HOSTWAY + SilverSky

Managed Security Glossary

AGENT In RADAR, the agent is an application used for gathering information about your application logs, system logs, application files, and registry files to see if any log entries have changed; used to monitor files formalicious events.

ALERTS Messages sent to the SilverSky SOC analysts or from them to the customer to warn of attacks to the customer's network or network device.

AUTHENTICATION The process of checking whether or not a user has permission to access an application, computer, or network.

BOTNET A large number of compromised computers that are used to send spam, viruses and denial of service atatcks

CDE Cardholder Data Environment - The cardholder data environment is comprised of people, processes and technology that store, process or transmit cardholder data or sensitive authentication data. The PCI DSS security requirements apply to all system components. In the context of PCI DSS, "system components" are defined as any network component, server, or application that is included in or connected to the cardholder data environment.

CERTIFICATES A digital document used for authentication and secure exchange of information on open networks such as the Internet and intranets. A certificate securely binds a public key to the entity that holds the corresponding private key. Certificates are digitally signed by the issuing certification authority and can be used for a user, a computer, or a service.

CVSS Common Vulnerability Scoring System - A standard measurement system used to calculate the severity of the vulnerabilities found on a system.

DDOS Distributed Denial of Service Attack

DEFENSE IN DEPTH Defense In-Depth is the approach of using multiple layers of security to guard against failure of a single security component.

DES Data Encryption Standard - An U.S. government approved cipher. It is easy to break in its simplest form, but used multiple times with key of at least 128 bits provides good security.

DHCP Dynamic Host Configuration Protocol - Allows you to configure connected network devices so they can communicate with other hosts.

HOSTWAY + SilverSky

Managed Security Glossary

DMZ Demilitarized Zone - In computer security, in general a demilitarized zone (DMZ) or perimeter network is a network area (a subnetwork) that sits between an organization's internal network and an external network, usually the Internet. DMZ's help to enable the layered security model in that they provide subnetwork segmentation based on security requirements or policy. DMZ's provide either a transit mechanism from a secure source to an insecure destination or from an insecure source to a more secure destination. In many cases, a screened subnet which is used for servers accessible from the outside is referred to as a DMZ.

ENCRYPTION Encryption means encoding data using a cryptographic cipher. Encrypted data can be read (decrypted) only by an authorized entity.

FIM File Integrity Monitoring - Verifies that program and operating system files have not been compromised.

FIREWALL Controls what data is allowed to enter through your network to connected network devices, such as computers, servers, and databases. Its security policy determines what traffic is authorized to pass in each direction.

GLOBAL BLOCK The rule that blocks IP addresses of computers that do not reside on your network from sending data to the NSA. These blocks are implemented across all SilverSky customers based on global security event activity.

IDPS Intrusion Detection System/Intrusion Prevention System. IDS and IPS systems detect and prevent attacks on your system.

IDS Intrusion Detection Service

INCIDENT Related security events that can be perceived as a threat to your network, prompting action by the StillSecure SOC analyst according to the incident handling policy established for that customer.

IPS Intrusion Protection Service - Stillsecure separates out the detection and protection service.

IPSEC Internet Protocol Security - Part of VPN that uses encryption and virtual IP addresses to ensure secure connections between machines on a network.

LOCAL BLOCK A rule that prevents IP addresses of machines connected to your network from sending or receiving information through the NSA.

HOSTWAY + SilverSky

Managed Security Glossary

LM / LMS	The StillSecure Log Management service (LMS) consolidates and organizes security log events from a myriad of network systems, devices, applications, and other tools, providing detailed visibility into the security of your network and bringing it into compliance with applicable regulatory information security mandates.
MULTI-FACTOR AUTHENTICATION	Process of confirming the correctness of a claimed identity through multiple factors. Something the user knows and something the user has. StillSecure uses RSA key fobs for multi-factor authenication of mobile VPN users.
NAT	Network Address Translation - It is used to share one or a small number of publicly routable IP addresses among a larger number of hosts. The hosts are assigned private IP addresses, which are then "translated" into one of the publicly routed IP addresses. NAT is often used for servers as an additional layer of protection.
NETWORK SEGMENTATION	The act of splitting a computer network into subnetworks, each being a network segment or network layer. Advantages of such splitting are primarily for boosting performance and improving security.
NSA	Network Security Appliance - The device installed on your network that collects and monitors network security information to keep your network secure from harmful local or global data that is sent to it. NSA can contain one or more managed security services that focus on different parts of your network (such as the firewall or network traffic).
OSSEC	Open Source Security. The host-based intrusion detection software that is the underlying tool for the File Integrity monitoring managed service.
OWASP	Open Web Application Security Project - Open source guidelines for tools and software to keep Web sites secure.
PCI DSS	Payment Card Industry Data Security Standards
SIGNATURES	Rules that consist of pre-configured and pre-defined attack patterns used by IDPS to locate threats to a network. The IDPS monitors network traffic for matches to these signatures. When a match is found, the system takes the appropriate action. Signatures are also used in file integrity monitoring to determine if an application or system file has been changed.
SOC	Security Operations Center

HOSTWAY + SilverSky

Managed Security Glossary

SSH	Secure Shell - Developed by SSH Communications Security, it is a standard for encrypted terminal Internet connections. SSH programs provide strong authentication and encrypted communications, replacing less secure access methods like telnet. SilverSky uses SSH as a secure remote access method used to manage the NSA and for auditing purposes to keep track of who logged into the NSA.
SSL	Secure Sockets Layer - Protocol developed by Netscape to provide encryption for commercial transactions data that should be protected while traveling over the Internet, like credit card numbers. SSL uses httpsprotocol. Before using SSL in commerce, you'll also need to get is a certificate from a Certificate Authority.
SSL CERTIFICATE	Digital ID used for SSL transactions. It includes owner's public key, the name of the owner, the issuer, hostname, and the expiration date.
SYSLOG	System Logging - An alternate method (to agent software) for collecting data from log files; used to monitor files for malicious events.
VLAN	Virtual Local Area Network.
VPN	Virtual Private Network
VULNERABILITY SCANNING	A vulnerability scanner is a computer program designed to assess systems, networks or applications for weaknesses.
WAF	Web Application Firewall - The SilverSky Web Application Firewall (WAF) service protects your Web-based applications from attack by monitoring input, output and access attempts, and blocking any malicious activity.