CompuSource Systems, Inc.

Core Compliance

Core Compliance Package Overview

DataSure24

A FREED MAXICK TECHNOLOGY COMPANY

www.css4cu.com • (800) 295 - 9100

Table of Contents

Core Compliance Overview 3

Asset Discovery 4-5

Vulnerability Assessment 6-9

Availability Monitoring 10

Intrusion Detection 11-12

Incident Response 13

Additional 14

Overview

CompuSource Systems, Inc. has partnered with it's long term technology partner DataSure24 to provide Cyber Security Services using the award winning AlienVault cyber security software. CSS's Core Compliance package offers a simple and effective cyber security solution, for small-medium size organizations to meet areas of compliance, and detect and respond to threats and when they emerge. Once the technical requirements are met at each of the customer locations, we will begin the installation of our specialized software ready for operational use within 1-2 weeks. The following services are included in this package:

Asset Discovery - Active and passive scans will discover all assets on the network as well as their operating system, running services, and more. An actively updated asset inventory will be maintained that will give a detailed view of related security events, vulnerabilities, and availability.

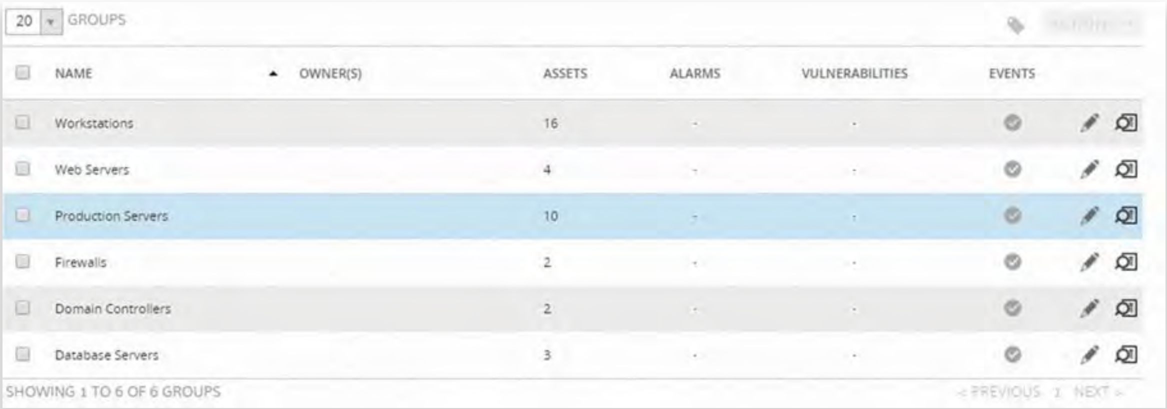
Vulnerability Assessment - A vulnerability assessment will be completed to detect vulnerabilities on a system and its software. The scan will be reviewed by analysts and a detailed report will be completed to prioritize any remediation action-necessary and improve security posture. After the initial assessment is completed monthly scan will be completed and a report will be provided.

Intrusion Detection - Through our 24x7 Security Operation Center (SOC) DataSure24 will provide around the clock monitoring with the ability to detect and analyze malicious activity on your network.

Availability Monitoring - Core assets and their services will be monitored for their availability to ensure uptime.

Incident Response - Any alarm with a risk level 5 or higher will have a 1-2 hour response time. Analysts will alert the CompuSource Technical team with details of the event and recommend course of action. An alarm with a risk level of 3-4 will prompt a notification within 48 - 72 hours. A monthly alarm report will be provided showing a breakdown of all alarms.

Asset Discovery



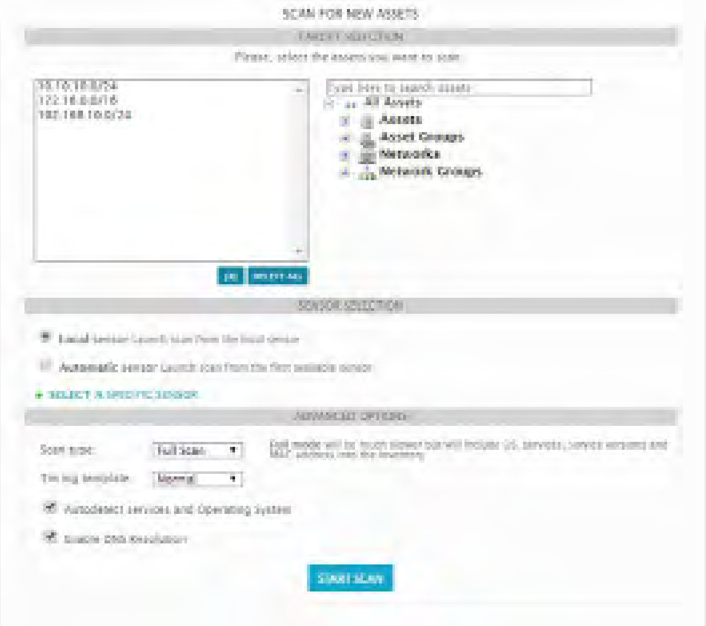
20 GROUPS

□	NAME	OWNER(S)	ASSETS	ALARMS	VULNERABILITIES	EVENTS
□	Workstations		16	-	-	✓
□	Web Servers		4	-	-	✓
□	Production Servers		10	-	-	✓
□	Firewalls		2	-	-	✓
□	Domain Controllers		2	-	-	✓
□	Database Servers		3	-	-	✓

SHOWING 1 TO 6 OF 6 GROUPS

This essential service allows discovery of all assets in your environment. Also, can discovery changes to assets in your environment. The above screenshot shows **asset groups**, with the below image detailing the scanning process taking place. The service scans a customer's network to find all assets attached to a customer's network. This may include workstations, web servers, firewalls, devices, tablets and more.

