Service Definition

Table of Contents

1   INTRODUCTION

This Service Definition is subject to all terms and conditions of the Service Order to which it was attached. This Service Definition describes and contains additional terms that apply to Synoptek's Network Anomaly Security (the "Service").

The service definitions found herein reflect Synoptek's standards at the time the Service Order(s) was issued. Synoptek reserves the right to change any particular standard herein to reflect Synoptek's current best practices or industry standards at its sole discretion with or without notice.

2   SERVICE OFFERING

Synoptek's Security Services are designed to defend and minimize your attack surface. Our Security Services include threat detection, investigation, and reporting. Our security personnel will continue to advise on ever changing threats and recommended actions.

As a network-based solution, Synoptek's Network Anomaly Security Service couples a physical monitoring device on your network with Synoptek's cyber-security staff to iteratively learns your pattern of life for every network, device and individual user, correlating this information in order to spot subtle deviations that may indicate in-progress threats.

Key Features:

- Detection of emerging cyber-attacks using sophisticated self-leaning mathematics
- Signature-free probabilistic approaches allow detection of anomalies and abnormal behaviors
- Real-time alerts as threats arise
- Powerful visualization platform enables analysis of internal and external threats
- Network appliance plugs directly into infrastructure and does not require software roll-out

2.1   SOLUTION PURPOSE

Our team of threat analysts are analyzing the behavioral statistics continuously in detection of threats for our customers. They quickly hone in on the root cause and severity of detected anomalies, formulate findings into actionable insight and predict whether any anomalous network behavior is significant enough to cause alarm. Synoptek Threat Analysts can detect anomalies within customer networks, including previously unknown "zero-days" and, provide visibility of emerging threats. This shortens the time it takes for containment of threats and limits the extremity and cost of an attack when (not if) it occurs.

2.2   HOW IT WORKS

Synoptek utilizes a Cyber Intelligence Platform (CIP), which is a network solution for detecting and investigating emerging cyber-attacks that have evaded network border defenses. By applying advanced mathematics to model behaviors in your enterprise, CIP is an advanced monitoring solution that detects anomalies in your organization's complex computer and user activities. CIP's mathematical approaches do not require signatures or rules and so can detect emerging 'unknown unknown' attacks that have not been seen before.

CIP is delivered as an appliance that takes passive feeds of raw network traffic from the centers of your networks. Once connected, the platform immediately begins using a range of mathematical approaches to create numerous models of behavior for each individual user, network, and machine. CIP produces Network Anomalies with a computed threat probability.

CIP's self-learning mathematics initially take 2-4 weeks to become effective and continue to learn on an ongoing basis - constantly updating as the organization evolves.

Creating powerful 'pattern of life' models of every individual and device on your network allows CIP to detect even subtle shifts in data access behaviors, communications or use of technology. This may indicate that an individual's credentials have been stolen and their device compromised, or that a disaffected person is acting maliciously.

Examples such as network reconnaissance, traversal, unexpected downloads from unusual internet domains, intranet or file system cloning, sensitive data logins from a new device and location, unusual applications and protocols, or a change in pattern of information uploading are all detectable through mathematical modeling. These activities may be worthy of investigation if they represent a significant departure from normal behavior.

