OPERATIONS & INTELLIGENCE CYBER SECURITY REPORT

Inspira Health Network

January 2018

CONFIDENCIAL

Tel: +1 609-651-4246
Tel: +507-836-5355

Info@glesec.com
www.glesec.com

Table of Contents

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

About This Report

The purpose of this document is to report on the "state" of security for your organization. It must be noted that GLESEC bases its information analysis on the services under contract. The information generated by these services is then aggregated, correlated and analyzed. The more complete the set of services under contract the more accurate and complete the results will be.

The report is organized in three parts; the first is the Executive Summary with recommendations (as necessary or applicable), the second is the Intelligence Section with more detail information and analysis dashboards and the last is Operational Section with status of the services and counter-measures under contract, tickets for change management and incidents reported and consulting activity for the month.

We at GLESEC believe that information security is a holistic and dynamic process that requires on-going research and follow up and should be handled with the right tools, systems, processes, skill personnel and focus attention. The process is dynamic due to the constant discovery of new security vulnerabilities and exploits, the proliferation of hacking tools that make it easier for script-kiddies with minimal knowledge to cause damage. The increase in malware, phishing, insider threats, espionage, organized crime, intellectual property theft, and hacktivism are the very cause of information security exposure and are most commonly driven by financial gain. GLESEC's outsourcing services, based on its proprietary TIPTM platform portfolio provide the ideal response to the above.

Confidentiality

GLESEC considers the confidentiality of client's information as a trade secret. The information in this context is classified as:

- Client name and contact information
- System architecture, configuration, access methods and access control
- Security content

All the above information is kept secure to the extent in which GLESEC secures its own confidential information.

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

Scope of this Report

GLESEC Contracted Services Table
This table list of GLESEC TIP™ services and indicate which are contracted and the corresponding service expiration dates of the contracts.

Type	Service	Contracted?	Service Expiration
Threat Mitigation	MSS-APS	YES	1/1/2018
Threat Mitigation	MSS-APS-SSL		
Threat Mitigation	MSS-APS-PS		
Threat Mitigation	MSS-APFW		
Vulnerability Testing	MSS-VME	YES	1/1/2018
Vulnerability Testing	MSS-VMI		
Compliance	MSS-EPS		
Threat Mitigation	MSS-SIEM		
Risk assessment	MSS-BAS		
Threat Mitigation	MSS-EIR		
Threat Mitigation	MSS-UTM		
Threat Mitigation	MSS-INT		
Access Control	MSS-TAS		

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

Executive Summary

This report corresponds to the period from January 01 to January 31, 2018.
The following table describes the major categories that GLESEC has identified to report on the state-of-security of its member-clients. The categories in the table below are based on risk-management methodology. This is a principal foundational aspect of GLESEC.

RISK

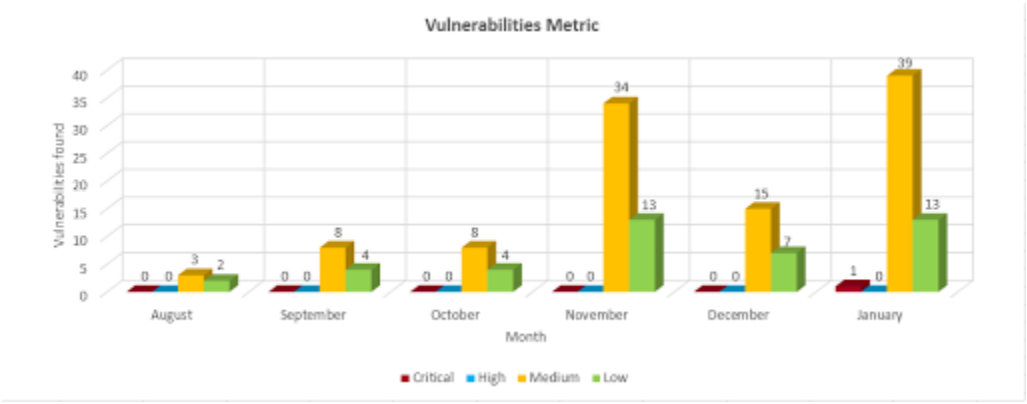
Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. With this information, organizations can determine the acceptable level of risk for delivery of services and can express this as their risk tolerance. The NIST Cyber-Security Framework

One of GLESEC's foundational columns is basing all its activities to support RISK determination and mitigation. What any organization should want to know if what is their level of RISK, and in this case in particular to cyber-security. Cyber-Security RISK has a direct impact to the business and as such is of paramount importance to the Board and Management of the company.

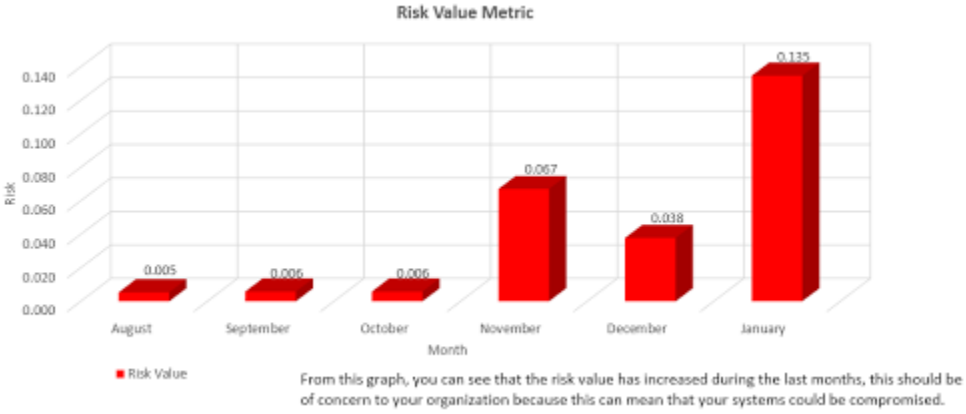
We at GLESEC measure RISK through a number of perspectives and using several of the TIP™ platform portfolio of services. The MSS-VM or Managed Vulnerability

Service provides us with one view, how weak are the systems of the organization. The MSS-BAS provides us a view of how weak are the defenses of the organization to the latest threats. The MSS-APS, MSS-SIEM, MSS-UTM, MSS-EIR, MSS-EPS provides us with attack information both internal and external, DDOS, Malware, Ransomware and other attack vector information as well as provide protection level services. The MSS-EPS also provides us RISK level information for non-compliance with internal or external requirements and/or regulations. All in all a variety of services provide us with different views and together we have the most complete view of our client's security posture.

The RISK VALUE METRIC histogram below represents the changes in the Vulnerability based Risk Value Metric over the past six months.



The risk conditions for this month based on the contracted services are 1 critical vulnerabilities on 1 hosts that should be remedied.



From this graph, you can see that the risk value has increased during the last months, this should be of concern to your organization because this can mean that your systems could be compromised.

VULNERABILITIES

GLESEC's MSS-VM(E/I) service is used to conduct two weekly testing to external and/or internal systems (depending on the options of the contracted service). Of the two tests performed weekly, one is to test for discovery of assets on the network and the other to test for vulnerabilities. The external testing is performed from GLESEC' cloud platform and the internal is conducted with the GLESEC Multi-Security Appliance (GMSA).

Vulnerabilities are weaknesses that if exploited can compromise the organization and as such are a component of RISK for the organization. If there are vulnerabilities and also threats there is RISK that the organization can be impacted. The vulnerabilities reported by GLESEC should be considered all important and addressed according to the priority (Critical, High, Medium and Low). An effective process is to work with the GLESEC provided information and GLESEC consulting team to address the recommendations provided in a systematic and continuous way. Progress can be determined by the weekly testing.

Overall the vulnerabilities for Inspira Health Network this period has been of 2 critical ,0 high ,39 medium and 13 low risk and we found 2 critical vulnerabilities on host 170.75.33.142 these are classified as integer overflow that should be remedied as soon as possible.

Risk Value Metric

GLESEC utilizes a metric to provide a way to quantify the vulnerabilities based risk of an organization. This metric is to measure the relative value of vulnerabilities and also the record of change over time.

It is important to mention that this metric considers a median value for the vulnerabilities classified as "critical", "high", "medium" and "low", giving them a weight of 100%, 75%, 50% and 10% respectively.

This takes into consideration all of the vulnerabilities, but is important to point out that these values (100%, 75%, 50% and 10%) are arbitrarily chosen by us, so this measure can in time change as we understand more of the risks involved. We can use this metric to evaluate the progress in time and to compare one over the other using a common amount set.

The following external network ranges 170.75.48.0/20,170.75.32.0/20 for Inspira

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

Health Network were scanned for vulnerabilities.

The following table indicates the external vulnerability metric.

Total IP's Scanned	IP's Vulnerable
58	19

Risk Distribution				
Critical	High	Medium	Low	Total
1	0	39	13	53

According to the metrics:

RV= 0.134743006

The following values are to clarify RV:

RV=1 Points to every IP address in the infrastructure that are susceptible to attacks

RV=0 Points to no IP address in the infrastructure aret susceptible to attacks

RV=0.1 Point to 1/10 IP address in the infrastructure that are susceptible to attacks

External listing of vulnerabilities by condition:

Host	Critical	High	Medium	Low	Total
170.75.33.134	0		5	2	7
170.75.33.136	0		4	2	6
170.75.33.137	0		4	2	6
170.75.33.139	0		4	2	6
170.75.33.55	0		4	1	5
170.75.33.133	0		4	0	4
170.75.33.113	0		3	0	3
170.75.33.142	1		1	1	3
170.75.33.4	0		2	0	2
170.75.33.129	0		1	1	2

The following table provides a comparison of persistent external vulnerabilities of the current month and previous month.

host-ip	Previous Month	Current Month
170.75.32.15	5	
170.75.33.109		1
170.75.33.113		3
170.75.33.117		1
170.75.33.118	1	
170.75.33.119		1
170.75.33.125		1
170.75.33.129		2
170.75.33.132		1
170.75.33.133		4
170.75.33.134		7
170.75.33.136	6	6
170.75.33.137		6
170.75.33.139	6	6
170.75.33.142		3
170.75.33.152		2
170.75.33.167		1
170.75.33.169		1
170.75.33.4	2	2
170.75.33.55		5
170.75.33.58		1
170.75.49.35	2	

Please view Recommendations for more details. This can be seen on the GLESEC MEMBER PORTAL (GMP).

Vulnerability Categories

The following table indicates the categories that we use for vulnerabilities as a way to provide context to them and facilitate the prioritization of how to handle remediation.

