SOLUTION BRIEF

CRITICAL**START** Managed Detection & Response (MDR) Services

BENEFITS OVERVIEW:

- ✓ Reduce risk acceptance
- ✓ Increase SOC efficiency & productivity
- ✓ Validate value of security investments
- ✓ Report on security posture

Detect all events. Resolve all alerts. Stop breaches.

Today's reality is daunting. And no one needs to tell you that your job is getting harder. You're navigating a maze of security challenges--from staffing, to lack of visibility across disparate security tools, to an increase in sophisticated threats which are triggering massive volumes of alerts.

What if we told you there is a better way to approach threat detection and response? A better way that truly reduces risk acceptance, increases Security Operations Center (SOC) productivity, and helps you validate return on your security investments.

All MDRs are not all created equal.

Traditional threat detection and response services are designed to rank or suppress alerts, addressing only critical and high-priority alerts. Service providers often force customers to accept risk in the form of medium and low-priority alerts. **However, devastating breaches can arise from even low-level alerts.**

MDR METHODOLOGY	HOW IT WORKS	WHAT IT MEANS TO YOU
Input-Oriented	✓ Disables inputs or alters correlation logic that generates alerts to control false positives	✓ Acceptance of unquantified risk and decreased SOC effectiveness
Prioritization	✓ Only focuses on critical and high alerts, leaving most alerts untouched	✓ Acceptance of quantified risk
CRITICAL**START**	✓ Assumes every alert is bad until it can be proved good. Resolves 99% of alarms automatically and investigates remaining 1%	✓ Elimination of false positives at scale and optimal SOC team efficiency

We resolve more than 99% of alerts

We escalate less than 0.01% of alerts to customers

We reduce customer investigation time by an average of 99.3%*

*Assumption of workload based on average of 7-minute CRITICAL**START** alert investigation time. Customer workload with ZTAP and MDR is 22 hours/week. For the same volume of alert resolution without CRITICAL**START** MDR service and ZTAP platform, it would take 3,179 hours/week.

CRITICAL**START**
They're good. We're better.

What sets us apart?

Resolving alerts is good. Resolving all alerts is better.

Our unique trust-oriented model is based on resolving every alert. CRITICAL**START MDR** is driven by ZTAP, the Zero Trust Analytics Platform. ZTAP features the Trusted Behavior Registry (TBR), the largest registry of known good alerts (false positives), delivering the scalability to resolve every alert.

We take every alert from your security tools into ZTAP and match it against known good alerts in the TBR. If there is a match, the alert is automatically resolved. If there is no match, the CRITICAL**START** SOC investigates the alert.

Built-in transparency

Unlike traditional MDRs that take a "black box" approach to monitoring, CRITICALSTART is transparent by design. Our ZTAP dashboard lets you see exactly what our SOC analysts see.

- ✓ You have complete visibility and access to every alert with full investigation details, every action taken – all of it can be audited and reported on.
- ✓ Our Detection Engineering team uses the CRITICAL**START**™ Threat Navigator to map newly developed detections and out-of-the-box security tool detections to the MITRE ATT&CK® framework. This gives you full visibility and transparency into your threat detection coverage.
- ✓ Beyond visibility into the service, you have visibility across your security ecosystem. You can better understand how your security tools are performing and validate the return these investments plus your MDR service.
- ✓ We can prove it with contractual SLAs for Time to Detect (TTD) and Median Time to Resolution (MTTR). Our guarantee is that we will triage every alert in minutes with a 1-hour SLA.

Not more resources. Better ones.