Asset discovery uses passive tools, such as passive operating system fingerprinting and passive service discovery. Active scanning is also utilized, to perform scheduled asset scans to discover any rogue assets existing on the network.



SCAN FOR NEW ASSETS

TARGET SELECTION

Please, select the assets you want to scan

10.10.10.0/24
172.16.0.0/16
192.168.10.0/24

SENSOR SELECTION

● **Local** sensor Launch scan from the local sensor

○ **Automatic** sensor Launch scan from the first available sensor

ADVANCED OPTIONS

Scan type: Full Scan

Full mode will be much slower but will include OS, services, service versions and MAC address into the inventory

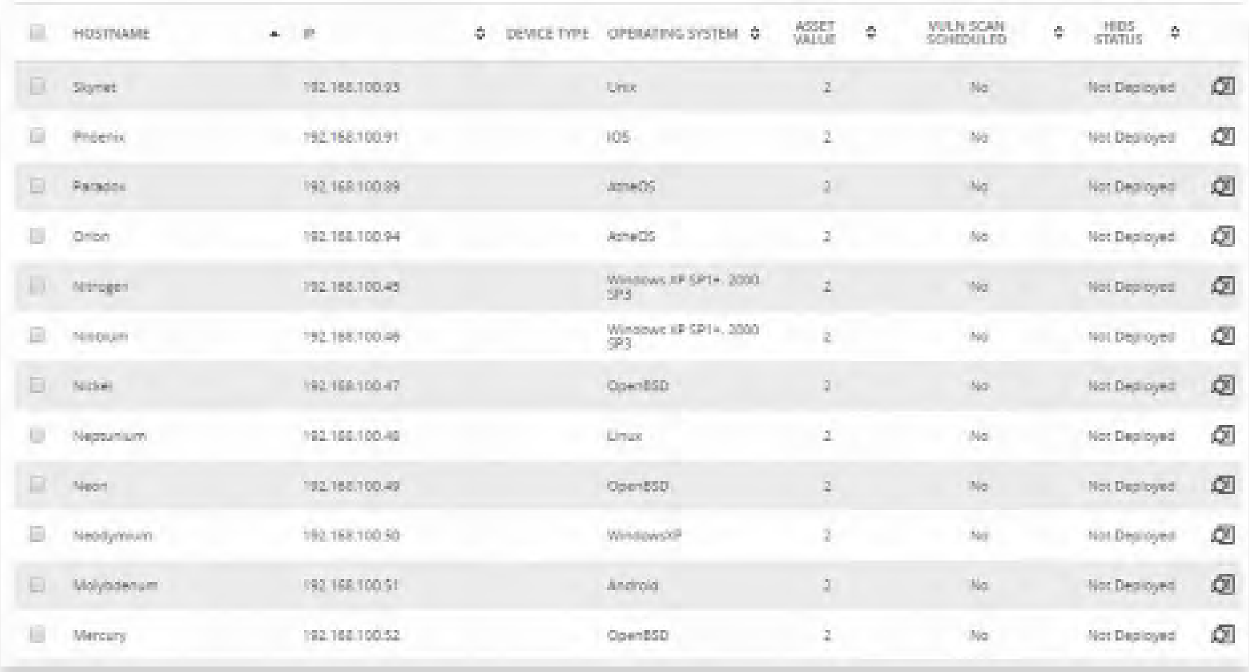
Timing template: Normal

☑ Autodetect services and Operating System

☑ Enable DNS Resolution

Asset Discovery

Below is an example asset list, broken down from the groups detailed in the previous image. This asset discovery gives us a full picture of the assets on your network so that we know what we are monitoring and exactly what should be on your network. The asset information displayed shows which operating system the asset runs on and whether we have a vulnerability scan scheduled for it.



☐	HOSTNAME	IP	DEVICE TYPE	OPERATING SYSTEM	ASSET VALUE	VULN SCAN SCHEDULED	HIDS STATUS
☐	Skynet	192.168.100.93		Unix	2	No	Not Deployed
☐	Phoenix	192.168.100.91		IOS	2	No	Not Deployed
☐	Paradox	192.168.100.89		AtheOS	2	No	Not Deployed
☐	Orion	192.168.100.94		AtheOS	2	No	Not Deployed
☐	Nitrogen	192.168.100.45		Windows XP SP1+, 2000 SP3	2	No	Not Deployed
☐	Niobium	192.168.100.46		Windows XP SP1+, 2000 SP3	2	No	Not Deployed
☐	Nickel	192.168.100.47		OpenBSD	2	No	Not Deployed
☐	Neptunium	192.168.100.48		Linux	2	No	Not Deployed
☐	Neon	192.168.100.49		OpenBSD	2	No	Not Deployed
☐	Neodymium	192.168.100.50		WindowsXP	2	No	Not Deployed
☐	Molybdenum	192.168.100.51		Android	2	No	Not Deployed
☐	Mercury	192.168.100.52		OpenBSD	2	No	Not Deployed

Vulnerability Assessments

Vulnerability assessments are completed by trained SOC staff with minimal intrusion, to identify, define, and prioritize system susceptibilities. These assessments are continuously updated to ensure absolute safety against the latest threats. Our SOC Analysts provide a detailed summary accompanied by a more detailed report to give a break down on any vulnerability threatening your systems.

