SOLUTION BRIEF

Advanced Threat Assessment

A Symantec Proposal

Symantec™

Executive Summary

Problem

Building cyber security is more than just deploying a technology. It requires the right security measures in the appropriate configurations, along with policies and user awareness. Security leaders often need to balance between security solutions and policy enforcement, on one hand building security controls against the latest threat, on the other maintaining productivity in the organization.

Objectives

The objective of the Advanced Threat Assessment is to take a proactive stance in uncovering threats in the organization, understand where gaps have been exposed and potentially exploited by malicious actors, and help you create a plan to address them. This free service from Symantec or certified partners is purely on a monitoring basis, maintaining full visibility into security issues within the organization without impacting the productivity of the workforce. The approach is as follows:

- **Assess** – Identify security risks and rank them according to level of severity. These are then correlated with current security investments in place to highlight gaps in coverage and/or effectiveness.
- **Analyze** – Perform root cause analysis to identify the source of the problem. In the case of security breaches, investigate and report so you can remediate quickly and ensure the incident is contained.
- **Resolve** – Recommend process, technology, or user awareness changes needed to close the existing gaps and strengthen the existing security posture. Rank the roadmap to prioritize the security investments.

Why is this Critical?

Traditional risk or vulnerability assessments focus on answering the question, “What could happen to your organization?” This means the breach has not happened yet, but there is an exposure of this weakness.

The Symantec Advanced Threat Assessment poses a new question: “What has already happened, or happening, to the security of your data or network?” This approach focuses on incidents that have already occurred to which your technology investments have not effectively alerted you. This is common in today’s security landscape – and the last thing CISOs want is to buy another security solution that is only partially effective. They need visibility and insight into the operational efficiency of security operations before they can know what to fix in their organization. Therefore taking an active security response and forensic approach to advanced threats has become critical.

Scope of Assessment

The Advanced Threat Assessment focuses on identifying threats not fully addressed by current security investments. It harnesses sophisticated technology to identify weakness and gaps in architecture and security practices. The purpose is to uncover the existence of such gaps and help organization to gain a higher level of visibility into them.

The three major areas of Advanced Threat Assessment:

1. **Forensics of Malware Infection**
2. **Identifying Indicators of Compromise**
3. **Security Validation**

Forensics of Malware Infection

Harnessing the combination of the threat intelligence that comes with Symantec Security Analytics, the ATA can identify both known malware and potentially threatening content that is lurking within the organization. Beyond just identifying the malware, the objective is to perform a root cause analysis that includes the following tasks:

- Look for the origin of the malware
- Identify the background of the malware
- Identify the extent of the malware
- Identify the behavior of the malware
- Identify the damage the malware inflicts

Identifying Indicators of Compromise

The Indicators of Compromise track finds indicators of an intrusion. Sophisticated attacks that successfully penetrated the organization are usually the result of exploiting unknown vulnerabilities, or a combination of poor security practices, social engineering, or configuration gaps. One purpose of the assessment is to identify threats within the organization that mainstream technologies such as SIEM (security information and event management) and NIPS (network intrusion prevention systems) failed to identify.

This is achieved by understanding what is abnormal in the organization through Symantec's best practice approach and Security Analytics' anomaly detection capabilities. This is particularly for infections that occur outside of the organization's security perimeter, such as USB infections or infections outside the company's network.

Security Validation

The last assessment area identifies security gaps that are not commonly known due to lack of visibility on the network. Often, CIOs do not effectively plan their security roadmap because of this lack of visibility. Security gaps often bring about loopholes that allow attacks to occur.

Security policies are very useful as they help clarify the organization's security culture; the use of Symantec Security Analytics helps to validate that culture.

Security Validation also verifies whether security technologies and process are working to protect the organization, supports compliance and auditing, and identifies security gaps. Examples include:

- Security policy violation
- Network visibility
- Threats from encrypted traffic
- Data loss use case
- Network misconfigurations
- Gaps in security strategy

Assessment Framework

The ATA framework is composed of three phases:

- Understanding the environment
- Deploying Security Analytics (Appliance, Software or Virtual Appliance)
- Preparing reports, including the Security Analytics Risk and Visibility Report

Deploying Security Analytics

Install Security Analtyics at an organization's egress point (generally less than an hour for deployment and setup)

Security Analytics records network traffic (a week or more, depending on scope of assessment)

Generate Risk and Visibility Report and assess results (2-3 days)

Review key findings from report with customer (1-2 hours depending on scope of results)

Information is securely erased, appliance returned to Symantec (1 hour)

Understanding the Environment

Meetings with key stakeholders are conducted to understand the environment and the key findings are outlined in the report:

- **CISO** – Understanding the security roadmap of the organization (e.g cloud for business, acquisition of technology, renewal of architecture, latest incidents) and building the use case around the concerns and directions.
- **Security Manager** – Understanding the security policies and culture of the organization, the incident response process, and outstanding incidents that needed root cause analysis.
- **Internal Team (Business, Operations)** – Identifying key assets and compliance requirements of business operations, key concerns to productivity, or other company-related information.

