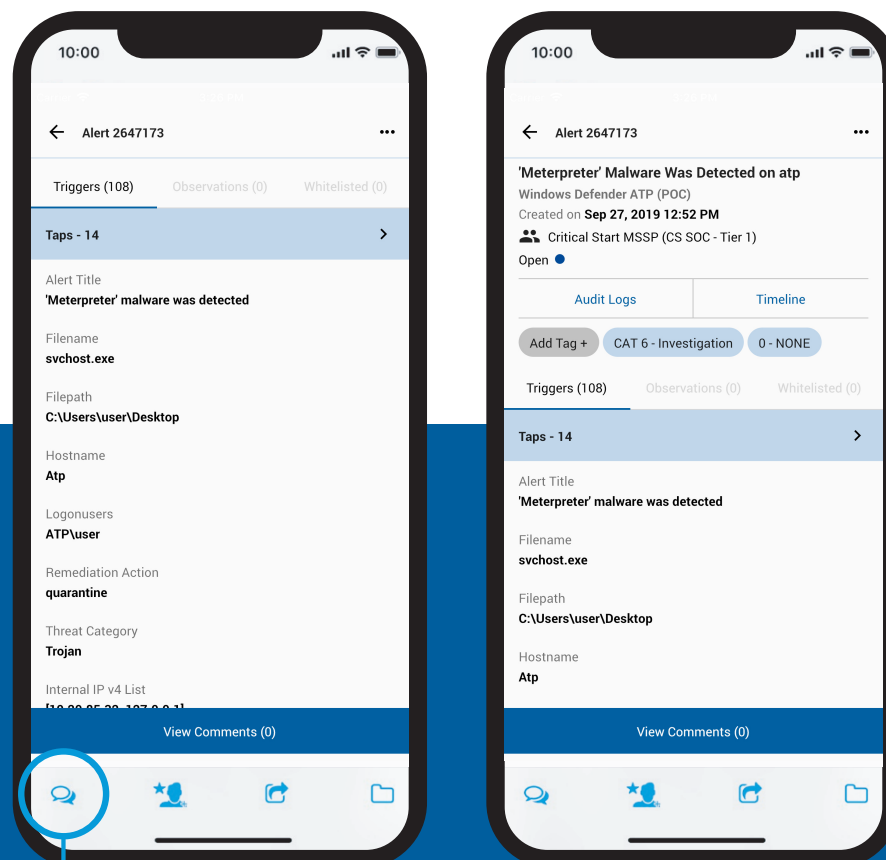
WHAT'S NEEDED: MOBILITY CONVENIENCE & SECURITY

Investigate, escalate, and remediate security incidents from anywhere using the MOBILESOC app for Android and iOS. Threat Analysis Plugins (TAPs) allow a user to investigate and respond to attacks via our MOBILESOC app:

Isolating
a host

Investigating
an endpoint

Blocking an IP
or domain



MORE LIKELY TO RESPOND, FASTER TO RESPOND,
MORE EFFECTIVE TO INTERACT BECAUSE WE
HAVE ADAPTED TO YOU

QUICK GUIDE

HOW DID WE GET HERE?

HOW CRITICAL**START** PROTECTS ORGANIZATIONS

OUR MDR SOAR PLATFORM

WHAT'S NEEDED: MOBILITY

5

NOTHING TO HIDE

WHAT TO ASK YOUR MDR PROVIDER



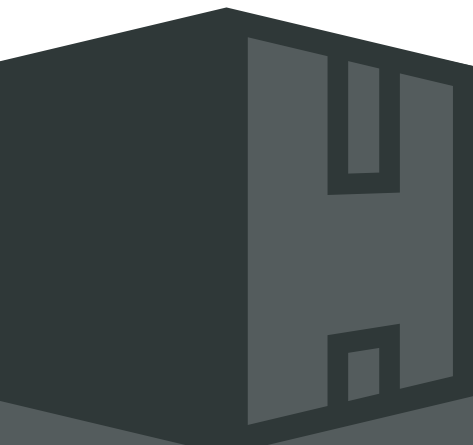
100% TRANSPARENCY – NOTHING TO HIDE

Transparency is very important to **CRITICALSTART**. We believe customers should “trust but verify” versus the “security through obscurity” approach used by many MDR providers. Our service extends beyond the one-size-fits-all approach of other MDR providers by leveraging the network effect that allows us to adapt to the unique business processes of each customer.

We create additional playbooks for each client to account for the unique scripts, software, administrative activity, network connections, and even temporary behaviors. To reach the effectiveness of an in-house SOC and detect all attacks, an MDR provider must address customer specific behaviors.

We designed our MDR service so that each customer has access to ALL playbooks, ALL rules, and ALL analytics used to resolve security alerts – nothing to hide and no black box. We deliver the same level of transparency as having an in-house SOC – allowing customers to move at the speed of business.

This radical transparency means complete transparency and access to all analysts, investigation comments, security analytics, and administrative consoles.



Avoid the black box approach of other MSSP/MDR providers that conduct investigations behind the curtain and magically teleport security alerts to a ticketing app, email client, or web portal.

TRUST BUT VERIFY

- ✓ What rules were applied to my events?
- ✓ Was there an SLA violation?
- ✓ How long did it take before triage began?
- ✓ Who performed the analysis?
- ✓ What were the results of security events that were closed?
- ✓ Was every security event investigated?