Preliminary Analysis	Firewalls	Network Devices
SMB/NetBIOS	SSH Servers	Malformed Packets
Simple Network Services	Mail Servers	Proxy Servers
Policy Checks	SQL Servers	Wireless AP
Web Servers	FTP Servers	Webmail Servers
RPC Services	Server Side Scripts	NFS Services
Backdoors	SNMP Services	Printers
Encryption and Authentication	DNS Servers	

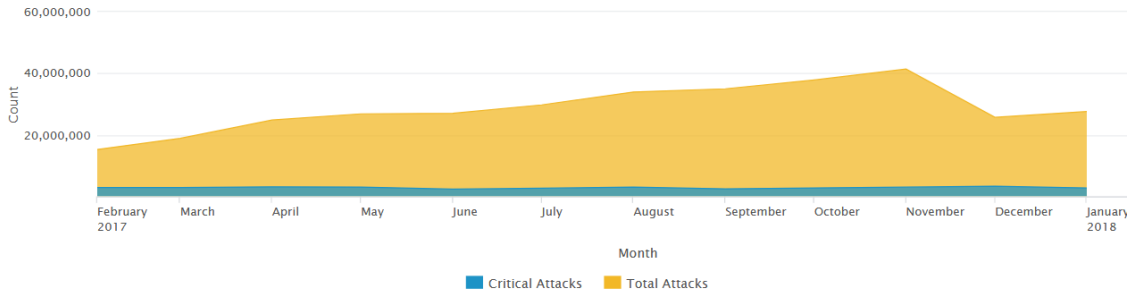
Based on the above the following table shows a matrix of the total external vulnerabilities by category.

Name	Critical	High	Medium	Low	Total
General	0		34	5	39
Misc.	0		0	4	4
Service detection	0		5	0	5
Web Servers	0		0	4	4
Windows	2		0	0	2

THREATS

GLESEC uses its MSS-APS, MSS-EPS, MSS-SIEM, MSS-EIR and MSS-UTM to determine threat intelligence activity.

The Threats as reported by the MSS-APS, for this month are IPv4 TCP-SYN floods (DoS) and anomalies in BGP protocol (Intrusion).



This month we are seeing an increase in attack activity from prior month of about 7.3% and a decrease in critical attacks from prior month of about 16.7%.

Most of the attacks have duration of more than one hour and they target multiple ports. GLESEC's GOC was able to recognize that the persistent attacks for more than one hour can be categorized as TCP scans and anomalies, anomalies in the TCP headers can happen due to collision or a high level of noise in the network, however, these attacks were dropped. We also found a considerable amount of attacks to unregistered port (8545), most of these attacks are horizontal TCP scans, and this port is filtered.

Most of the attacks seem to be of reconnaissance (scanning). About 79% of the attacks for this month came from scanning which can be considered reconnaissance and it is what precedes further attacks.

The attacks are mostly from Russian Federation, which represents approx. 41% of total attacks this month followed by USA and Chile, as the three top sources. A significant number of attacks are scanning which can be considered reconnaissance

and is what precedes further attacks.

.

Based on the information gathered from the security countermeasures during this period 25,753,535 attacks on Inspira; 3,332,512 of which were considered critical were all stopped by the GLESEC managed security countermeasures.

Inspira receives an average of 27,625,326 total attacks and 2,774,602 critical attacks on a monthly basis. This equates to an average of 915,227 total daily attacks and 96,352 critical daily attacks.

Systems at Maximum Capacity

Both DefensePro systems, the one in Bridgeton and the one in Elmer are deployed with a "Throughput-limit license" of 600 Mbps. The license limits the total throughput of the device. The calculation of the DefensePro throughput license counts "*legitimate traffic"*. Legitimate traffic is traffic that exits the device, for example White-List packets, or traffic-exclusion packets. The license is calculated based on all egress traffic at the egress port—regardless of whether that traffic has a matched policy.

Notes:

- The license is calculated based on the amount of traffic sent to the egress port regardless of the port status (up/down).
- DefensePro allows momentarily exceeding the limit on legitimate traffic - up to approximately 10% over the limit for 10 seconds.
- All traffic that DefensePro processes (that is, not dropped) is counted towards the license (including white-listed traffic).

What happens when the throughput reaches and exceeds the license limit?
The user is notified when throughput reaches 90% of license. When throughput exceeds 100% of license:

- DefensePro issues the message "WARNING Device reaches 100% capacity - packets dropped".
- DefensePro drops packets that exceed the throughput limit—for as long as the throughput is exceeded.

In January of this year, we started receiving the message that the throughput has reached the 90% of the license. Please se below the capture of the log file of the DefensePro in Bridgeton:

Rows: 3 Reset Filter

Event Log

Event Number	Description
0	*26-01-2018 10:03:17 Throughput has reached 90% of the limit of your throughput license*
1	*06-02-2018 11:54:34 Throughput has reached 90% of the limit of your throughput license*
2	*07-02-2018 01:01:32 Throughput has reached 90% of the limit of your throughput license*

Recommendations

GLESEC recommends for Inspira Health Network to address the following

1. Take immediate actions to the detailed recommendations in this report.

2. Apply the necessary patches for the vulnerability known as integer overflow that is categorized as critical, and could compromise your hosts.

3. Remedy the vulnerabilities that are still present from last month on your hosts, there are 3 hosts in this condition. Refer to the table of persistent external vulnerabilities for details on affected systems. Some of these vulnerabilities include known vulnerabilities such as POODLE attack.

4. There are obsolete cipher suites, such as SSL RC4, SSLv2 and v3, in use that should be disabled to minimize the amount of vulnerabilities that could be exploited. we recommend the use of TLS v1.2 as it's the latest stable version.

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

5. We recommend upgrading the DefensePro to match the upgraded bandwidth into Bridgeton and Elmer. The lack of upgrade of these systems may cause interruption of all Internet traffic.

6. To avoid reaching the maximum throughput license we recommend that an upgrade of the two systems be performed as soon as possible in order to avoid Internet performance or total Internet blackout.

In our GLESEC Member-Client's Portal you will find more information about the affected hosts of the mentioned vulnerabilities.

GLESEC
USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

Intelligence Section Per Service Module

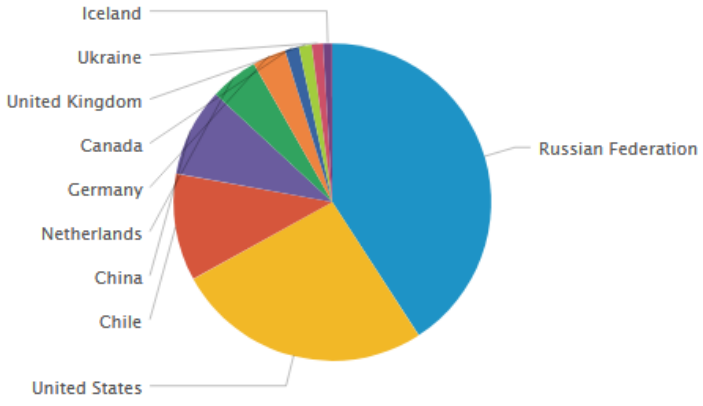
MANAGED ATTACK PROTECTION SERVICE (MSS-APS) SECURITY INTELLIGENCE SECTION

The MSS-APS is a comprehensive Managed Attack Protection Service that provides protection against: Directed or automated intrusion attacks, DDOS attacks, Internal and external attacks, network-based level attacks, encrypted attacks, attacks to cloud based services, attacks that can consume the bandwidth of the Internet Service Providers to your organization. The service responds to Risk of lack of availability for critical systems due to a DDOS attack, Risk of data leakage due to an intruder, Risk of loss of funds due to an intruder, Risk of corporate image tainting thru a defacement of organization public sites.

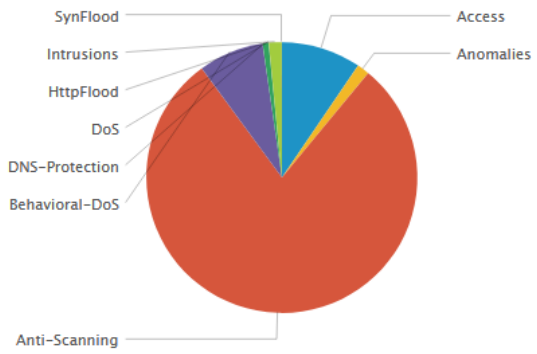
The purpose of this section is to highlight intelligence gathered from the services under contract as well as outside sources such honeypots, known malicious sources, vulnerability databases, relationships with CERT and CSIRT teams that GLESEC possesses, together with various other threat feeds.

The following graphs are dashboards generated by GLESEC's TIP™ platform. These dashboards are representative of metrics for this service.

The distribution of attack sources can be seen in the following chart.

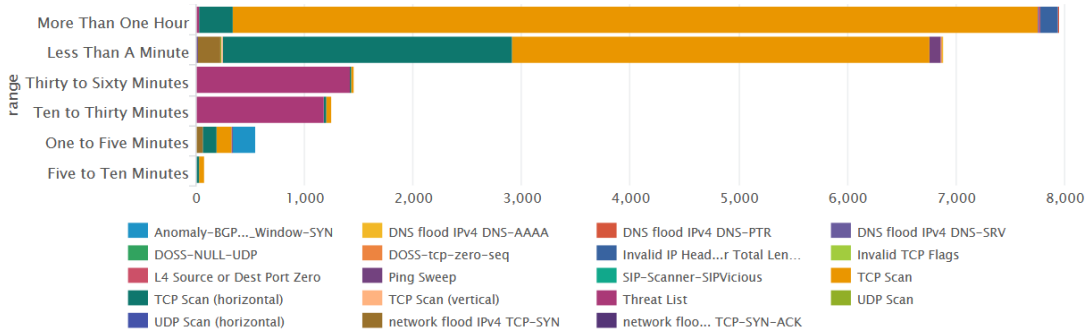


The distribution of attacks per type can be seen in the following diagram.



Duration

Attack duration for specific categories for this report period is illustrated below.



Bandwidth

The following table presents the traffic dropped by category.

