WHITE PAPER: SYMANTEC SECURITY INTELLIGENCE SERVICES

Symantec™ Cyber Threat Analysis Program

Program Overview

Symantec Cyber Threat Analysis Program Team

White Paper: Symantec Security Intelligence Services

Symantec™ Cyber Threat Analysis Program

Program Overview

Contents

Overview

One of the greatest challenges facing security organizations today is the ability to efficiently and cost effectively integrate products and services within existing network infrastructures, without disrupting established policies and procedures. The current economic downturn has also put additional emphasis on the cost of integration and the ability to leverage past investments while delivering enhanced security.

Cyber security threats aimed at corporations and government organizations arrive faster and are more sophisticated than ever before. Cyber incident identification, analysis, and response are often limited by an organization's view into the global threat landscape and a lack of validated cyber intelligence to substantiate an effective response. This can be exacerbated by the products, services, and resources an organization employs to defend its assets.

While a security professional's intent is to create both a proactive and reactive defense posture to mitigate cyber risk, their organization may lack access to the critical components and the intelligence necessary to meet this requirement. As threats evolve, even the intended functionality or configuration of a solution can add to this problem. These limitations can create a false sense of security and lead to compromises, which ultimately increase an organization's risk.

According to many independent sources, the sophistication, complexity and targeted nature of these attacks will continue to grow. Trying to determine where the next attack will come from is a daunting challenge and without effective intelligence, it can be a futile effort.

Symantec™ Cyber Threat Analysis Program

The Symantec Cyber Threat Analysis Program (CTAP) mitigates cyber risk with a comprehensive approach to threat identification, intelligence gathering and validation, and response to protect critical client information. The result is a highly customized solution that integrates multiple components that address the specific security requirements of customers.

CTAP is designed to integrate with your existing IT environment. This provides the opportunity to consolidate resources and introduce heightened security awareness while enhancing workflow that creates a more secure enterprise security model. The CTAP approach leverages and extends your current investments in both technology and human capital.

Delivering Effective Security Protection

The ability to implement a comprehensive threat mitigation strategy within any organization requires the correlation of data across disparate networks within the infrastructure. This correlation must incorporate credible and validated external datasets that identify threats while ensuring the integrity of the information for a decisive and efficient threat mitigation response. However, without skilled cyber analysts to integrate data from multiple sources and interpret findings, effective mitigations can be diminished. The Symantec Cyber Threat Analysis Program provides customers with access to an enhanced view of the threat landscape, supported by onsite subject matter experts and specialized tools to enact response. CTAP analysts leverage the Symantec™ Global Intelligence Network as well as the same proprietary tools and infrastructure that Symantec uses internally to detect, block and remove threats, resulting in increased protection for client networks and assets around the world.

CTAP analysts enhance situational awareness by creating a client-specific contextual landscape that is formed by integrating client-specific incident data, Symantec's global vulnerability and threat intelligence data, and open source data. This unique insight is then augmented with access to Symantec's internal proprietary tools and specialized infrastructure to enhance response capabilities. This correlation ultimately assists organizations in their understanding of both strategic and tactical cyber threats to create a comprehensive mitigation strategy to defend its networks. Work can be performed in a secure environment, and no customer data is removed, unless specifically directed by the client.

Proactive methodologies assist in delivering mitigation strategies to protect against today's sophisticated threats - both existing and new, unseen threats. The result? Enhanced protection from your network and technology investments. CTAP analysts have access to a wide range of detection technologies such as the Symantec distributed honeypot, spam, underground, P2P, and crawler networks. These automated technologies analyze system behaviors and network communications to detect and actively block threats.

Validate security threats

- Leveraging customer investment in existing detection technologies
- Help identify attacks that may have already occurred
- Provide incident analysis and briefings on threat dispositions
- Identify groups of bad actors
- Identify persistent methods and procedures of criminals and other cyber attackers

Block malicious behavior

- Provide proactive threat analysis
- Prevent attacks before they happen
- Harden the infrastructure to make it more difficult for attackers to get in, thus Increasing the cost to attackers so that they give up and go elsewhere

Remove the threat

- Provide countermeasure support and implementation guidance
- Support a decision matrix that outlines courses of action to defend against attacks
- Counter electronic espionage through data leakage remediation

This comprehensive program allows you to proactively define threats and take decisive action. CTAP ensures the confidentiality, integrity and availability of your networks, but also ultimately improves your situational awareness within the threat landscape in the face of critical events.

