SOLUTION BRIEF

CRITICAL**START** Threat Hunting Services

Faster threat containment for better security.

When your organization is under attack, response time matters. Once a threat has infiltrated your network and the longer it is inside your network, the more damage it can do.

Combined with a highly trained team of SOC analysts, our Managed Detection and Response (MDR) services leverage a sophisticated methodology to identify and contain threats faster and more effectively.

As a first step, CRITICAL**START** performs endpoint threat hunting over a 30-day period for the identification and escalation of malicious files, identification of suspicious script and command line activity, and other indicators of compromise within the existing environment.

The objective is to identify malicious activity observed on the network, isolate endpoints to prevent lateral movement and malicious communications, advise on the removal of damaging materials left by attacks/attackers, and monitor the network for indicators of compromise and anomalous activity utilizing industry leading tools in endpoint detection and response (EDR) and endpoint protection and prevention (EPP).

Our Methodology

CRITICAL**START** uses a Zero-Trust approach to improve the effectiveness of our threat hunting. With our platform, we investigate all security alerts until they are classified as good or normal and can be safely filtered out. Rather than assuming that any events are known good, we assume every unknown or uncategorized security event is considered anomalous and should be investigated.

Our platform performs monitoring, analysis, and searching for signs of malicious files, which are then triaged by the CRITICAL**START** CYBER**SOC** for monitoring and analysis.

CRITICAL**START's** MDR services use leading next-gen EDR and EPP tools to prevent sophisticated malware attacks, and machine learning and artificial intelligence (AI) to identify malicious code without relying on signaturebased detection, and provides memory protection. The EDR functionality provides the ability to isolate machines proactively by the SOC to prevent lateral movement of malicious activity without having to physically touch the machine.

The end result? We can handle the highest volume of incident "noise" without taxing our customers or missing critical events. This yields security monitoring that is more efficient, effective and comprehensive.

Multi-Phased Assessment

CRITICAL**START** provides detailed assessments to understand your risks and identify a clear path to proactively strengthen your security posture. We take a multi-phased approach to our assessments, which include:

1 DESIGN/SCOPING

We begin by gathering intelligence. As a first step, we set up a scoping call where we identify users, points of escalation and the management of systems. Next, we define the endpoint monitoring strategy and scope of services.

2 IMPLEMENTATION/DEPLOYMENT

During implementation, we setup cloud-hosted servers for EDR and set up the next-generation EPP tool. We will establish user accounts in a Single Sign-on (SSO) platform with two-factor authentication, as well as set up our platform. Our SOC team will then define the users, notification schedules and escalation paths.

We will hold a deployment call with our team and yours where we deliver installation scripts and validate your access to our SSO solution. We will also educate and train your users on our MDR tools, tactics and procedures. Finally, as your organization gets the various security tools deployed within your environment, the SOC will begin to receive events/alerts in ZTAP.

3 ENVIRONMENT BASELINING AND TUNING

All security events go through the ZTAP's Zero-Trust engine, which uses human-supervised machine learning and applies global filters that have established "known-good" events.

Events that did not meet the criteria for "known-good" will then appear in the incident queue for the SOC to triage, investigate, and/or escalate. This is the second part of the tuning process. We will then identify approved internal applications that are causing alerts and perform advanced filtering to identify authorized activity and remove it from the incident queue. This allows internal applications to be used but still ensures that unauthorized and/or unknown activity from the application are still alerted on and investigated.

SOC analysts will escalate incidents to the customer for one of two reasons: 1) The incident looks (or is) malicious and action needs to be taken; 2) The incident may be malicious but could be authorized activity and requires feedback from the customer. If the activity is deemed good by the customer, the SOC will then create a filter to remove that specific incident from appearing in the queue again.

REPORTING

CRITICAL**START** provides a detailed MDR report at the conclusion of the Threat Hunting engagement. The report provides an overview of the events and incidents observed by the CRITICAL**START** CYBER**SOC** over the 30-day period. This report includes event and incident counts, their type, source of detection, and additional findings made during the threat hunting process. The company provides an outline of significant threat findings, their level of risk, actions taken by the SOC, and recommended actions for each finding it outlined in the report.

Key findings are listed with an associated risk level, and recommended next steps are provided should the customer choose to follow. The goal of this report is to provide the customer with everything they need to make an informed decision on how to move forward, and the necessary information required to present to other teams and leadership within the company to gain the buy-in needed to execute on any changes or investment required.

4 MALWARE DETECTION AND THREAT HUNTING

Then the real work begins:

- ✓ We evaluate malicious executables identified by EDR and EPP: Ransomware, Trojans, Rootkits and Spyware. We also evaluate suspicious/malicious scripts and memory exploits identified by EDR and EPP. This can include: Encrypted Powershell, identifying what scripts running within the environment are authorized by the client, memory exploits attempted on endpoints, and other scripts in various languages being run on the customer environment.
- ✓ Next, we investigate suspicious/malicious activity flagged by EDR. This can include malicious behavior based on unique indicators of compromise. We also identify malicious/ suspicious files by MD5 hash.
- ✓ We will look into assets that exhibit suspicious communications to devices that are outside of the customer network, such as Botnet activity, command and control, and remote access. This includes communication with known malicious IP addresses and domains.
- ✓ We investigate suspicious behavior by known and unknown applications within the environment, such as commands being executed, system calls and the location of application and child processes involved. We also look into unique behaviors from known parent processes such as Acrobat, Java, Word, Chrome, and CMD line. Finally, we identify unique child processes and use of PowerShell, and unique file persistence in Windows Services and Tasks.
- ✓ For proactive prevention and response, we isolate endpoint machines showing malicious behavior that could result in lateral movement, propagation of malware, and/or data exfiltration. We then ban hashes that have been found to be associated to malicious executables, and set policies to auto-quarantine threats found by EPP technology.