Category	Gbps	Mbps
Access	125.74	128760.31
Behavioral-DoS	108.30	110903.75
Anti-Scanning	57.15	58522.92
Intrusions	18.46	18899.25
DNS-Protection	17.71	18139.41
Anomalies	6.57	6732.76
DoS	0.06	65.39
HttpFlood	0.00	0.00
SynFlood	0.00	0.00
Total Bandwidth in Gbps/Mbps	333.99	342023.79

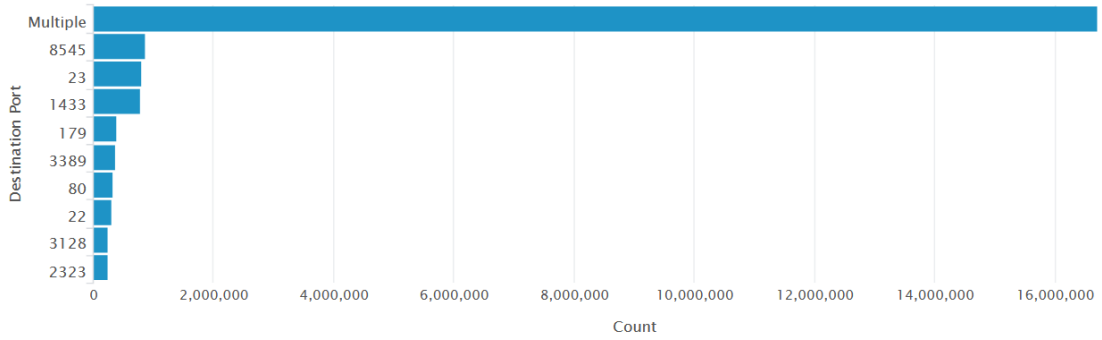
*Please view the Bandwidth Information, and Graph: Bandwidth by Blocked Threat Category by Hour of Day and Graph: Top Attacks Blocked by Bandwidth and Graph:

Attack Categories Blocked by Bandwidth available in the Security Intelligence section of the report.

Port Activity

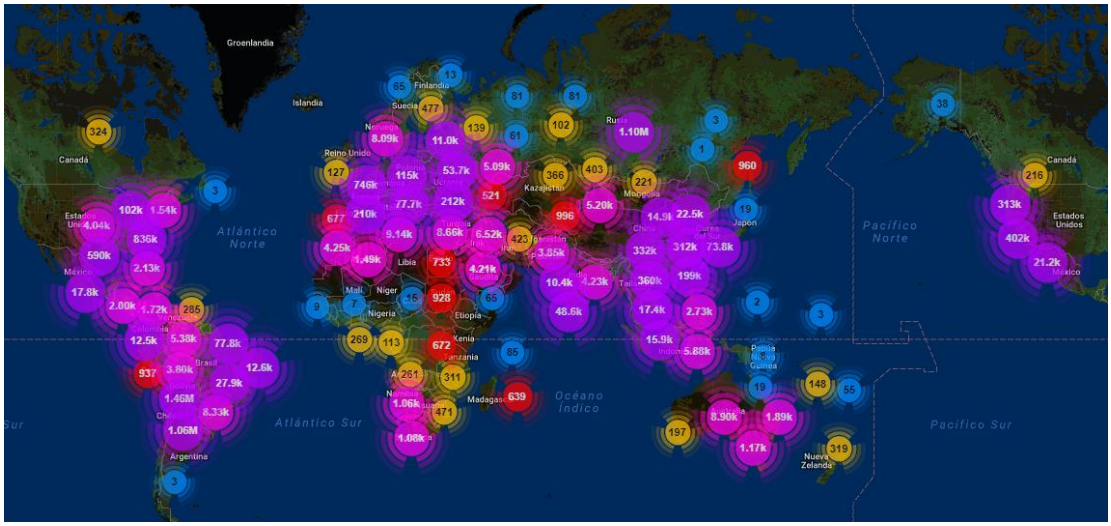
The advanced intrusion detection and prevention capabilities offered by the DefensePro IPS NBA, DoS and Reputation Service provides maximum protection for network elements, hosts and applications. It is composed of different application-level protection features to prevent intrusion attempts such as worms, Trojan horses and single-bullet attacks, facilitating complete and high-speed cleansing of all malicious intrusions.

The DefensePro assisted in preventing attacks directed at network and server level which were directed at well-known port numbers as seen in the following diagram.

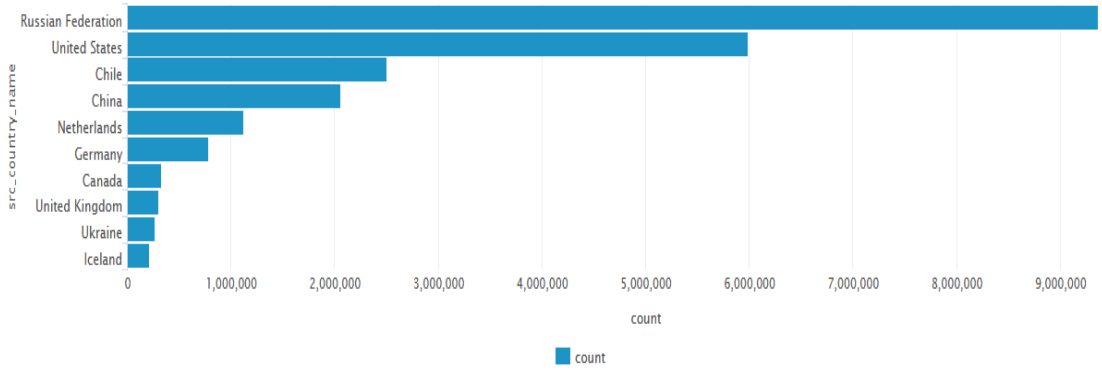


Port number information utilized is based on IANA Service Name and Transport Protocol Port Number Registry and additional outside sources are used to illustrate the relationship to commonly exploited attacks vectors.

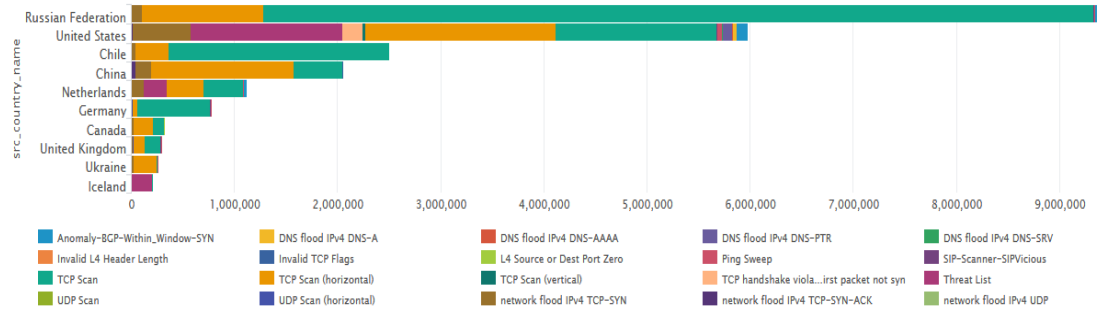
The vast majority of attacks on Inspira Health Network originated geographically from the following countries as seen in the attached diagram. Some results do not include location information that allows map plotting.



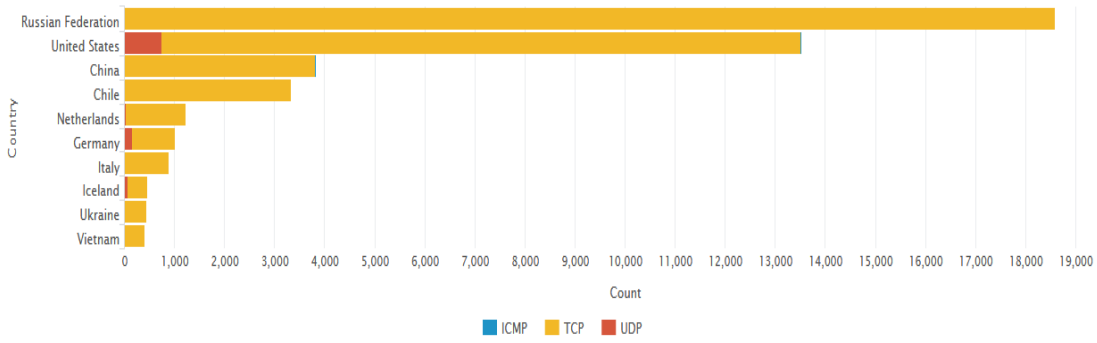
Graph: Top 10 Attacking Countries Blocked
This report provides the count of total attacks blocked by country.



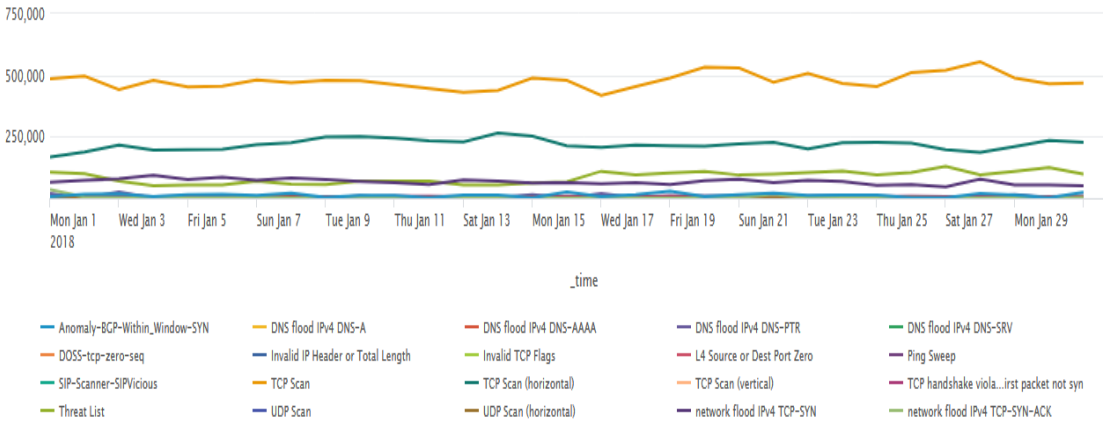
Graph: Top 10 Attacking Countries Blocked by Attack Type
This report provides the count of total attacks types blocked by country



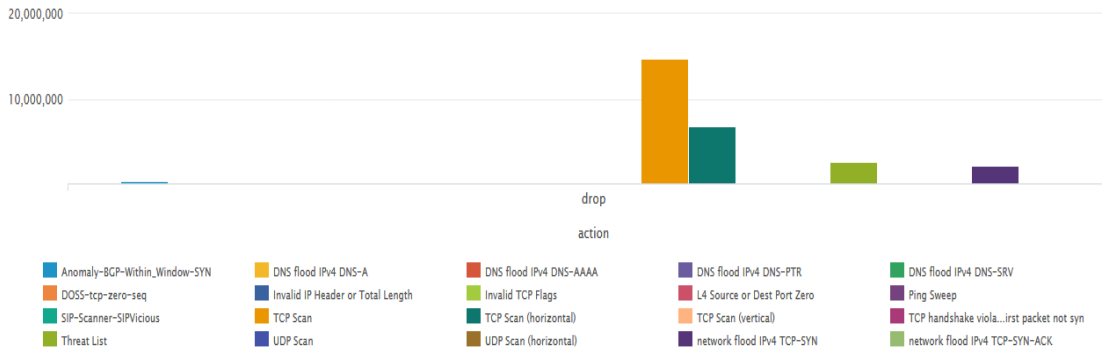
Graph: Top 10 Attacking Countries Blocked by Protocol
This report provides the count of attack protocols blocked by country



Graph: Attacks Types Blocked by Week
This report provides the count of attacks blocked by week



Graph: Attacks Denied
This report provides the count of total denied attacks along with network security rule.