Sophisticated Tools Deliver Enhanced Analysis Capabilities

Symantec CTAP analysts leverage sophisticated tools via a proprietary remote interface with embedded toolsets and internal systems that enable Symantec CTAP analysts to quickly identify emerging cyber security threats, develop countermeasures, and enact solutions.

By integrating client data and public data with Symantec Cyber Threat Analysis Program intelligence, Symantec can help determine the true nature of an attack and/or the required mitigation steps. CTAP analysts have secure access to Symantec's proprietary cyber intelligence catalogs, research facilities, proprietary tools, and human capital, as well as the greater CTAP community on behalf of our clients. Examples include:

- Attack, vulnerability, and malicious code intelligence
- Phishing, spam, data leakage, spyware, adware, and virus intelligence
- Underground cyber economy and honeypot network intelligence
- Symantec's internal Infrastructure and toolsets
- Subject matter experts
- Related analysis and cyber-specific reports

Client Confidentiality and Sensitivity

Symantec recognizes the specific requirements expected by our clients in the delivery of CTAP services. Symantec offers a unique and special relationship with clients who implement CTAP services, which differ from traditional client/vendor relationships. CTAP analysts reside within the client's domain and work as part of their own teams using the Symantec internal tools and data to deliver an effective security platform.

While our clients are happy to have this level of partnership, they are not necessarily open to advertising this. Symantec understands this and is very conscious in protecting and ensuring the confidentiality of our CTAP clients. The work we perform is sensitive and so are the environments we work in. CTAP analysts are part of a community of CTAP analysts and are trained to respect each client's confidentiality. They do not share client data or information, but they do help propagate better mitigation strategies across the team. We are committed to protecting our clients in every way.

Cyber Security Expertise

Symantec provides both on-site and remote Accredited Symantec Cyber Analysts (AISCA^{TM}). The CTAP Analyst Training Program leverages Symantec's internal training and education core, as well as third party sources in an effort to enhance the knowledge and capabilities of individuals hired within the program. Completion of the course indicates comprehension of the courseware and topics and identifies each individual as an "Authorized Symantec Consultant" and an "Accredited Symantec Cyber Analyst".

These security experts provide a range of customized analysis, reporting, and response actions to meet the unique solution requirements of each client. Symantec analysts leverage proprietary capabilities and have access to in-depth analysis, technology (malware, behavioral and heuristics engines) and resources. One example is the Symantec Technology and Response (STAR) organization. STAR is a global team of intrusion detection experts, security engineers, virus hunters, threat analysts, and technical support professionals that provide fast and accurate analysis of security data-24 x 7-to help Symantec customers guard against complex Internet threats and other security risks. Leveraging the output from this organization and others results in more timely protection for CTAP customers.

Experience

Symantec CTAP Analysts are highly skilled subject matter experts, often possessing a minimum of 6-8 years of cyber security experience. Analysts must meet stringent requirements in order to be considered for CTAP, and undergo ongoing training to enhance their capabilities. CTAP analysts work together to propagate better tactics, techniques, and procedures for each client. CTAP analyst teams focus on specific aspects of cyber defense and response across four key areas of discipline:

1. Cyber Intelligence Analyst
2. Network Operations Analyst
3. Forensics Analyst
4. Malicious Code Analyst

Symantec works with your organization to assess the specific tasks and skill sets required to meet your needs. The following are representative examples of what can be delivered within each discipline. It is not uncommon for an analyst to possess abilities across multiple skill sets.

1. Cyber Intelligence Analysis

CTAP Analysts will assist Client in discovering, tracking and reporting on global network events of interest that are identified by Client and/or Client systems, utilizing available cyber intelligence analysis data and methods.

Research available Symantec and Client-provided cyber intelligence data on an ongoing basis and, at Client's request, report on impact or attribution of such cyber intelligence data for Client.

- Analyze Client network logs, in conjunction with Client's security operations team, in an effort to assist with identification of possible threats to Client's network security.
- Advise on mitigation and remediation of threats to Client's network security, and coordinate with other analysts and data source catalogs for further action as appropriate.
- Assist in review of Client information security program strategy, policy, and processes and recommend modifications to such strategy, policy and processes to enhance Client's security posture.
- Provide technical expertise to Client in identifying, modeling and reporting on emerging threats.
- Provide documentation to support Symantec activities described above where necessary and requested by Client. Such documentation may include graphical representations of information when mutually agreed upon by the parties.

