DATASHEET

CRITICALSTART® Cyber Research Unit

Stay ahead of emerging threats.

KEY BENEFITS

- ✓ Enhance your overall SOC efficiency and operations
- ✓ Offload the burden of collecting threat intel
- ✓ Give your internal staff the freedom to focus on other strategic tasks
- ✓ Make decisions based on timely, relevant data
- ✓ More effectively prevent breaches and reduce attacker dwell time
- ✓ Stay one step ahead of advanced and emerging threats

The CRITICALSTART® Cyber Research Unit (CRU) is made up of an elite team of researchers and threat detection engineers who build and enrich detections and Indicators of Compromise (IOCs) and support our Managed Detection and Response services delivered 24x7x365 by our U.S.-based Security Operations Center (SOC). This team works as an extension of your team to stay ahead of emerging threats and prevent breaches.

Two teams are better than one.

Cyber Threat Intelligence (CTI) – Curates original and third-party threat research on behalf of our MDR customers and only sends you what is actionable, to provide proactive visibility into new and emerging threats. The following services are included with our MDR offering at no additional cost:

- ✓ Intelligence Summaries (INTSUMs) – Weekly summaries of relevant cybersecurity-related activities or threats
- ✓ Security Advisories – Timely notices of emerging threats or other cybersecurity activities
- ✓ Requests for Information (RFIs) – Manual infrastructure analysis and reporting (one per month)
- ✓ Operational Reviews/Quarterly Business Reviews – Full reports on alert trends or groups of alerts presented as a quarterly summary
- ✓ Zero Trust Analytics Platform™ (ZTAP™) Enrichment – Ad Hoc intelligence-driven detection creation requests

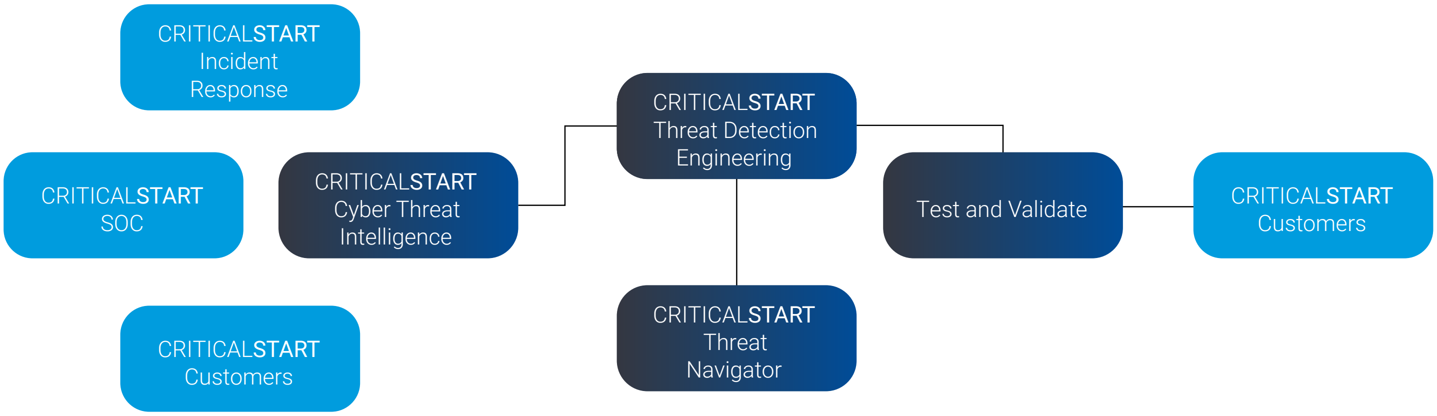
Threat Detection Engineering (TDE) – Leveraging the original and third-party intel produced by the CTI team, previous SOC investigations, and Incident Response investigations, the CRITICALSTART Threat Detection Engineering (TDE) team develops and enriches new detections and IOCs. By doing so, the TDE team provides additional value to the out-of-the-box detections and IOCs. Leveraging the CRITICALSTART® Threat Navigator, the TDE team also maps detections to the industry-leading MITRE ATT&CK® framework, ensuring you are protected against the latest attacker Techniques, Tactics and Procedures (TTPs).

CRITICALSTART®

© 2022 CRITICALSTART. All rights reserved.

How We Do It

Whenever the Threat Detection Engineering team is notified of a new threat or attack, it uses Threat Navigator to identify gaps in your security tool's detection coverage. Threat Navigator maps detections to the MITRE ATT&CK framework. Leveraging this framework, the TDE team develops and enriches new detections and IOCs, verifies the effectiveness of these detections in ZTAP, tunes out any false positives, and then pushes the new detections to all of our MDR customers. This process enables us to respond early in the attack cycle and prevent repeat attacks.


CRITICALSTART Incident Response
CRITICALSTART SOC
CRITICALSTART Cyber Threat Intelligence
CRITICALSTART Customers
CRITICALSTART Threat Detection Engineering
CRITICALSTART Threat Navigator
Test and Validate
CRITICALSTART Customers

Contact Us

Request a Free Assessment

© 2022 CRITICALSTART. All rights reserved.