Using credentials given to the scanning tool, a pathway into the system can allow the tool to view exact program versions and other vulnerabilities that may not be visible from the network. The scan is also able to operate inside of the host, reducing the load on your network.

The vulnerability assessment covers all major operating systems such as Windows or Linux in addition to vendor specific operating systems like VMware, and applications like Java.

The vulnerability scanner can check for over 55,000 different types of vulnerabilities, including some common types below:

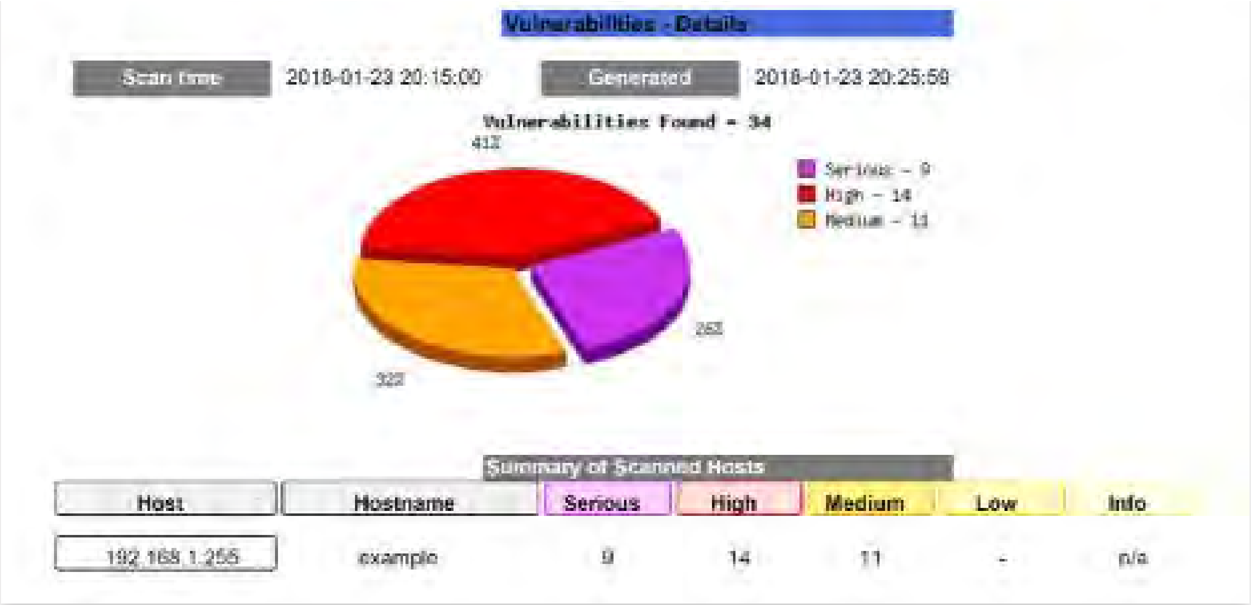
Security Updates:
- Windows Updates and Microsoft Security Bulletins
- Missing Application Security Updates.

Attacks:
- SQL Injection and XSS Attacks
- Web Server and Application Attacks
- Database Attacks
- Remote Code Execution

Privilege Escalation
Denial of Service Attacks

System Configuration:
- Default Accounts
- Remote Shell Access
- SSL / TLS Configuration
- Certificates
- Service Detection
- Local System Security

Vulnerability Assessments



Vulnerabilities - Details

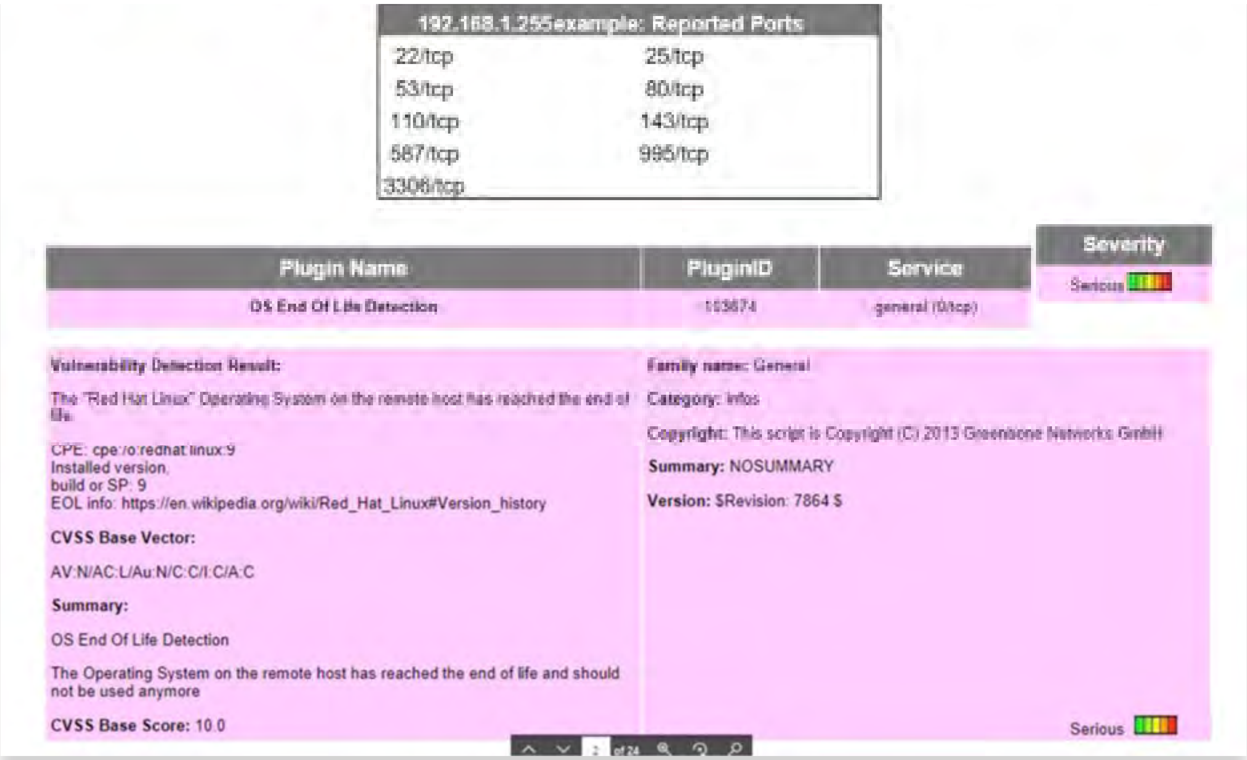
Scan time 2018-01-23 20:15:00 Generated 2018-01-23 20:25:58