2. Network Security Operations Analysis

CTAP Analysts will assist with ongoing Client operational security analysis, leveraging generally available best practices in controls, audit and event management.

CTAP Analysts may perform the following task(s) as Network Operations analysts:

- Collect attack and investigation metrics and trending data from the Symantec Global Intelligence Network (GIN) and Client-provided information sources.
- Track trends associated with characteristics of network threats or actors and perform network nodal analysis on the Client network infrastructure to determine security gaps and network configuration deficiencies.
- Prioritize identified threats to Client's network, managing risks associated with such threats, and assisting with Client response to such threats.
- Develop graphical representations of social and physical networks associated with specific network threats or actors.
- Assist with development of Client strategies and network architectures to facilitate creation of secure Client cyber environments.
- Provide leadership to cross-functional teams responsible for responding to network incidents and providing remediation against attacks.
- Provide information regarding Client's network operations to assist with various security assessments and auditing engagements as requested by Client.
- Develop mechanisms to intake data feeds from data sources to enhance overall situational awareness.
- Provide documentation to support Symantec activities described above where necessary and requested by Client. Such documentation may include graphical representations of information when mutually agreed upon by the parties.

3. Forensics Analysis

CTAP Analysts will support Client's forensic investigation efforts by providing forensics analysis for Client's internal use related to internal IT environments, systems, and infrastructure.

CTAP Analysts may perform the following task(s) as Forensics analysts:

- Assist in investigating and analyzing Client computer network intrusions.
- Assist in the collection and preservation of evidence associated with Client computer network intrusions following industry best practices and established procedures.
- Assist in the performance of forensic analysis of compromised systems, including identification of malicious code, methods of compromise, threat attribution, and data extraction techniques.
- Provide guidance for the continued development and implementation of a Client computer security incident management program. Such guidance shall be based upon information collected by Symantec as part of the investigation and analysis of Client computer network intrusions.
- At Client's request, provide reporting and analytical support on information security trends, standards, concepts and solutions.
- Provide documentation to support Symantec activities described above where necessary and requested by Client. Such documentation may include graphical representations of information when mutually agreed upon by the parties.

4. Malware Analysis

CTAP Analysts will investigate and review malware and assist Client in signature development, identifying hostile actor methodology and developing mitigation scenarios.

CTAP Analysts may perform the following task(s) as malware analysts:

- Conduct a behavioral and code-based review of items identified as possible Malware.
- Reverse engineer items identified as possible Malware, including protocol disassembly and reconstruction.
- Verify Malware attack vectors and testing potentially impacted security controls.
- Reverse engineer new vulnerabilities in order to build counter attack signatures against known and unknown threats.
- Research emerging malware capabilities and delivery techniques and assist with integration of appropriate countermeasures and mitigations into Client processes.
- Provide documentation to support Symantec activities described above where necessary and requested by Client. Such documentation may include graphical representations of information when mutually agreed upon by the parties.

CTAP Intelligence Catalogs, Infrastructure, and Tools

CTAP analysts have secure remote access to many of Symantec's internal systems and data repositories through the CTAP Remote Interface. This includes global threat intelligence and vulnerability data spanning the last 20 years. These systems represent more than one billion dollars of investment in cyber security focused capabilities. These systems are web accessible and have a myriad of embedded tools developed over the last two decades. CTAP Analysts utilize this proprietary environment for client-specific research, analysis, and proactive activities.

CTAP analysts typically reside onsite at the client. Depending on the client's requirements, multiple onsite analysts may be paired with other CTAP resources resident at a Symantec facility as part of the solution requirement. Analysts do not remove sensitive client data from the client's networks to perform analysis unless directed by the client. This does occasionally occur in the case of malware analysis and forensics analysis.