Port Information

Port Information: Port 80 (http), Port 1443 (ms-sql), Port 8080 (https-alt), Port 3306 (mysql) Commonly scanned in order to attack web servers. SQL injection is currently the most common form of web site attack in that web forms are very common, often they are not coded properly and the hacking tools used to find weaknesses and take advantage of them are commonly available online. This kind of exploit is easy enough to accomplish that even inexperienced hackers can accomplish mischief. However, in the hands of the very skilled hacker, a web code weakness can reveal root level access of web servers and from there attacks on other networked servers can be accomplished. Structured Query Language (SQL) is the nearly universal language of databases that allows the storage, manipulation, and retrieval of data. Databases that use SQL include MS SQL Server, MySQL, Oracle, PostgreSQL, MongoDB, Access and Filemaker Pro and these databases are equally subject to SQL injection attack.

Web based forms must allow some access to your database to allow entry of data and a response, so this kind of attack bypasses firewalls and endpoint defenses. Any web form, even a simple logon form or search box, might provide access to your data by means of SQL injection if coded incorrectly.

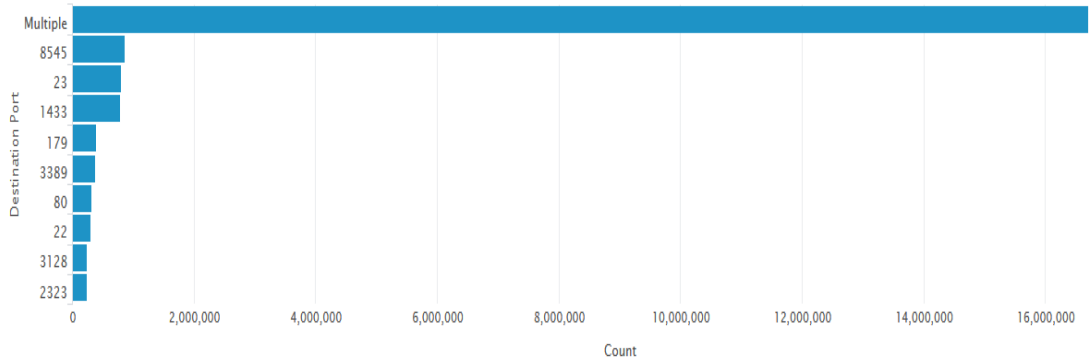
OWASP Top 10 lists A1-Injection as the greatest threat and defines this category as:

Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

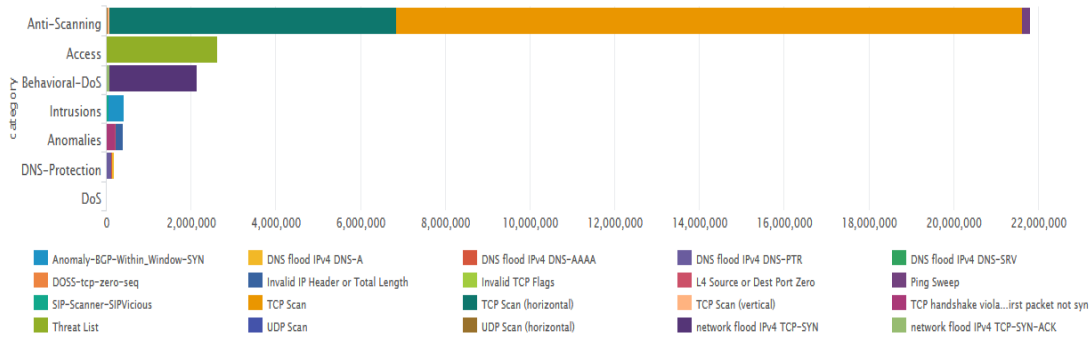
A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.

Graph: Attacks Blocked by Destination Port

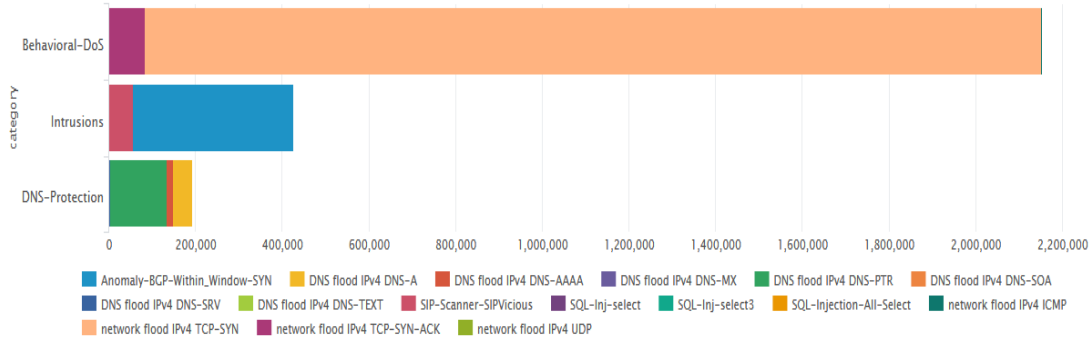
This report provides information on the total number of attacks blocked that were attempted on which port and for how many times.



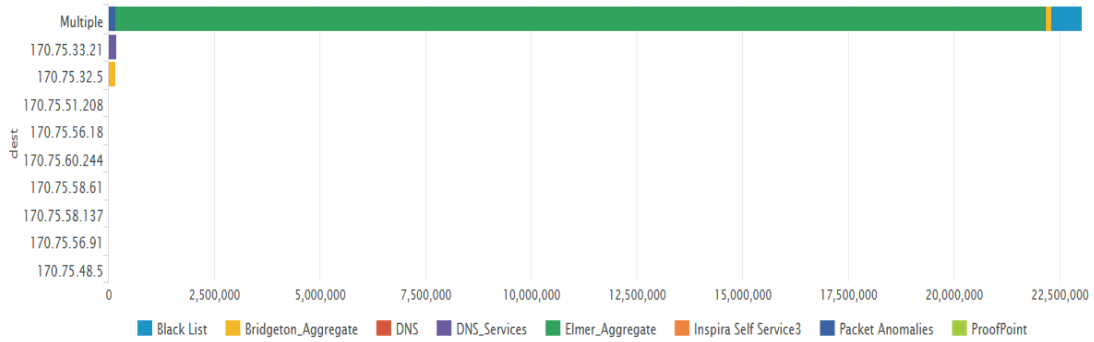
Graph: Attacks Blocked By Threat Category
This report lists the attacks blocked per Attack Category, listing the attack name.



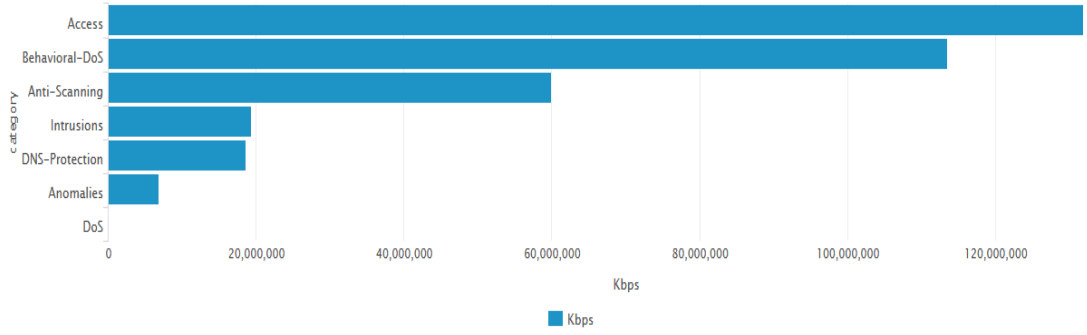
Graph: Critical Attacks Blocked
This report provides Critical Attacks information, attack name, network security rule along with the number of times the attack was launched.



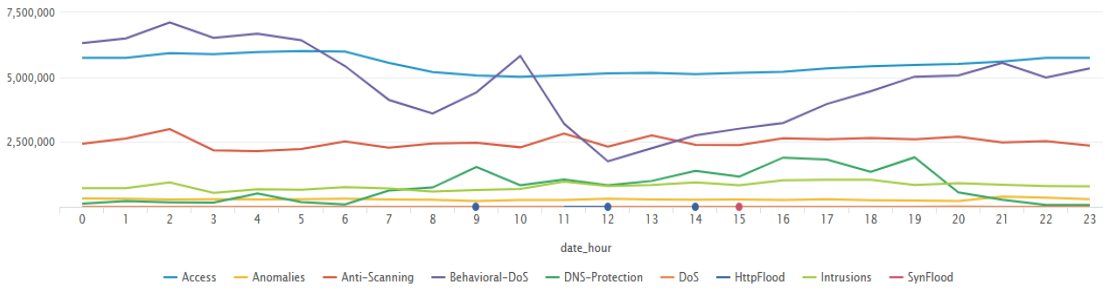
Graph: Top Attacked Destinations Blocked
This report provides information on the system IPs, which were the destination of the attacks for most number of times along with the network security rule.



Graph: Attack Categories Blocked by Bandwidth
This report shows the attack categories based on the BW of the attacks sharing the same category including Kbps.

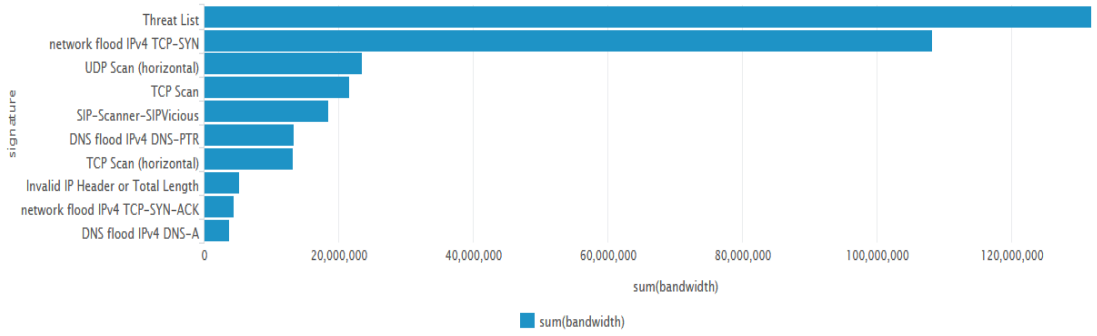


Graph: Bandwidth by Blocked Threat Category by Hour of Day
This report shows the most bandwidth consuming threat categories based on the bandwidth of the attacks sharing the same threat category for each hour of day.