Summary of Scanned Hosts

Host	Hostname	Serious	High	Medium	Low	Info
192.168.1.255	example	9	14	11	-	n/a

Above is an example **vulnerability report** for one asset on a customer's network. This is what is generated by our threat detection systems before analysis takes place and a summary is generated by one of our Tier 2 SOC analysts. On the next page, you will find an example page from a report, breaking down one of the vulnerabilities as it arrives. The vulnerability summary identifies incoming threats by comparing them with a database of known vulnerabilities. This can also be used to check compliance of an organization and is an important part of many areas of compliance.

Vulnerability Assessments



192.168.1.255example: Reported Ports	
22/tcp	25/tcp
53/tcp	80/tcp
110/tcp	143/tcp
587/tcp	995/tcp
3306/tcp	

Plugin Name	PluginID	Service	Severity
OS End Of Life Detection	103674	general (0/tcp)	Serious

Vulnerability Detection Result:

The "Red Hat Linux" Operating System on the remote host has reached the end of life.

CPE: cpe:/o:redhat:linux:9
Installed version,
build or SP: 9
EOL info: https://en.wikipedia.org/wiki/Red_Hat_Linux#Version_history

CVSS Base Vector:

AV:N/AC:L/Au:N/C:C/I:C/A:C

Summary:

OS End Of Life Detection

The Operating System on the remote host has reached the end of life and should not be used anymore

CVSS Base Score: 10.0

Family name: General

Category: infos

Copyright: This script is Copyright (C) 2013 Greenbone Networks GmbH

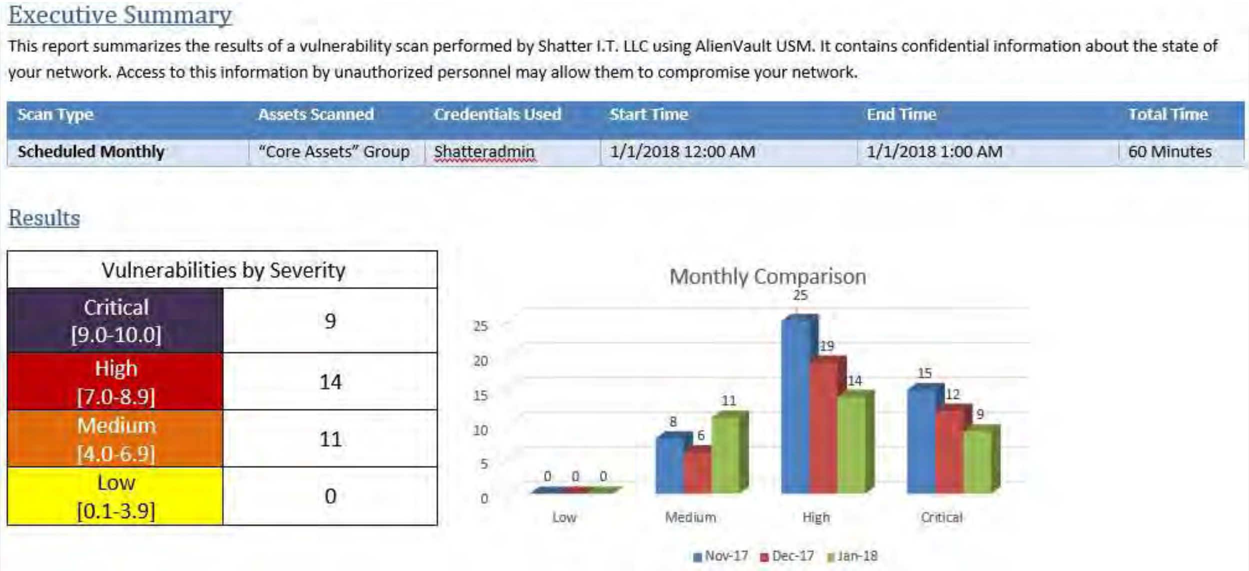
Summary: NOSUMMARY

Version: $Revision: 7864 $

Serious

This is an example of a **serious vulnerabilit**y being reported to the customer. Following summaries of all vulnerabilities will be sent to customers monthly following extensive review from our SOC analysts. SOC analysts can schedule vulnerability scans dependent on the package selected by the customer, commonly occurring monthly.