Sample graphic representation

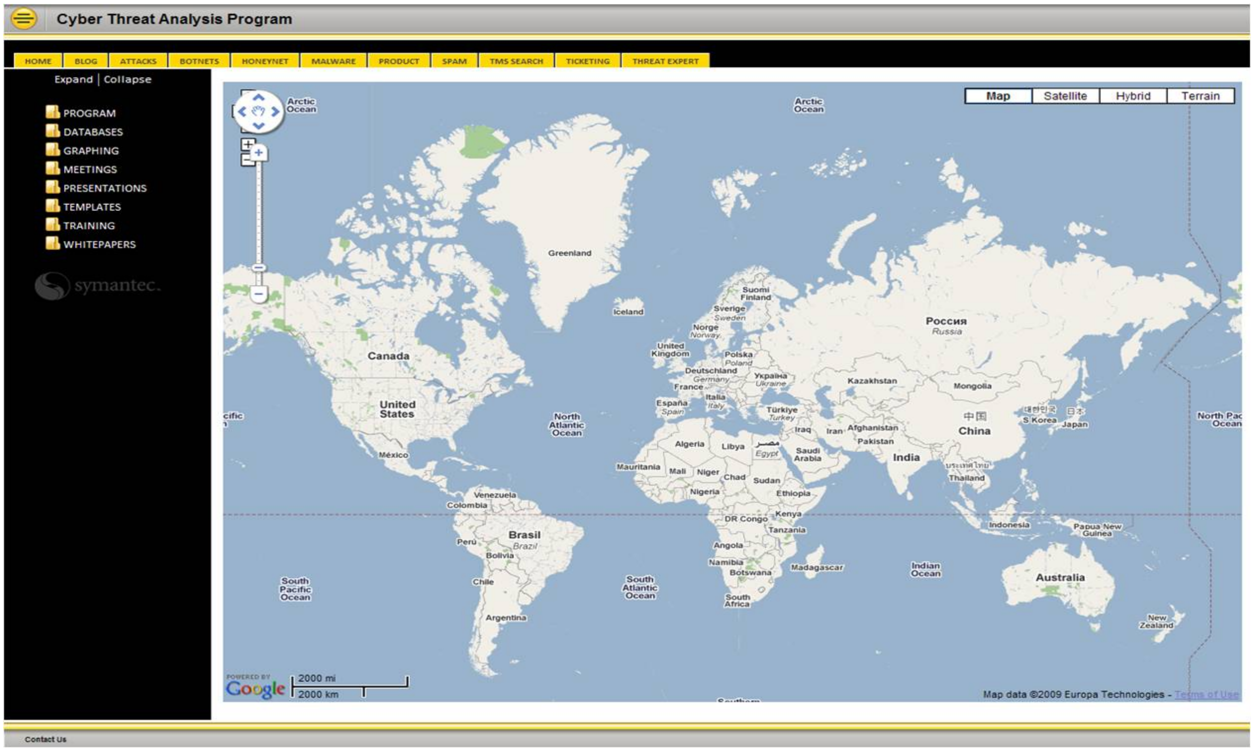

Figure 1: Symantec Cyber Threat Analysis Program Remote Interface

Sample Global Intelligence

The following are some examples of Symantec's Global Intelligence Catalogs and the associated data sets available to an analyst.

Pro-active Threat Intelligence:

- Protocol
- Source and destination IP address
- Source port and destination port
- Date/time of attack
- Type of attack
- Frequency of attack
- Number of events
- Targeted system
- Associated IDS/IPS signatures
- Associated malicious code
- Associated vulnerabilities

Attack Intelligence:

- Server names
- IP addresses
- IRC channel names
- Server passwords
- Drop site information
- Channel passwords (if any)
- IRC nicknames in use
- Any user information that is not part of the IRC protocol
- Port numbers trying to connect
- Record of all DNS queries
- Timestamp of connect
- MD5 hash of sample

SPAM/Phishing Intelligence:

- Spam zombie IPs
- Email spam source IPs
- Email spam signatures
- Email spam samples
- URLs in email spam
- Email phishing samples
- Email phishing attacks/campaigns

Reputation Intelligence:

- What percentage of sites host malware
- Breakdown of sites by types of malware
- How many sites and which ones host a specific threat
- What viruses exist in various malicious binaries
- When a site was infected and how much the infection has spread

Command and Control (Botnet) Intelligence:

- Identify C&C and Botnets
- Observed testing of new bonet technologies

Summary

To protect against the growing number of targeted attacks, organizations must react and respond immediately with the proper knowledge, experience, and data. Additionally organizations must have access to new and unforeseen threat intelligence by incorporating mechanisms to collect over the horizon intelligence. Symantec provides the most comprehensive and proactive line of defense available against cyber threats. The Symantec Cyber Threat Analysis Program provides the capability to furnish customers with cyber intelligence data that is truly global, practical, and applicable to each customer's defense posture.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our website.

Symantec World
Headquarters
20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

7/2009 20050478