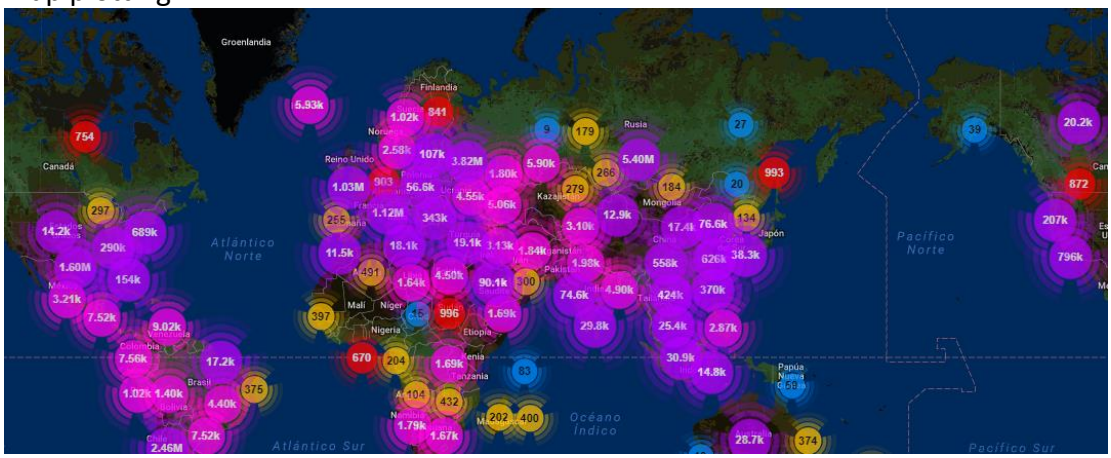
Graph: Top Attacks Blocked by Bandwidth
This report shows the most bandwidth consuming attacks based on the BW of the attack including Kbits.

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355



Scanning Information

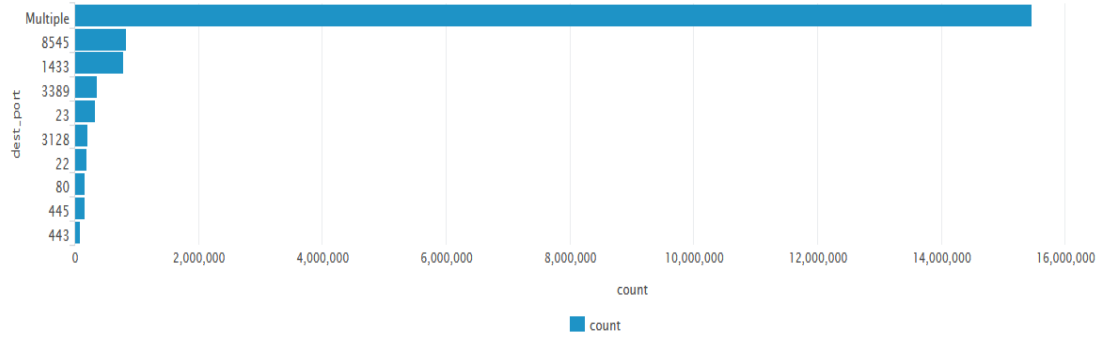
The following map displays geographic distribution of 21,810,895 attacks on Inspira from scanning sources. Some results do not include location information that allows map plotting.



Network-wide Anti Scanning protections dropped enumeration attempts which otherwise thwart any effort for threat modeling, commonplace after the information gathering phase of a targeted or planned attack.

Graph: Top Probed Applications Blocked

This report shows historical view of the Top probed L4 ports.

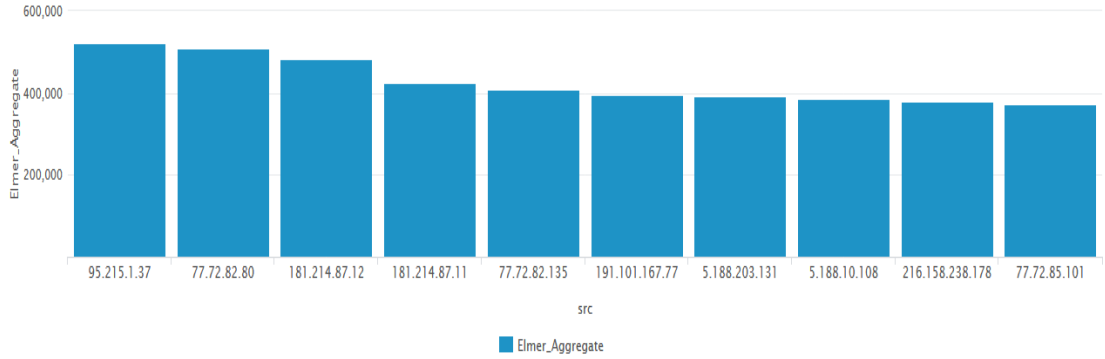


Graph: Top Probed IP Addresses Blocked

This report shows historical view of the Top probed IP addresses that were being scanned along with the network security rule.

Graph: Top Scanners Blocked (Source IP Addressed)

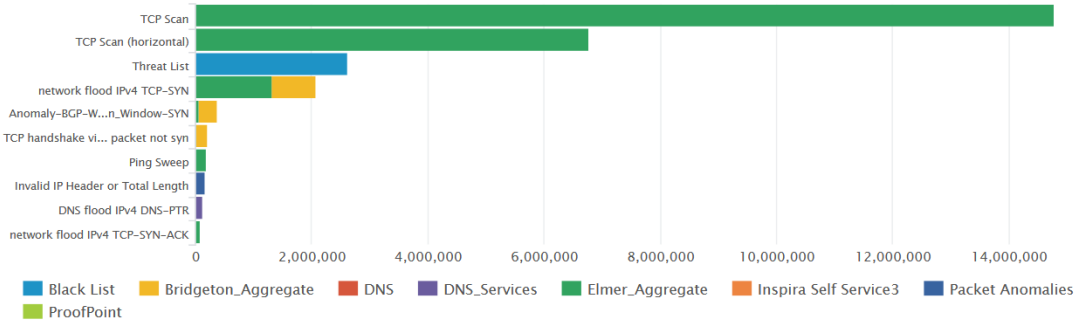
This report shows historical view of the Top source IP addresses that have scanned the network-by-network scanning activities along with the network security rule.



NOTE: See Appendix 2 – Top Scanners Blocked (Source IP Addressed)

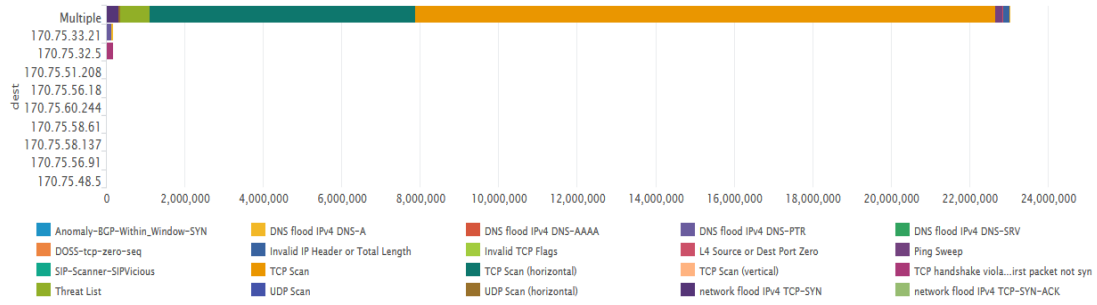
Graph: Top Attacks Blocked

This report provides information on the Top Attacks Blocked, the attack name, network security rule and the total number of attacks blocked with this combination.



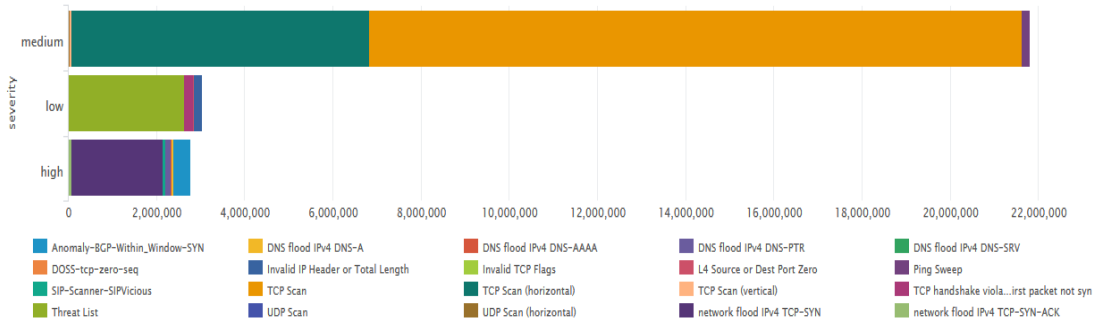
Graph: Top Attacks Blocked by Destination

This report provides information on the top attacks targeted at destinations that were blocked on the DP IPS. In this report the destination on which the attack was targeted, attack name, and count are shown.



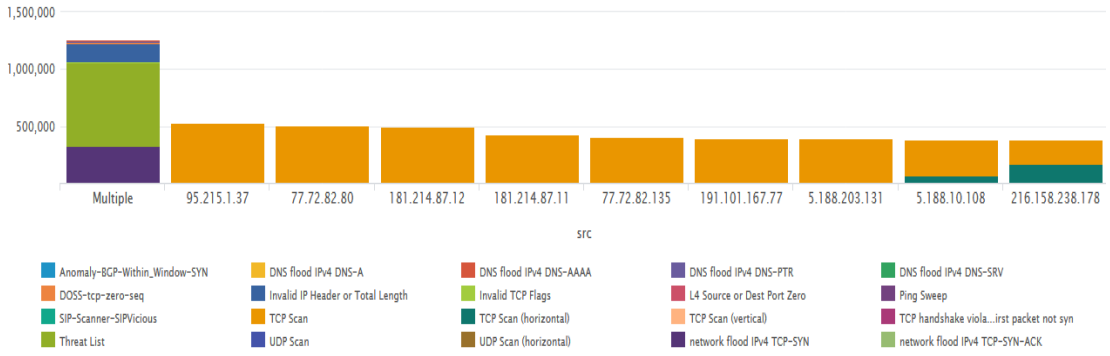
Graph: Top Attacks Blocked By Risk

This report provides information on the attacks, which were blocked on DP IPS based on their risk. In this report the risk of the attack and attack name are shown.