Vulnerability Assessments



Executive Summary

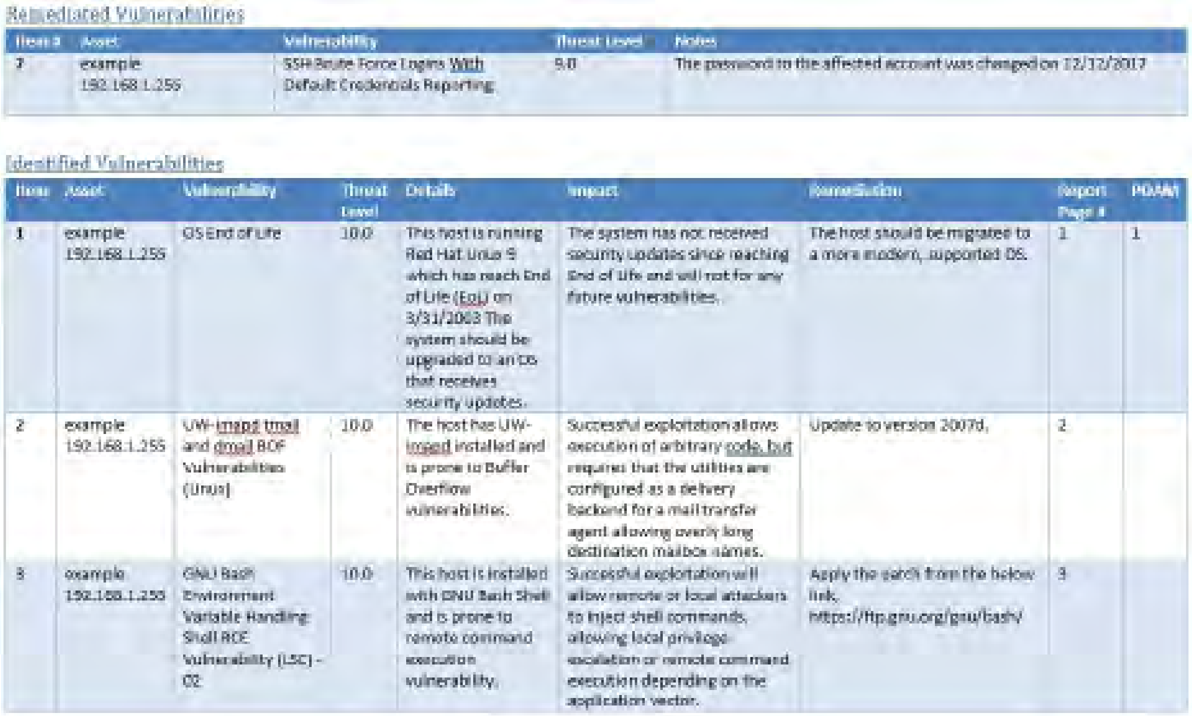
This report summarizes the results of a vulnerability scan performed by Shatter I.T. LLC using AlienVault USM. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

Scan Type	Assets Scanned	Credentials Used	Start Time	End Time	Total Time
Scheduled Monthly	"Core Assets" Group	Shatteradmin	1/1/2018 12:00 AM	1/1/2018 1:00 AM	60 Minutes

Results

Vulnerabilities by Severity	
Critical [9.0-10.0]	9
High [7.0-8.9]	14
Medium [4.0-6.9]	11
Low [0.1-3.9]	0

A **vulnerability summary** is then developed from the report by a Tier 2 SOC analyst and sent off to the customer (see below). The vulnerability summaries are developed from analysis of the information received through our SOC alarm procedures and the vulnerability reporting. It is divided into critical, high, medium and low-level vulnerabilities for the customers viewing. Further explanation then occurs in the bottom image.