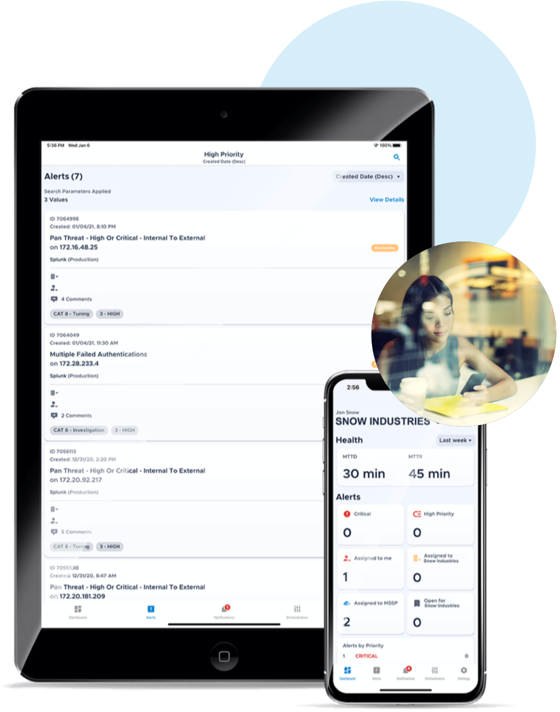
Leverage the collective experience of security experts with backgrounds in SIEM engineering and expertise across a broad range of security domains.

- ✓ 24x7x365 human-led investigation and response by highly skilled analysts who work in a U.S.-based SOC 2 Type 2 certified Security Operations Center (SOC).
- ✓ Rigorous training program–Every analyst completes 200 hours of training during onboarding and another 40-80 hours annually.
- ✓ CRITICAL**START**™ Cyber Research Unit (CRU)--Elite team, comprised of Cyber Threat Intelligence (CTI) and Detection Engineering (DE). Our CTI team curates original and third-party intel that our DE team uses to develop new detections.

Never miss a threat.
Or your desk.

Take threat detection and response on-the-go with the MOBILESOC application.

- ✓ Puts the power of ZTAP in your hands, via IOS or Android app.
- ✓ Provides on-the-go visibility and interactivity with direct communication with analysts, in-app responses and full details around the investigation – and has full parity to web.
- ✓ Allows you to contain breaches right from your phone.



5:36 PM Wed Jan 6 100%

High Priority
Created Date (Desc)

Alerts (7)
Created Date (Desc)

Search Parameters Applied
3 Values
View Details

ID 7064998
Created: 01/04/21, 8:10 PM
Pan Threat - High Or Critical - Internal To External
on 172.16.48.25
Splunk (Production)
Reviewing
4 Comments
CAT 8 - Tuning 3 - HIGH

ID 7064049
Created: 01/04/21, 11:30 AM
Multiple Failed Authentications
on 172.28.233.4
Splunk (Production)
2 Comments
CAT 6 - Investigation 3 - HIGH

ID 7056113
Created: 12/31/20, 2:20 PM
Pan Threat - High Or Critical - Internal To External
on 172.20.92.217
Splunk (Production)
5 Comments
CAT 8 - Tuning 3 - HIGH

ID 7055530
Created: 12/31/20, 8:47 AM
Pan Threat - High Or Critical - Internal To External
on 172.20.181.209

2:56
Jon Snow
SNOW INDUSTRIES

Health
Last week

MTTD	MTTR
30 min	45 min

Alerts

Critical 0	High Priority 0
Assigned to me 1	Assigned to Snow Industries 0
Assigned to MSSP 2	Open for Snow Industries 0

Alerts by Priority
1 CRITICAL 0

We take the journey with you.

Our commitment to your security doesn't end with your deployment. We assign each new customer their own Customer Success Manager—a dedicated point of contact who is devoted to providing regular communications and concierge services, including custom reporting, feature requests, and Executive Briefing Center (EB)/roadmap reviews.

Unparalleled partnerships

CRITICAL**START** integrates with best-in-breed technologies across Endpoint, SIEM, Identity, Cloud and more, to create a comprehensive security strategy with the tools you already use or that best fit your environment.

We only work with **the best.**

CRITICAL**START** Managed Detection and Response (MDR) services integrate with leading security technologies to detect every alert, resolve every alert and respond to breaches. Our services provide you full operating potential for threat detection and response and help you accelerate return on your security investments.

Microsoft Defender for Endpoint
Microsoft 365 Defender
Azure Sentinel
CORTEX BY PALO ALTO NETWORKS
splunk>
DEVO
vmware Carbon Black
BlackBerry CYLANCE
SentinelOne
CROWDSTRIKE

Goodbye, alert fatigue. Hello, CRITICALSTART.

Contact Us

Request a Free Assessment

CRITICAL**START**
They're good. We're better.