3   INSTALLATION AND CONFIGURATION
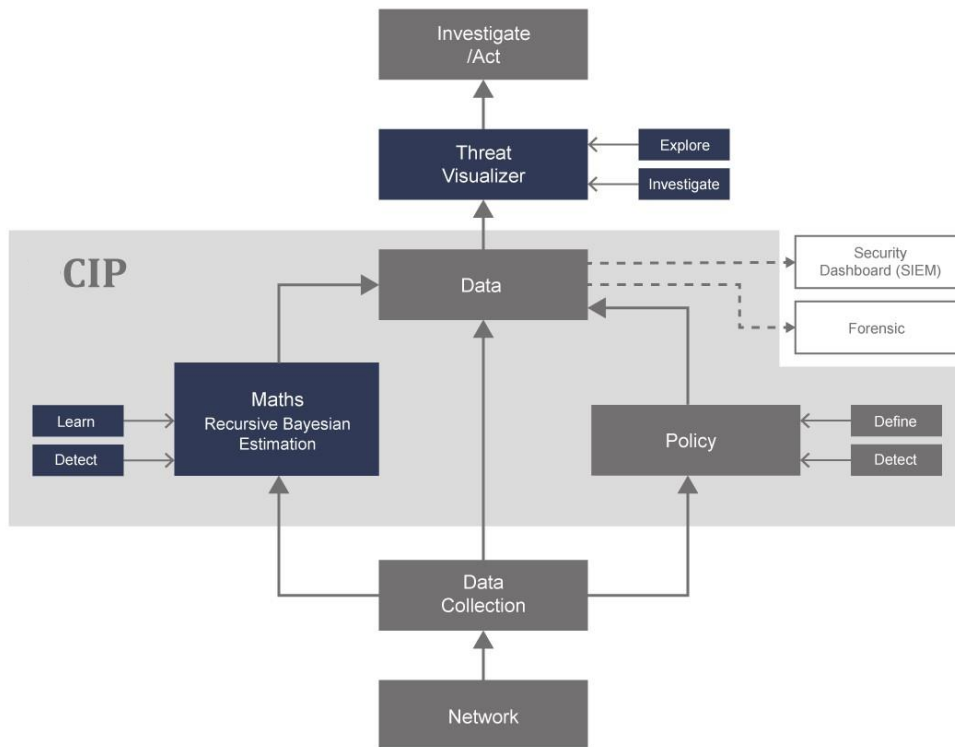
3.1   ENVIRONMENTAL REQUIREMENTS AND INSTALLATION

CIP consumes raw network traffic, collected by either:
• port spanning your existing network equipment
• inserting/re-using an inline network tap
• accessing any existing repositories of network data

For most customers a single appliance takes up 1U of rack space per physical location.

3.2   INSTALLATION

Synoptek installation can be scheduled to be performed within a 4-hour service window and is non-disruptive to your systems.

3.3   EASY TO SCALE

A single CIP appliance can take multiple inputs of network traffic and cover up to tens of thousands of individual machines, depending on peak traffic volumes. Multiple CIP appliances can cluster to cover geographically distributed networks, eliminating the need to move large volumes of data around your network.

3.4   INITIAL CONFIGURATION

CIP's self-learning capabilities initially take 2-4 weeks to become effective and continue to learn on an ongoing basis - constantly updating as the organization evolves. The first weekly Threat Intelligence Report will be delivered within 10 business days from the date of installation. Initial reports will have a low signal to noise ratio, or low percentage of actual versus perceived threat. Ongoing tuning, which is included in the service, will progressively provide improvement in report data quality.

4   THREAT INVESTIGATION AND ANALYTICS SERVICE

Synoptek's Security Analysts are experts in defense, intelligence and interpreting anomalous activities around probable threats. This process includes analyzing traffic patterns of data as it enters, exits as well as circulates within your network. Threat analysis of this kind is often like finding a needle in a hay stack and requires skills and understanding far beyond the normal abilities of most network professionals. No automated technology can achieve complete accuracy, thus our service couples great tools with the insight of experienced threat analysts.

Our manual threat intelligence service involves analyzing the network anomalies from the CIP and investigating the high probability anomalies that may be indicative of a threat. For every high-probability anomaly detected, our analysts draw on their expertise, external sources of intelligence and the context of the network before presenting an informed and considered explanation of the threats faced. Investigative work is delivered in two ways: a) a comprehensive weekly Threat Intelligence Report (see Appendix A) of discovered threats classified and scored in terms of severity (see Appendix B), in conjunction to recommended actions; and b) notification of incident alerts that are high-probability anomalies following our P2 SLA.