Remediated Vulnerabilities

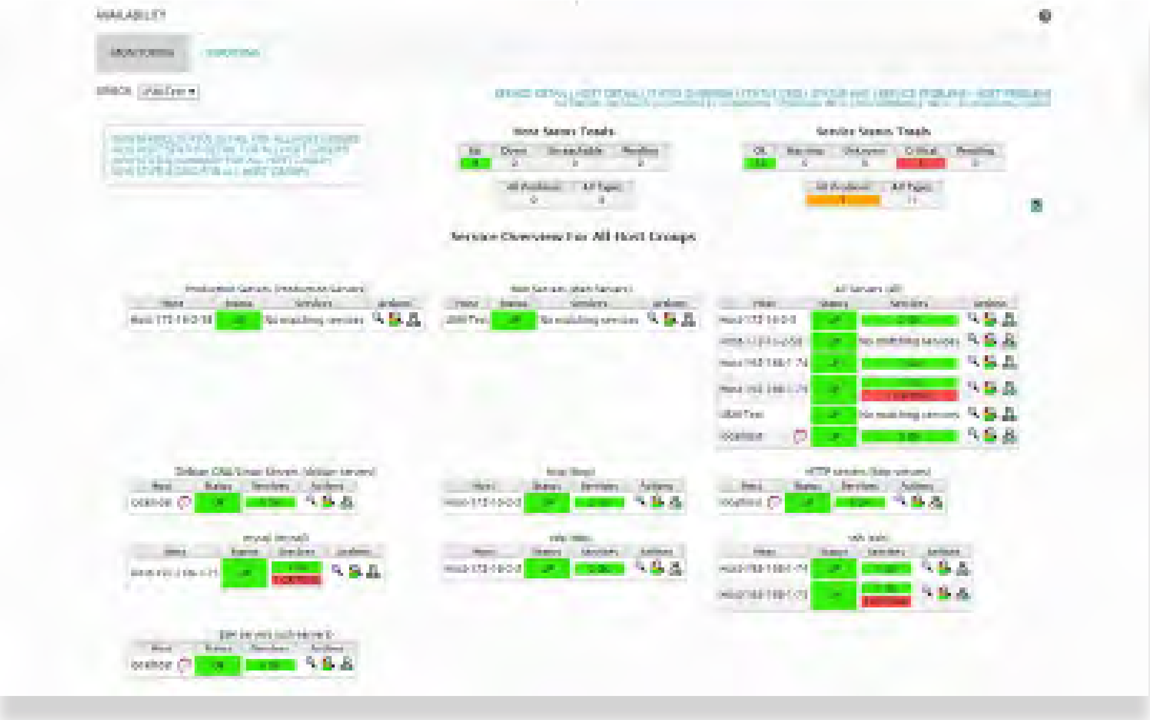
Item #	Asset	Vulnerability	Threat Level	Notes
7	example 192.168.1.255	SSH Brute Force Logins With Default Credentials Reporting	9.0	The password to the affected account was changed on 12/12/2017

Identified Vulnerabilities

Item	Asset	Vulnerability	Threat Level	Details	Impact	Remediation	Report Page #	POAM
1	example 192.168.1.255	OS End of Life	10.0	This host is running Red Hat Linux 9 which has reach End of Life (EoL) on 3/31/2003 The system should be upgraded to an OS that receives security updates.	The system has not received security updates since reaching End of Life and will not for any future vulnerabilities.	The host should be migrated to a more modern, supported OS.	1	1
2	example 192.168.1.255	UW-imapd tmail and dmail BOF Vulnerabilities (Linux)	10.0	The host has UW-imapd installed and is prone to Buffer Overflow vulnerabilities.	Successful exploitation allows execution of arbitrary code, but requires that the utilities are configured as a delivery backend for a mail transfer agent allowing overly long destination mailbox names.	Update to version 2007d.	2	
3	example 192.168.1.255	GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 02	10.0	This host is installed with GNU Bash Shell and is prone to remote command execution vulnerability.	Successful exploitation will allow remote or local attackers to inject shell commands, allowing local privilege escalation or remote command execution depending on the application vector.	Apply the patch from the below link, https://ftp.gnu.org/gnu/bash/	3	

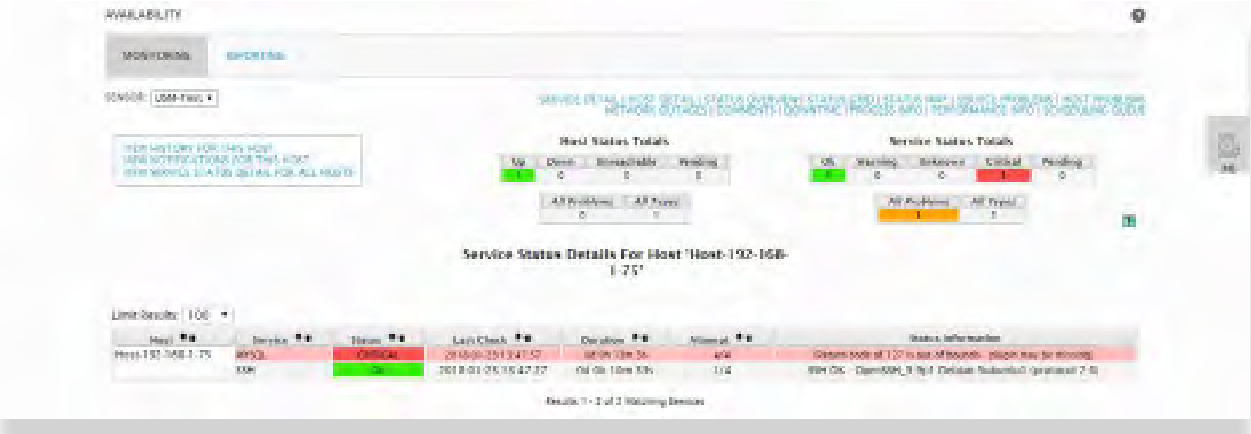
Availability Monitoring

After the asset discovery scan has been completed, DataSure24 can monitor an assets availability, to ensure that the customer's systems are up and running in the way that they should be, and that down-time is avoided. This also provides visibility into the traffic patterns of the customers, allowing quick detection of abnormal activity levels. We will notify of any down assets on your network that you are not planning for.



Service Overview For All Host Groups

The left shows an overview of all asset groups availability, while the bottom image shows an individual assets availability and information about it, including; source IP, destination IP, type of service & number of bytes.