Deploying Security Analytics

Ideally, Security Analytics is deployed at the egress point of the organization, either as an appliance, software or a virtual appliance. This is the gateway where all the employees access the Internet. If the organization has more than one exit point, another ideal location may be an exit point that the customer has that the CISO had identified.

An architecture discussion is conducted to determine the best position to deploy Security Analytics to ensure maximum visibility.

Preparing Reports

After sufficient traffic is captured, the Risk and Visibility report is automatically generated from Security Analytics and combined with other details found during a review of captured traffic, alerts, root cause analysis and anomaly detection. This is then shared with the customer (SecOps, CISO, or who the customer identifies as critical stakeholders). The report will highlight what security measures are working effectively, identify existing gaps, rank the most critical threats, and list recommendations around the threats found.

Boundaries and Constraints

The following are the limitations of the activities of an Advanced Threat Assessment:

- It does not provide a performance assessment for the entire organization: If the organization has more than 1 egress point, the assessment is based solely on one egress point. If further assessment or an official POC is required, Symantec will discuss that with the customer.
- This is a threat assessment and not a consultative governance assessment of the organization. Therefore it is not based on all the business units and critical assets of the organization. If an active, ongoing threat is identified, Symantec offers dedicated, in-depth Incident Response services and proactive Threat Hunting exercises. Options will be discussed with the customer.
- The default scope of the assessment does not extensively examine encrypted traffic such as SSL or other encryption that the organization wants visibility into. However, the assessment will reveal the extent

“

...using root cause analysis from Symantec, we were able to pinpoint how the exploit occurred, understand the full scope of the problem, and completely prevent that exploit from ever happening again...”

of encrypted traffic crossing thenetwork. If encrypted traffic visibility is needed, a Symantec SSL Visibility Appliance can be deployed as part of an extended assessment.

- The activities listed in the Scope of Assessment (above) are based on best effort, depending on the information available in Security Analytics at the time of capture and the timeline given to Symantec.
- Information within Security Analytics will be kept protected. In the event the customer wants additional security to ensure that the hard disk is destroyed, the customer may elect to purchase the hard disk from Symantec.

Advanced Threat Assessment (ATA) Case Studies

USE CASE #1: Security Incident Response and Resolution

Security incident response involves quickly analyzing, identifying, and resolving cyber-attacks and breaches. It remains the most popular use case for using Security Analytics.

Security Incident Response at a Major Online Retailer

A large online retailer built its security operations center and incident response process around Symantec Security Analytics. They use it to identify malicious activity inside and outside the network, to pinpoint all compromised systems through root cause analysis, and to conduct assurance testing on preventative controls by replaying attacks in a lab environment. Security Analytics provides much-needed context to alerts, including alerts from their new advanced malware analysis appliances.

USE CASE #2: Situational Awareness

Situational awareness is the ability to extract information from the environment, integrate that information with knowledge, extensive external threat intelligence sources, and use the resulting mental picture to anticipate future events.

Situational Awareness in the Military

An organization in the U.S. armed forces uses Symantec Security Analytics to monitor the Internet traffic of a large group of military analysts and ensure that their activities are consistent with each person’s role and security privileges.

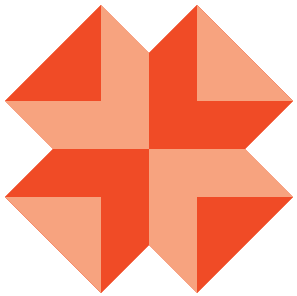
USE CASE #3: Continuous Monitoring

Continuous monitoring is the ability to capture, index, and play back all network data, and to provide administrators and security professionals with timely, targeted and prioritized information.

Continuous Monitoring at a Leading Financial Firm

A large investment bank uses Symantec Security Analytics to monitor more than a dozen locations and

“Symantec Security Analytics gives us the ability to look at historical records we didn’t have access to in the past. Now we can analyze what happened 15 minutes ago or 15 days ago – we can see exactly what led up to a security alert as well as what happened after the fact.”



to achieve complete visibility into network traffic, users and data. Security Analytics also provides context to information available from other security systems, including a third-party sandbox, Symantec ProxySG, and Symantec SSL Visibility. These capabilities have significantly reduced incident response times.

USE CASE #4: Data Loss Monitoring and Analysis

The ability to precisely identify data losses can produce major cost savings. Breach notification costs and regulatory fines are often proportional to the amount of data compromised in an attack.

Data Loss Monitoring at a Leading-edge Technology Company

A technology company with world-famous consumer electronics products uses Symantec Security Analytics to ensure that employees and contractors do not leak intellectual property, confidential business plans, or corporate financial information. They also use it to determine material impact when information leakage does occur.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world’s leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec’s Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world’s largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

19A163012_SB_ADVANCED_THREAT_ASSESSMENT_EN