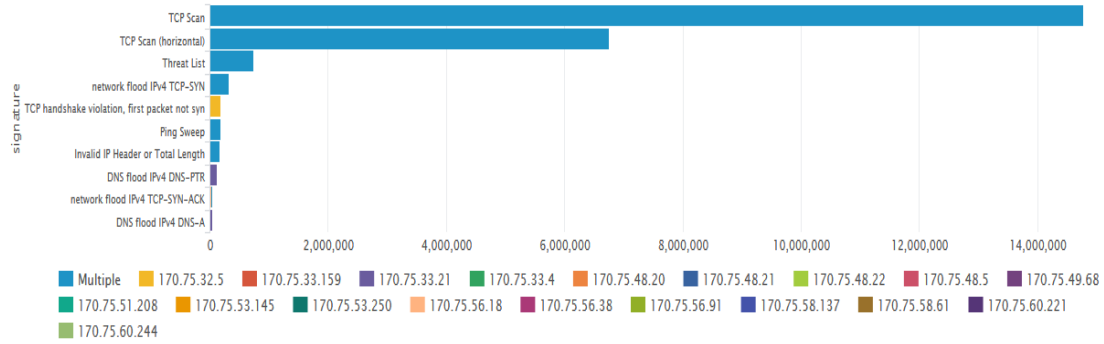


Graph: Top Attacks Blocked by Source

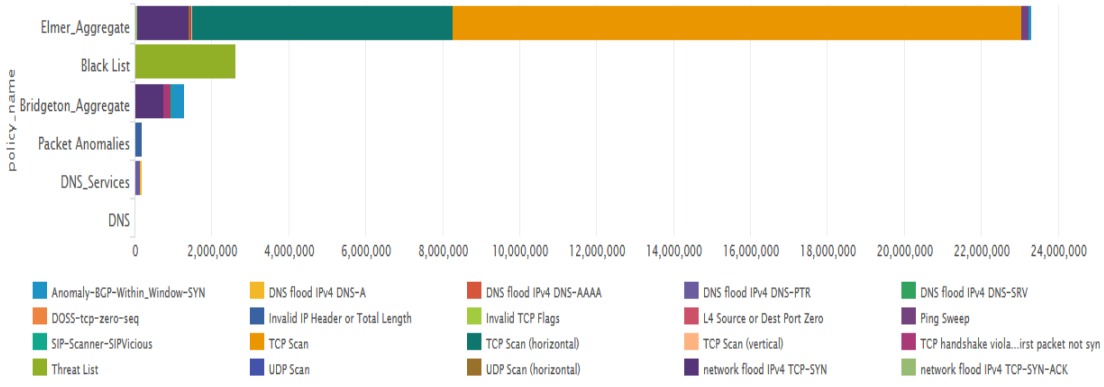
This report provides information on the top attacks blocked, categorized by attacks for each source that was the source of attacks along with the attack name and the number of attacks that triggered with this combination.



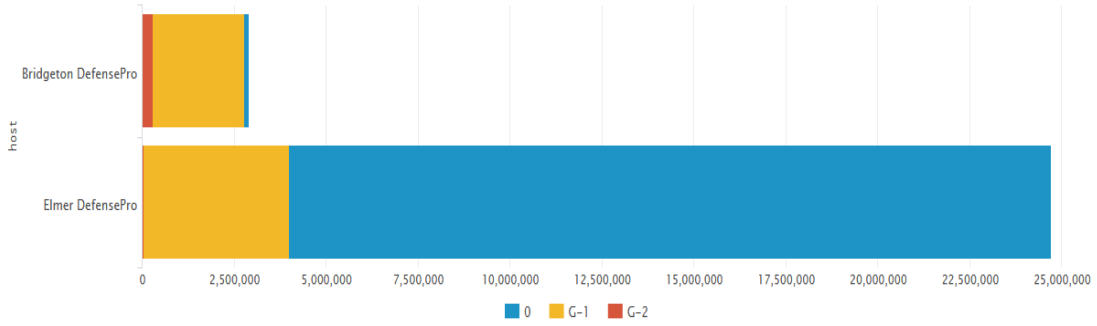
Graph: Top Destinations by Attacks Blocked
This report provides information on the attacks attempted for the most number of times on the destination's protected system IPs.



Graph: Attacks Blocked by Network Security Rule
This report lists the attacks per network security rule, listing the attack name.



Graph: Attacks Blocked by Physical Port (per single IPS device)
This report lists the attacks per physical port.



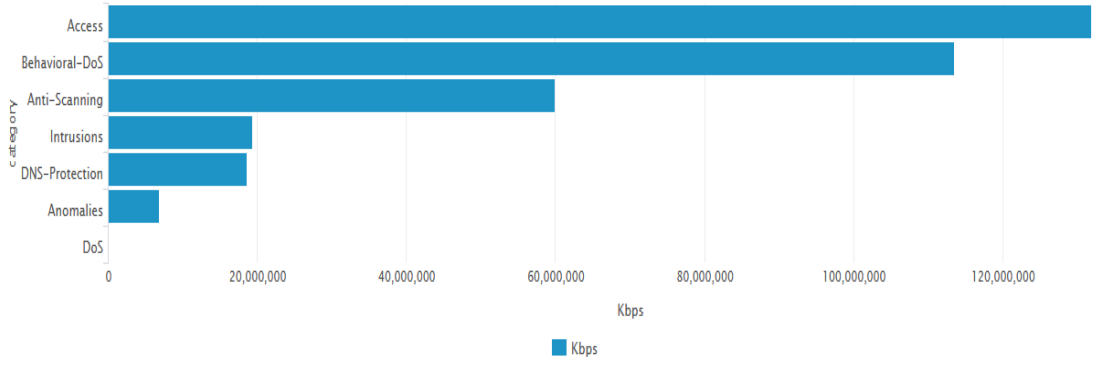
Bandwidth

The following diagram shows the bandwidth of the attacks for the month.

Category	Gbps	Mbps
Access	125.74	128760.31
Behavioral-DoS	108.30	110903.75
Anti-Scanning	57.15	58522.92
Intrusions	18.46	18899.25
DNS-Protection	17.71	18139.41
Anomalies	6.57	6732.76
DoS	0.06	65.39
HttpFlood	0.00	0.00
SynFlood	0.00	0.00
Total Bandwidth in Gbps/Mbps	333.99	342023.79

Graph: Attack Categories Blocked by Bandwidth

This report shows the attack categories based on the BW of the attacks sharing the same category including Kbps.



Managed Vulnerability Service (MSS-VM) Intelligence Section

The Managed Vulnerability Service (MSS-VM) enables organizations to minimize the risk of vulnerabilities by quickly discovering weaknesses, measuring the potential risk and exposure, reporting, providing remediation information necessary to mitigate those risks on an on-going basis and facilitating reporting and compliance with regulations and best practices.

The purpose of this section is to highlight intelligence gathered from this and other services under contract as well as outside sources such honeypots, known malicious sources, vulnerability databases, relationships with CERT and CSIRT teams that GLESEC possesses, together with various other threat feeds.

The following graphs are dashboards generated by GLESEC's TIP™ platform. These dashboards are representative of metrics for this service.

It is important to establish a vulnerability management program as part of the information security strategy because soon after new vulnerabilities are discovered and reported by security researchers or vendors, attackers engineer exploit code and then launch that code against targets of interest. Any significant delays in finding or fixing software with dangerous vulnerabilities provides ample opportunity for persistent attackers to break through, gaining control over the vulnerable machines and getting access to the sensitive data they contain. Organizations that do not scan for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their systems compromised.

Many of the vulnerabilities will provide CVE data. CVE (Common Vulnerabilities and Exposures) is a list of information security exposures and vulnerabilities sponsored by US-CERT and maintained by the MITRE Corporation. The CVE mission is to provide standard names for all publicly known security exposures as well as standard definitions for security terms. The CVE can be searched online at http://nvd.nist.gov/.

<u>Vulnerability Score</u>

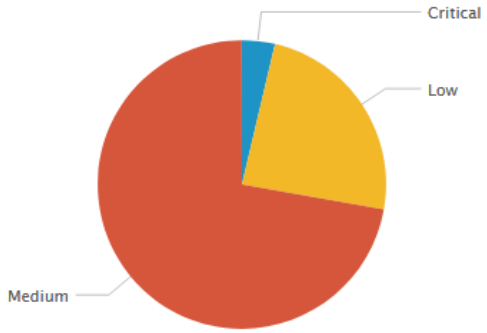
The score of a vulnerability is determined by its risk factor; Critical, High, Medium or Low, as well as its value in the Common Vulnerability Scoring System (CVSS). The CVSS "base score" represents the innate risk characteristic of each vulnerability. CVSS is a vulnerability scoring system designed to provide an open and standardized method for rating IT vulnerabilities. CVSS helps organizations prioritize and coordinate a joint response to security vulnerabilities by communicating the base, temporal and environmental properties of each vulnerability. In addition to numeric

scores, the CVSS provides severity rankings of High, Medium, and Low but these qualitative rankings are simply mapped from the numeric CVSS scores. Vulnerabilities are labeled as:

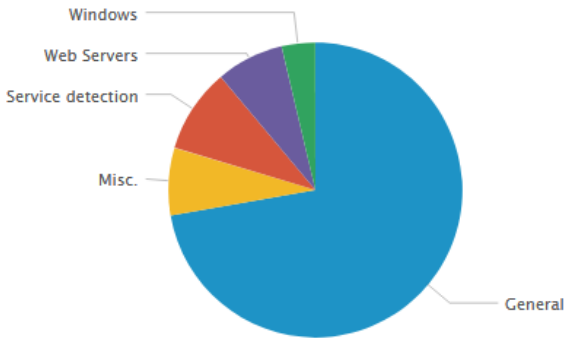
Low risk if they have a CVSS base score of 0.0 – 3.9
Medium risk if they have a CVSS base score of 4.0 – 6.9
High risk if they have a CVSS base score of 7.0 – 10.0