Host Status Totals

Up	Down	Unreachable	Pending
1	0	0	0

All Problems	All Types
0	1

Service Status Totals

OK	Warning	Unknown	Critical	Pending
1	0	0	1	0

All Problems	All Types
1	2

Service Status Details For Host 'Host-192-168-1-75'

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
Host-192-168-1-75	MYSQL	CRITICAL	[illegible]	[illegible]	4/4	[illegible]
	SSH	OK	2018-01-25 15:47:27	[illegible]	1/4	SSH OK - OpenSSH_[illegible]

Results 1 - 2 of 2 Matching Services

Intrusion Detection

Included in our core compliance package is an intrusion detection service, that can ensure dedicated and thorough monitoring and protection of our customers systems and information.

This services is included in the core compliance package, and consists of network-based intrusion detection. (NIDS) aspects.

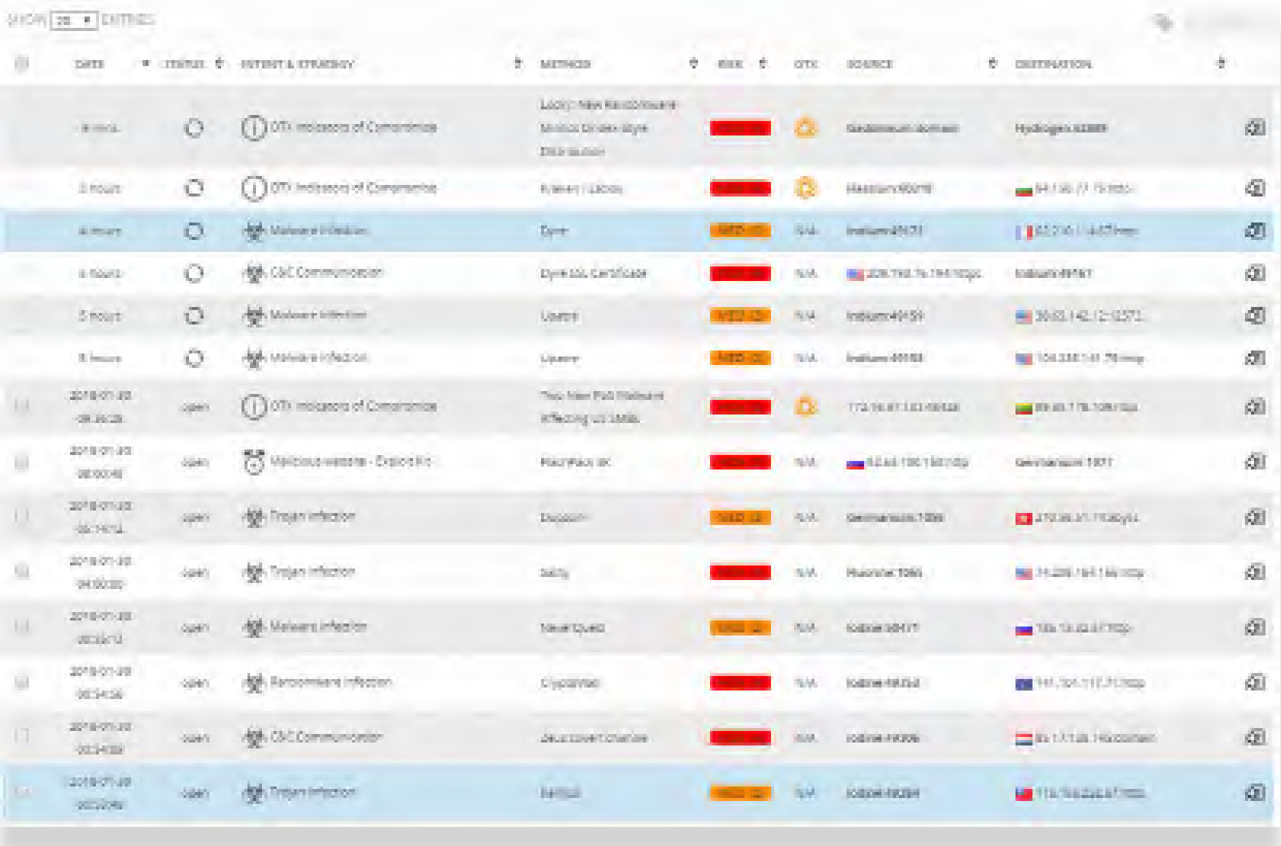
A network-work based intrusion detection system is used for passive sniffing of interfaces, and will monitor for potentially malicious activity trying to access your information.

DataSure24’s Intrusion Detection System (IDS) can view all traffic on a network by mirroring all traffic flowing through a switch or firewall and analyzing it for malicious events. These events are correlated together to identify threats by detecting behavior patterns across different types of assets.

The IDS also utilizes threat intelligence through the Open Threat Exchange to add context to potential security events and protect against emerging or zero-day threats.

Intrusion Detection

Below is an example of alarms incoming to DataSure24 for analysis. The network intrusion detection system (NIDS) passively analyzes payload data and monitors for potentially malicious data. The alarms are viewed in real-time by either our Tier 1 or Tier 2 SOC analysts and are elevated to appropriate staff members to alert the customer of potential incidents to their system.