QUICK GUIDE

HOW DID WE GET HERE?

HOW CRITICAL**START** PROTECTS ORGANIZATIONS

OUR MDR SOAR PLATFORM

WHAT'S NEEDED: MOBILITY

NOTHING TO HIDE

6

WHAT TO ASK YOUR MDR PROVIDER



TODAY'S MANAGED SECURITY SERVICE OPTIONS



Legacy MSSP traditionally provides security device management and monitoring with automated forwarding of events – very little or no analysis.

LEGACY MSSP | SYMANTEC,
SECUREWORKS, OPTIV



MDR goes beyond MSSP to provide more advanced services that detect threats and include investigation comments by security analysts.

MDR | CRITICALSTART, EXPEL,
ESENTIRE, ARTIC WOLF



Outsourced security for managed services is offered by large consulting companies and outsourcers.

OUTSOURCED SECURITY |
DELOITTE, ACCENTURE, DXC



Product vendors such as CrowdStrike, FireEye, etc. offer endpoint detection and response services.

PRODUCT VENDOR | FIREEYE,
CROWDSTRIKE

MANAGED SECURITY SERVICE CAPABILITIES

CAPABILITY	MSSP	MDR	CRITICALSTART
Zero-Trust Engine with SOAR Platform			●
Transparent view to all rules, comments, audit logs, and metrics			●
Native iOS/Android applications for alert investigation and collaboration			●
SOCREVIEW for automated and audited review of subjective analyst alert analysis with numerical scores			●
Service Level Agreement for analyst time to respond to alert		◐	●
24x7 monitoring by cybersecurity analysts (SOC)	●	●	●
SSAE 18 SOC 2 (TYPE 1 and TYPE 2) certified	◐	◐	●
Analyst will proactively respond (isolate, block, whitelist, etc.)		◐	●
Multi-tenant so client can have multiple organizations with centralized parent			●
Alert notifications include short and long term recommendations		◐	●
Security alert investigation and notification performed by security analysts		●	●
Advanced threat detection and hunting		●	●
SIEM (log data collection, storage, security use cases)	◐	◐	●
Automated alert processing	●	●	●
Security device monitoring (alert forwarding)	●	●	●
Flexibility to expand portfolio of tools	◐	◐	◐
Security device management (firewall, SIEM, EDR, etc.)	●	◐	◐

DEFINE YOUR ORGANIZATION

"Our team is exceptionally small and tasked with providing as much as we can on razor-thin budgets and timelines which makes relationships that I have with your company so critical to our success. I have enough things to worry about on any given day and it is a breath of fresh air that CRITICALSTART and your SOC is not one of them."

**VICE PRESIDENT OF INFORMATION SECURITY
& INFRASTRUCTURE, FINANCIAL CLIENT**

ONE-PERSON SHOP



1-2 security personnel

Network, desktop, and server teams own parts of security

Only looking at most critical security events from a subset of tools

SMALL, EXPERIENCED TEAM



Have effective security tools

Team has cybersecurity expertise

Maintenance of tools and alert investigation takes too much time

Not enough resources to get to all projects

LARGER TEAM WITH PARTIAL SOC



All the security tools you need (maybe too many)

Desire for true 24x7x365 coverage with dedicated security analysts

Unable to properly investigate ALL the security events

FULL 24x7x365 SOC PROVIDER



24x7x365 fully staffed SOC providing services to customers

Sufficient metrics and processes to make risk-based decisions

Looking at ways to increase productivity through automation

QUESTIONS TO ASK YOUR MANAGED SECURITY SERVICE PROVIDER

1. Do you resolve every alert?
2. How long will it take to onboard and deploy?
3. Does your MSSP turn off features, in your security tools, to reduce the number of alerts they monitor for you?
4. What happens to my security tools if I end the contract?
5. Will escalated alerts include just the raw security event(s), or investigation notes, recommendations, and analysis that allow me to make a decision?
6. Will you take action to respond to threats such as isolating a host?
7. Will you refund monitoring fees for missing a SLA? Do you have a SLA?
8. Is a two-person review process enforced and audited for rules/logic that resolve false positives?
9. Is there an automated process to review quality of analyst reviews, and are these reviews transparent to the client?
10. Does the client have complete access to the rules, system audit logs, comments, and analysis notes for all security alerts – even for alerts not escalated?
11. Can clients collaborate, investigate, and respond to security alerts from native iOS and Android apps versus emails, web portals, and ticketing systems?
12. Do you have SSAE 18 SOC 2 certification with Type I and Type II?

THE CRITICALSTART DIFFERENCE: | DWELL TIME



RESOLVE EVERY ALERT

Eliminate Risk Acceptance.

ADAPTABILITY ENABLED WITH THE NETWORK EFFECT

BEYOND THE IN-HOUSE SOC

24x7x365 SOC monitoring investigation and response.

NOTHING TO HIDE – 100% TRANSPARENCY

INDUSTRY'S FIRST MOBILESOC

Customers interact directly with SOC analysts, on the go.

FASTER CONTAINMENT WITH NATIVE IOS/ANDROID APPS



Find out how Managed Detection & Response services from **CRITICALSTART** can transform your cybersecurity strategy. Visit us at criticalstart.com/mdrguide.

criticalstart.com