4.1   SERVICE LEVEL

Synoptek Security Analysts will continuously monitor for threat indicators as presented by the CIP. Threat indicators will be assessed, and categorized into three levels of severity. The most severe threats are categorized with the moniker "Board Level Advisory" (BLA), and for those Synoptek will gather and document the necessary context and activity logs required to build the weekly Threat Intelligence Reports (See below). See Appendix B for Threat Indicator levels and definitions.

For all Threat Indicators, Synoptek will deliver once-weekly Threat Intelligence Reports (see Appendix A) providing the necessary context and activity data required to investigate such threats. Notification will be provided in writing to the customer's designated alert contact.

4.2 SYSTEM TUNING

Synoptek is responsible for detecting network anomalies and sorting out the bad traffic patterns from among the vast false positive traffic patterns that show up on our screens hourly. As a result, Synoptek has its interests aligned with those of its clients to reduce false positives and increase the signal to noise ratio of potential threats. An initial 2-4 weeks of tuning are required before the system becomes effective. Ongoing tuning, which is included in the service, will progressively provide improvement in report data quality.

4.3 PREREQUISITES

This service requires bundled subscription to Synoptek's Security Analyst.

5 TECHNICAL SUPPORT AND MONITORING

Synoptek will provide support for troubleshooting and resolution for the CIP server that will be monitored by Synoptek's Security Services Team. In addition, a web-based ticketing system to support tickets, track, and provide correspondence for any support related issue. All communication will be handled through the Ticket System.

Synoptek will remediate issues related to the CIP server, identified either via monitoring and notification, or those initiated through contacting the Service Desk. In both cases, a service ticket will be created and prioritized based on severity. The service desk will attempt to resolve the issue remotely, escalating to level 2, then level 3 engineers as required. If the issue cannot be resolved remotely, a field technician will be dispatched.

6 SERVICE EXCLUSIONS

Synoptek's Network Anomaly Security Service is an excellent addition to an organization's strategy of defense in depth. Some threats attack users and systems in ways that may not immediately present any detectable network traffic. As a result, this service alone cannot detect all threats and is best used in conjunction with a SIEM, DNS filter, and other protective measures. Not all threats create anomalous network activity and thus will not be detected and reported. Furthermore, this service differs from a threat prevention service in that it is meant to detect the threats that manage to bypass your other security systems and protective barriers. While this service cannot prevent any intrusion, its utility is in early detection, and investigation.

Note that while access to the CIP is limited to Synoptek staff, it may be presented to customer staff during threat intelligence meetings as well as when presenting critical threat information.

7 PHYSICAL APPLIANCE FAILURE

In the event of an appliance failure, the following shall apply:

- If a replacement or software reinstallation is required, Synoptek will assist the customer in restoring their configurations and data from their backups;