SHOW 25 ENTRIES

	DATE	STATUS	INTENT & STRATEGY	METHOD	RISK	OTX	SOURCE	DESTINATION
	8 mins	○	OTX Indicators of Compromise	Locky: New Ransomware Mimics Dridex-Style Distribution	[illegible]		[illegible]	[illegible]
	3 hours	○	OTX Indicators of Compromise	Kelihos / Locky	[illegible]		[illegible]	[illegible]
	4 hours	○	Malware Infection	Dyre	[illegible]	N/A	[illegible]	[illegible]
	4 hours	○	C&C Communication	Dyre SSL Certificate	[illegible]	N/A	[illegible]	[illegible]
	5 hours	○	Malware Infection	Upatre	[illegible]	N/A	[illegible]	[illegible]
	8 hours	○	Malware Infection	Upatre	[illegible]	N/A	[illegible]	[illegible]
□	2018-07-20 [illegible]	open	OTX Indicators of Compromise	Two New PoS Malware Affecting US SMBs	[illegible]		[illegible]	[illegible]
□	2018-07-20 [illegible]	open	Malicious website - Exploit Kit	[illegible]	[illegible]	N/A	[illegible]	[illegible]
□	2018-07-20 [illegible]	open	Trojan Infection	[illegible]	[illegible]	N/A	[illegible]	[illegible]
□	2018-07-20 [illegible]	open	Trojan Infection	Sality	[illegible]	N/A	[illegible]	[illegible]
□	2018-07-20 [illegible]	open	Malware Infection	NeverQuest	[illegible]	N/A	[illegible]	[illegible]
□	2018-07-20 [illegible]	open	Ransomware Infection	Cryptowall	[illegible]	N/A	[illegible]	[illegible]
□	2018-07-20 [illegible]	open	C&C Communication	Zeus covert channel	[illegible]	N/A	[illegible]	[illegible]
□	2018-07-20 [illegible]	open	Trojan Infection	[illegible]	[illegible]	N/A	[illegible]	[illegible]

The alarms report on the type of vulnerability, source, destination, time of the event, method and the level of alarm that arrived. Alarms are ranked low (1), medium (2) or high (3). The above alarms are analyzed by our SOC analysts by utilizing our SOC alarm metrics, and tickets are created in both our internal alert ticketing system and the 24Seven ticketing system by SOC Tier 2 analysts. If a Tier 1 analyst finds an alarm worthy of analysis, it must be elevated to a Tier 2 analyst before a ticket is created in 24Seven and brought to the attention of the customer.

Incident Response

Following the intrusion detection stage and discovery of vulnerabilities, Tier 1 and Tier 2 analysts are in our SOC on a 24/7, 365 days a year basis to respond and inform on any incoming threats. Incident response is all about time. We dedicate our work to making sure we respond and inform in rapid time, to ensure any potential vulnerabilities do not make large impacts on your organization.

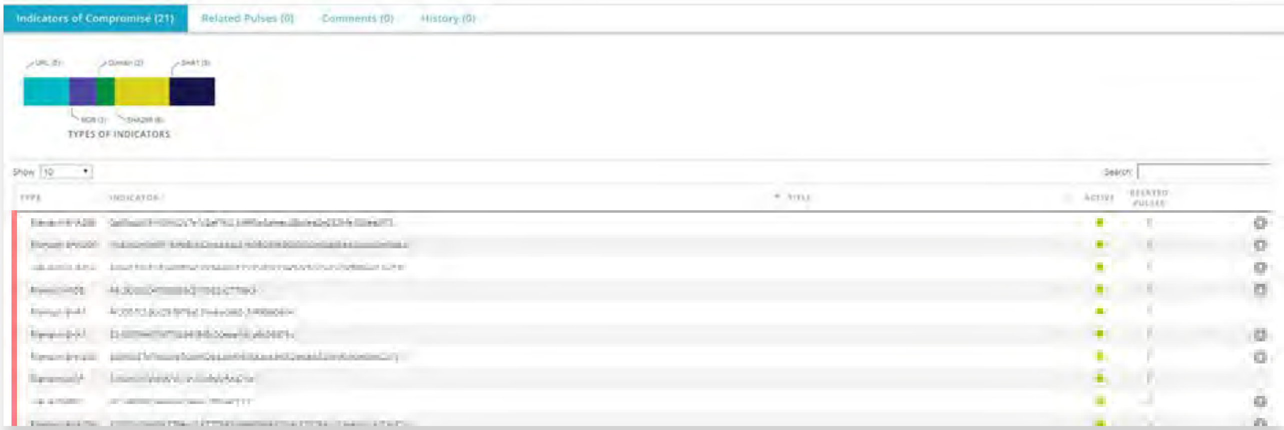
Any alarm with a high-level risk will have a 1-2 hour response time. Analysts will alert the customers technical team with details of the event and recommended course of action. An alarm with a medium risk level will prompt a notification within 48-72 hours.

Low levels alarms are analyzed in line with our metrics for assessing incoming alarms, with some being elevated to medium-level alarms.

Our incident response procedures and metrics developed by in-house experts allow for a speedy notification on any harmful events affecting your system, allowing remediation to being to optimize the time it takes to get your businesses systems back up and running.

Additional Information

In addition to our Core Compliance package, we also utilize Open Threat Exchange (OTX) services. This is a system that is designed for sharing threat intelligence information. OTX is a global community of cyber security professionals who contribute Indicators of Compromise of the latest threats to the exchange, where users can subscribe to and download rules for each new threat.



DataSure24 leverages the Open Threat Exchange by subscribing each customer monitoring server access to the OTX platform, where new rules are constantly added through an application programming interface (API). This additional data feed allows for the latest threats to be detected even quicker by allowing analysts to subscribe to new threats before updates to the monitoring server need to be applied.