# snc®

# Detect, Analyze & Report Threats (DART)

## Rapid Cyber Detection on Target

Adversaries actively attempt to hack U.S. government contractors' networks to exfiltrate sensitive or classified data. When successful, these efforts can compromise critical programs or technologies, eroding U.S. government competitive advantages. DART leverages leading edge, open source technologies to provide visibility of unknown threats and increase productivity in both cyber security and business processes. DART centralizes and automates the capture, triage and detection of cyber threats so operators can search, visualize, report and respond to them efficiently and with greater accuracy. It is the clear choice for companies looking to centralize their cybersecurity strategies.

# Detect, Analyze & Report Threats (DART)

| 250 MBps | <5 min |
|---|---|
| Raw Data Ingestion Speed | Raw Data Ingestion Speed |

**Search Speed on a 2PB System**

| <15 sec | <60 sec |
|---|---|
| Non-Aggregate Queries | Aggregate Queries |

## RAPID CYBER DETECTION ON TARGET

DART gives security teams centralized visibility into all network and security data to enable rapid analytic, detection and reporting capabilities – essential in today's fight against advanced threats and determined threat actors. DART scales to any size organization, and can ingest more than 20 terabytes of data per day from multiple data sources including firewall logs, intrusion detection logs, intrusion prevention logs, proxy logs, email logs, netflow, packet capture logs, threat intelligence feeds and much more. DART centralizes, indexes, normalizes and correlates this data at the time of ingestion, delivering comprehensive reports and visualizations in seconds.

DART provides actionable information to improve your security posture with applied analytics and artificial intelligence (AI)/machine learning (ML) analysis across multiple data points. DART is a unique cybersecurity intelligence tool that maps and fuses an organization's infrastructure with known cyber-attack patterns of foreign adversaries.

DART has proven ingest speeds of over 250MB records per second, can handle more than 20 terabytes per day, and has a maximum storage capacity of more than 2.5 petabytes. DART indexes all data at the time of ingestion, which delivers superior query performance. This process (Exhibit 1) is customizable to any data source. In one tailored instantiation of this capability, DART maps data for thousands of organizations and associated campuses, hundreds of thousands of IOCS and cyber sources to include 300+ million net flow records daily.

**Data Ingestion.** Scalable solution with proven ingest speeds of large volumes of data in near real-time.

**Cyber Battlespace Awareness.** Infrastructure and threat data combined with other sources to link cyber activity with specific company information like user data, asset data or threat data to enhance situational awareness.

**Discovery.** Ultra-high-speed searching with the ability to search hundreds of terabytes of data in seconds.

**Visualizations.** Near real-time visualizations to see developing cyber situations. Visualizations generated with DART show the situation, as it was minutes or even seconds ago.

**Advanced Analytics.** Open analytic platform with applied AI/ML and complex algorithms to analyze cyber threats such as data exfiltration, threat match, policy violations, geographic anomalies and external attacks.

| DART maps outward facing IP addresses & external domains/ subdomains | Customer fuses maps with counterintel data | Customer creates Threat Report | Customer partners with contractors to mitigate threats & vulnerabilities |
|---|---|---|---|

*DART defeats cyber threats through rapid detection, data visualization and applied analytics.*

**snc**®

10/31/2024