- During an installation's outage it will not be able to monitor the customer's network for anomalous behaviors and TIR's will not be generated;
- Synoptek's lead time to provide a replacement is between 24 – 48 hours from verification that a replacement/repair is required; and
- The difference between replacement/repair verification and the replacement appliance delivery is 10 business days.
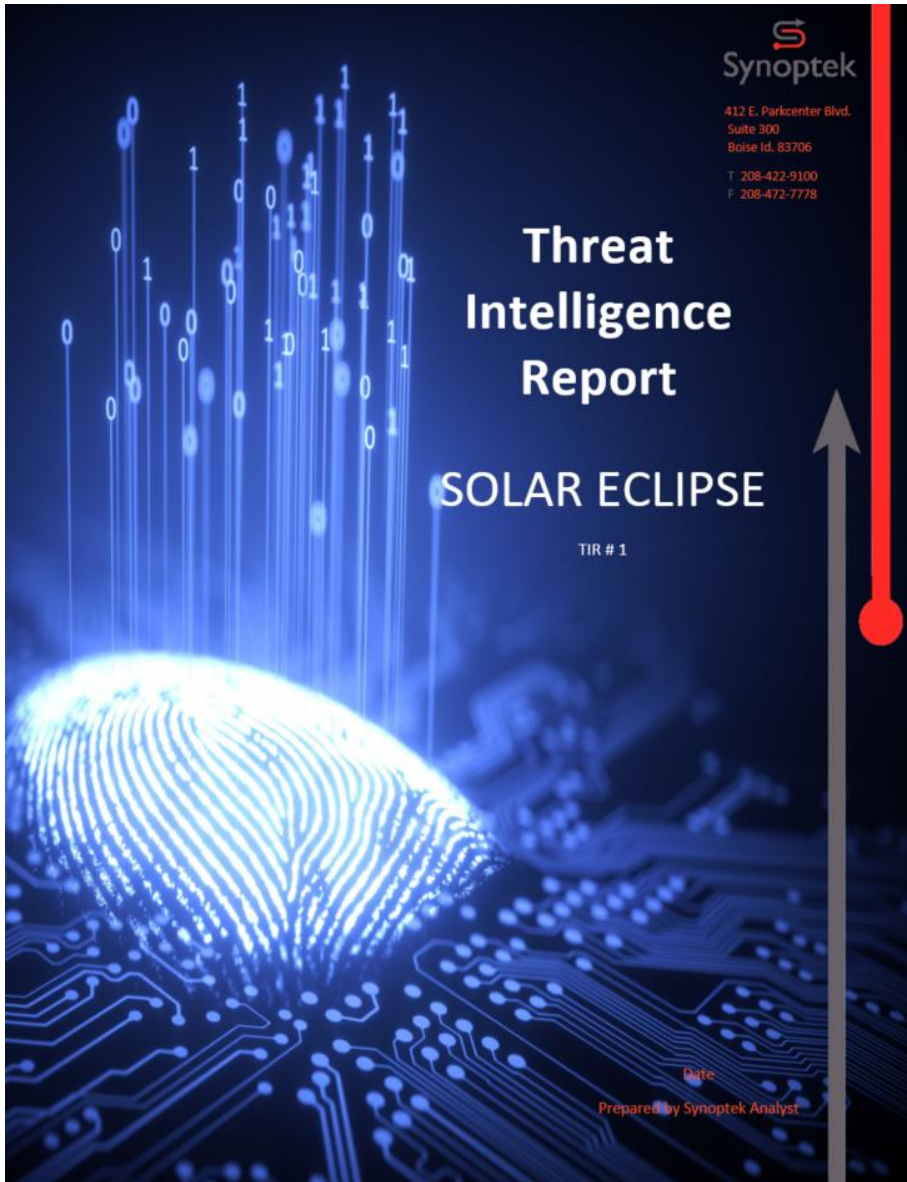
8   POINTS OF CONTACT – GENERAL SUPPORT

Email: SecurityServices@Synoptek.com

Telephone: 888-796-6783

Sample Threat Intelligence Report

(Image links to externally hosted download of Sample Report)

APPENDIX B

Threat Indicator Levels and Definitions

Severity Icon	Description
	Severe Threat Any incident (ongoing or detected) that has been determined to have the potential for severe commercial, legal and/or operational impact. Severe Threats are those that should be raised to the executive level immediately as data and/or resource confidentiality, integrity and/or availability are at significant risk.
	High Threat Any incident (ongoing or detected) that has been determined to have the potential for moderate commercial, legal and/or operational impact. High Threats are those that could indicate malicious use of corporate resources, are active infections or are otherwise placing the organization's data and/or resource confidentiality, integrity and/or availability at moderate risk.
	Caution Advised Any incident (ongoing or detected) that has been determined to have the potential for low or minimal commercial, legal and/or operational impact. Incidents categorized as Caution Advised are those that could indicate a risk to the organization if not addressed. Caution Advised represents low to minimal risk to data and/or resource confidentiality, integrity and/or availability; however, if left unresolved, these threats could escalate to a higher severity.
	Policy Advisory Any incident (ongoing or detected) that has the potential to be a risk to the organization through failure to comply with organizational policies, such as BYOD compliance; bad security practice (sharing of passwords or accounts); data risk (uploading to third party data repositories outside of the corporate network), etc.