CYBER DEFENSE NETWORK

Announcing the NC4 Cyber Defense Network

The objective of the Cyber Defense Network (CDN) is to help our nation's critical infrastructure communities and private sector companies defend themselves against cyber threats with greater efficiency, effectiveness, and speed.

CDN Cyber Triage

In the battleground of cyber warfare where both communities and enterprises are overloaded, triage of threats is essential. CDN provides a multi-tier cyber triage capability that drives proactive cyber defensive actions. Fast, effective and efficient triage is accomplished by a composite of people, technology and processes enabled by CDN. The triage functions are distributed across three tiers:

- **Tier 1 - In your trusted community:** CDN powerfully enables specific trusted, closed communities to triage threats. In this secure, private cloud-based triage network, new threats, enriched threats, and member-rated threats are continuously provided and constantly evolved by trusted members. In addition to providing the technical triage network, NC4 provides basic data enrichment, community facilitation and program management.
- **Tier 2 - On the Edge of your Enterprise - Automated Triage:** NC4 provides a CDN/Edge (or Soltra Edge Solution) which runs securely on-premise within your enterprise. This empowers each enterprise to create their own specific intelligent rules to make automated triage judgements relevant to their own company and their internal constituent organizations.
- **Tier 3 - Enterprise Internal Triage:** Your internal specialists (threat intel specialists, incident response teams, SOC analysts) further triage and analyze threats and determine courses of action potentially in conjunction with third party solutions such as TIPS, SIEMS, etc.

Proactive Defensive Actions

Using CDN/Edge (on-premise), threat intel and SOC groups can define, where appropriate, specific rules to automate actions through internal solutions (endpoint management, orchestration/ automation) using a variety of automation modes from "human-in-the-loop" to fully automated.

CDN Benefits

For **community level audiences** such as cyber threat information sharing organizations, NC4 CDN can power the next generation of ISACs and ISAOs through the advanced triage and automation capabilities.

Foundational Elements:

NC4 has been the leading company providing cyber threat sharing through two industry leading solutions:

- NC4 Mission Center Cyber Threat Exchange (CTX) is a secure portal-based solution used by cyber security specialists in the world's top critical infrastructure industries. NC4 Mission Center CTX enables secure information sharing and collaboration among trusted groups.
- Soltra Edge - A standards (STIX/TAXII) -based solution pioneered and developed by the FS-ISAC and DTCC. Soltra was acquired by NC4 in November of 2016.

For the **enterprise**, including corporate risk management, the CISO, threat intel groups and SOC analysts, CDN improves internal effectiveness and efficiency in dealing with cyber threats.

Automation Action Principles

CDN employs a variety of operational modes to adapt to diverse cybersecurity organizations, processes, and cultures. These include manual mode, semi-automatic "human-in-the-loop" mode, fully automatic, parallel or hybrid mode. These modes include simulation capability as well as audit and log capability.

CDN Dashboard

CDN provides participants an operational dashboard that allows them to see the results of community oriented triage and other activities relating to cyber threats.

Participation

Critical infrastructure community members can join the Early Adopter Program. You must be a Soltra Edge customer and must actively engage and participate with other members. NC4 will be limiting the number of early participants. Current Soltra Edge customers will receive priority.

Cost

The Soltra Edge solution costs $15,000 per year. Early pricing of $11,000 for the first year is available until August 15, 2017. The cost of the basic CDN Network is expected to be around $5,000 per year with production operations beginning in 2018.

Join Now

Community Members and Security Solution Vendors should contact us by e-mail at CDN@NC4.com to participate in the program.

Learn More

To learn more about CDN visit www.nc4.com/pages/cdn.aspx.

Schedule and Timing

NC4 intends to rollout the Cyber Defense Network over the next 12 months in three phases with the first 2 phases being rolled out during the summer and fall of 2017.

Phase 1: Community Triage - This phase includes the ability for members to receive STIX/TAXII based threat indicators as well as for members to manually create new threat indicators through a cloud portal, or through an on-premise Soltra Edge solution. Extraction capabilities facilitate creation of new threat objects based on emails, etc. Additionally, further augmented information from the trusted community along with NC4 supplied data enrichment will facilitate the triage process.

Phase 2: Enterprise Level Automated Triage-Based Notification - This phase leverages an on-premise Soltra Edge engine to triage incoming threats for human analysts (threat intel groups, SOC analysts), or actions improving the speed, effectiveness and efficiency of both groups.

Phase 3: Enterprise Level Automated Triage Based Action - This phase deploys the intelligent action integration into a variety of leading security solutions including: SIEMS, orchestration and automation solutions, and trouble ticket solutions.

REVOLUTIONIZING
SAFETY & SECURITY

NC4®
100 N. Sepulveda Blvd.
El Segundo, CA 90245
877-624-4999 | 310-606-4444