Vulnerability Information

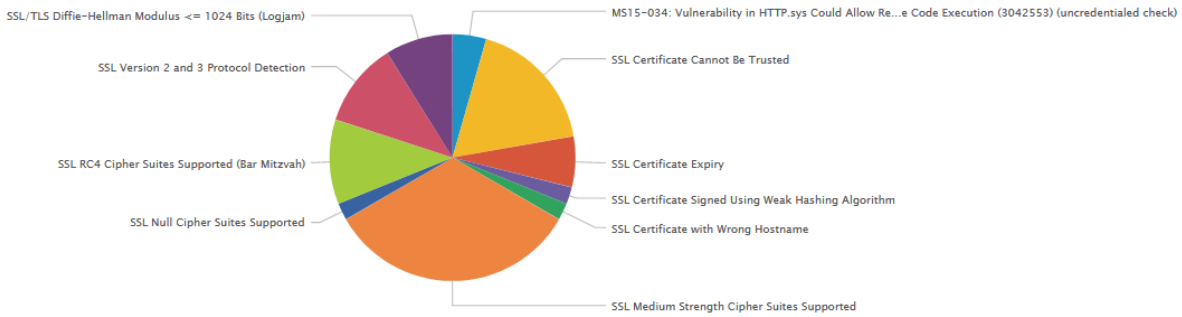
Graph: Risk Distribution
This report depicts the risk distribution of vulnerabilities discovered this report period



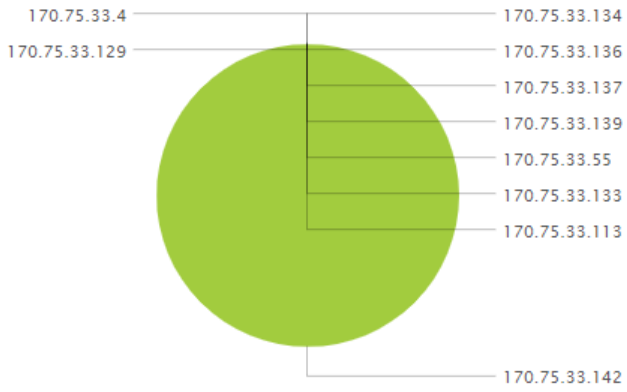
Graph: Most Frequent Vulnerability Category
This report depicts the most frequent vulnerabilities by category discovered this report period



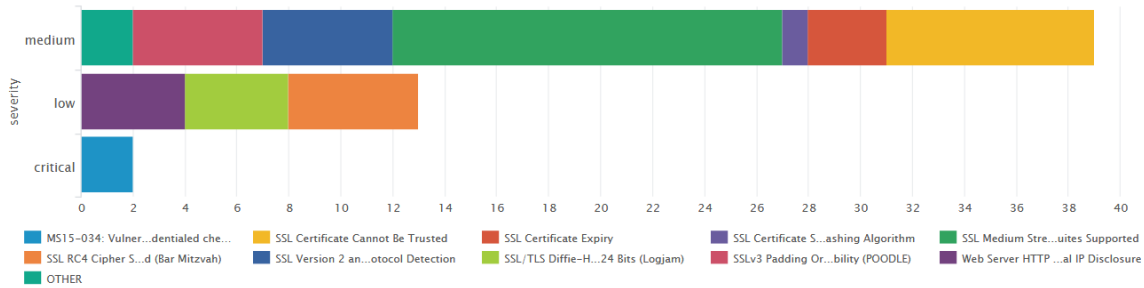
Graph: Most Frequent Vulnerability Name
This report depicts the most frequent vulnerabilities discovered this report period



Graph: Most Vulnerable Host
This report depicts the most vulnerable hosts discovered this report period

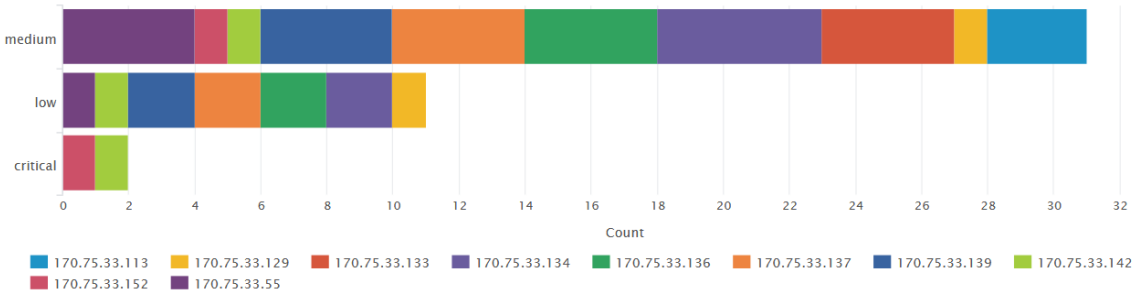


Graph: Vulnerability Risk by Vulnerability Name
This report illustrates the vulnerability risk and count by vulnerability name discovered this report period



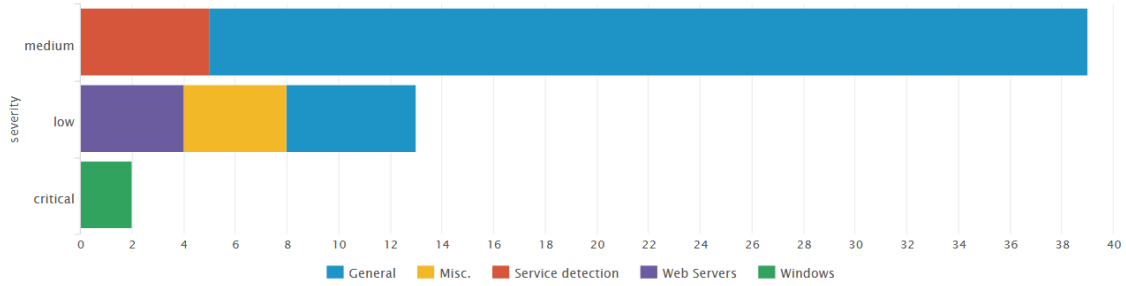
Graph: Vulnerability Risk by Host
This report illustrates the vulnerability risk and count by category discovered this

report period



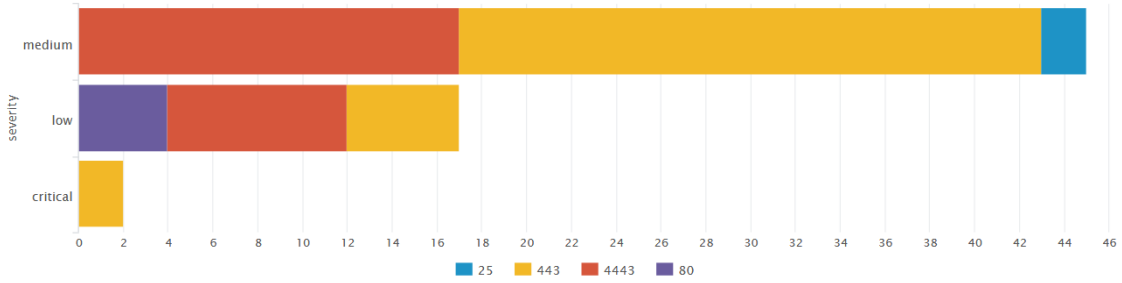
Graph: Vulnerability Risk by Category

This report illustrates the vulnerability risk and count by category discovered this report period



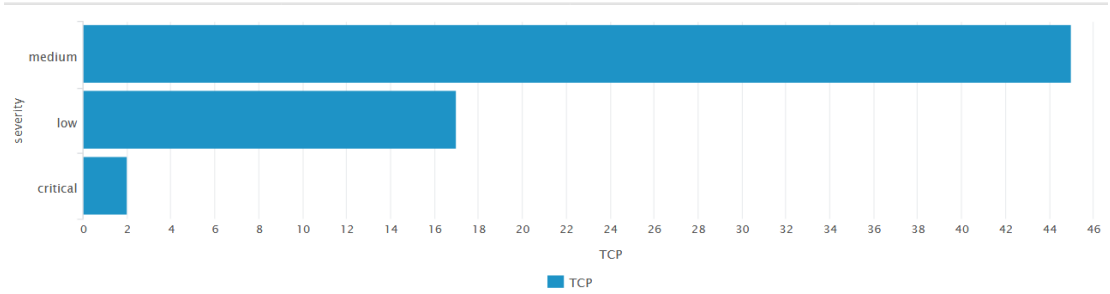
Graph: Vulnerability Risk by Port

This report illustrates the vulnerability risk and count by port discovered this report period

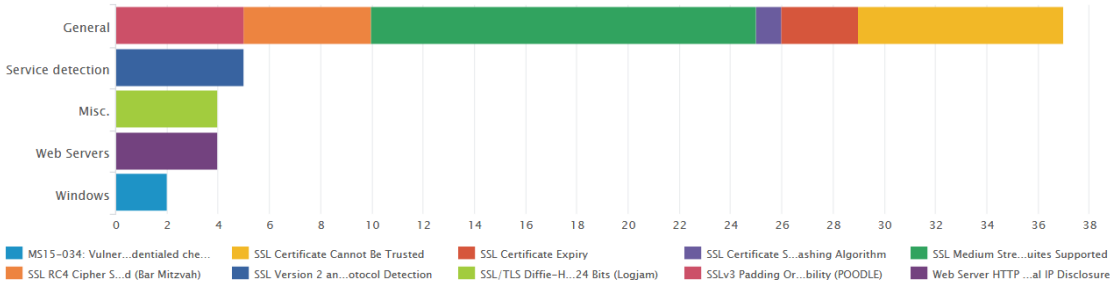


Graph: Vulnerability Risk by Protocol

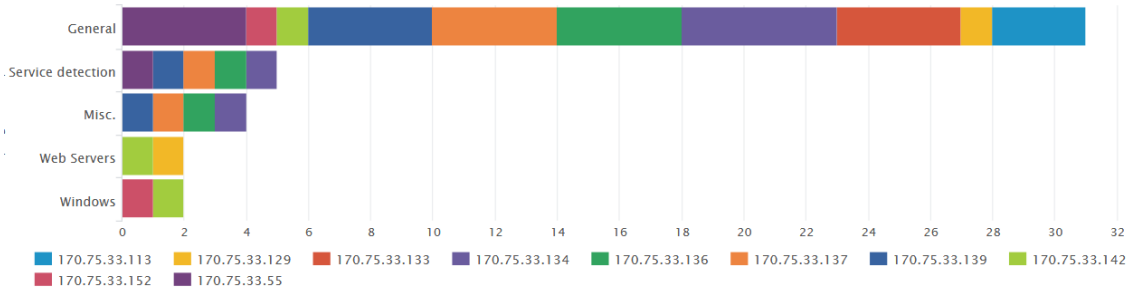
This report illustrates the vulnerability risk and count by protocol discovered this report period



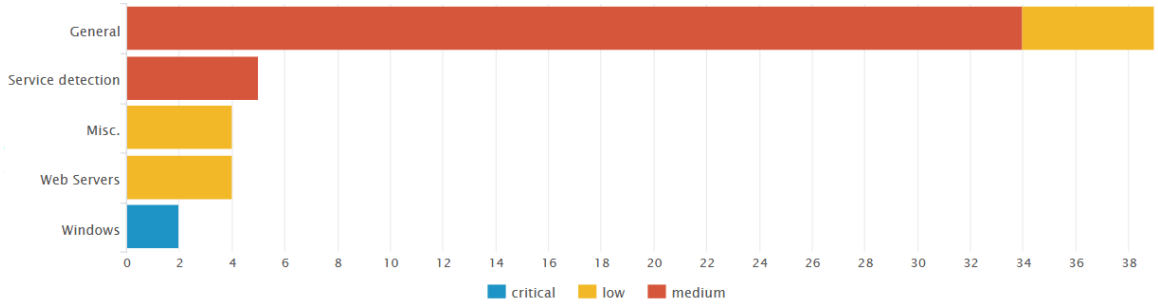
Graph: Vulnerability Category by Vulnerability Name
This report illustrates the vulnerability category and count by vulnerability name discovered this report period



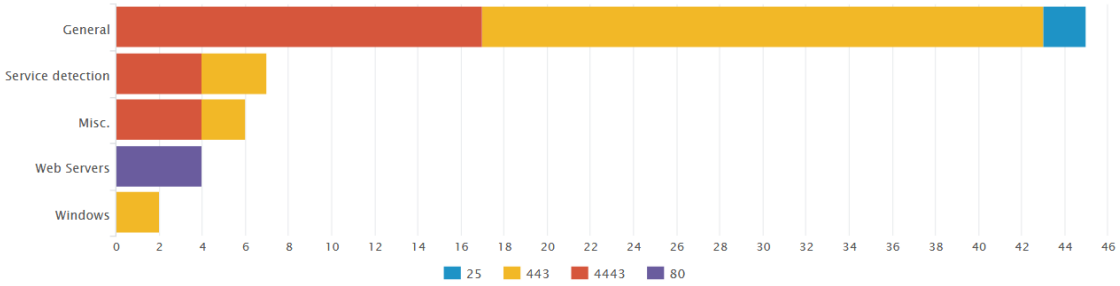
Graph: Vulnerability Category by Host
This report illustrates the vulnerability category and count by host discovered this report period



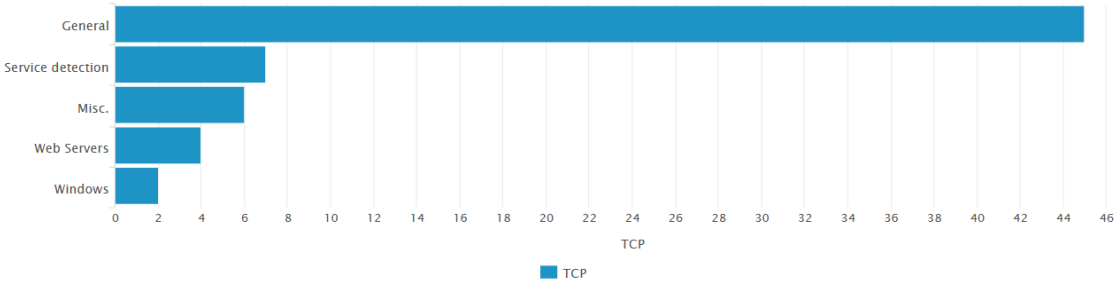
Graph: Vulnerability Category by Risk
This report illustrates the vulnerability category and count by risk discovered this report period



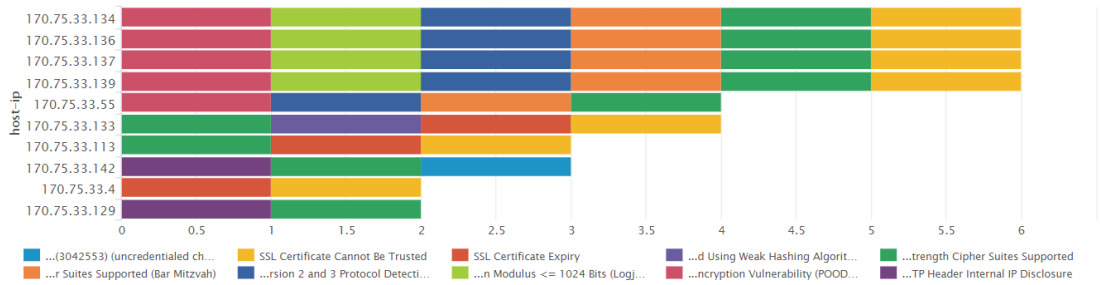
Graph: Vulnerability Category by Port
This report illustrates the vulnerability category and count by port discovered this report period



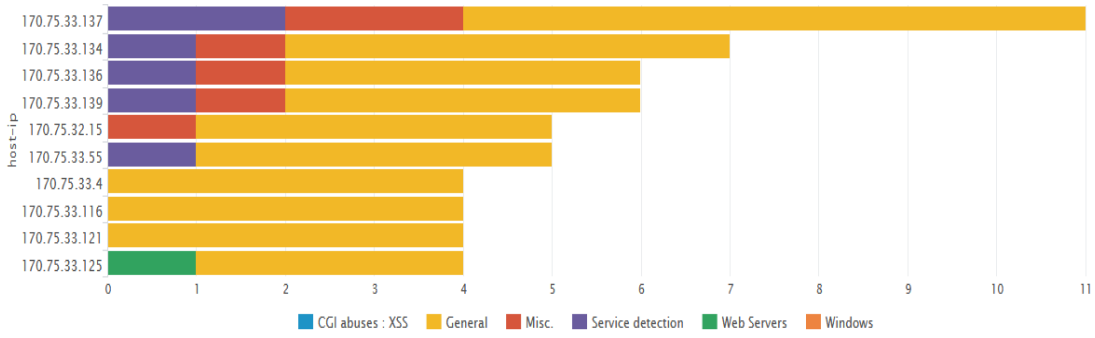
Graph: Vulnerability Category by Protocol
This report illustrates the vulnerability category and count by protocol discovered this report period



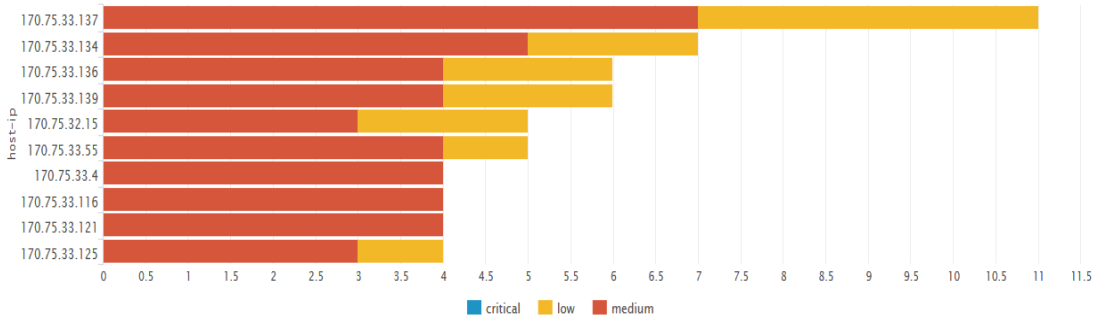
Graph: Host by Vulnerability Name
This report illustrates the vulnerability name and count by hosts discovered this report period



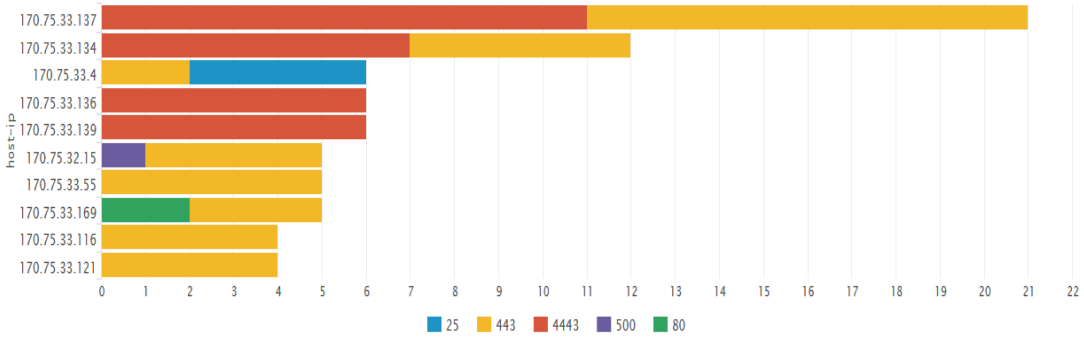
Graph: Host by Vulnerability Category
This report illustrates the vulnerability category and count by hosts discovered this report period



Graph: Host by Vulnerability Risk
This report illustrates the vulnerability risk and count by hosts discovered this report period

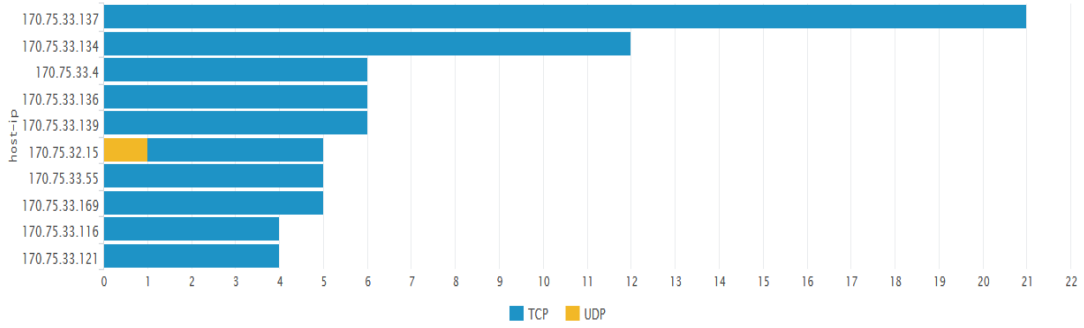


Graph: Host by Port
This report illustrates the port and count by hosts discovered this report period



Graph: Host by Protocol

This report illustrates the protocol and count by hosts discovered this report period



Cyber Security Operations

The purpose of this section is to highlight the activities performed by GLESEC's Global Operations Center (GOC) including: monitoring availability and performance of services under contract, Change Management, Incident Response activities and Consulting Activities.

MONITORING AVAILABILITY

This section reports on the availability of the countermeasures under GLESEC's contract.

The DefensePro Bridgeton was considered up and available 100% during this report period.

Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	31d 0h 0m 0s	100.000%	100.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	31d 0h 0m 0s	100.000%	100.000%
DOWN	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	31d 0h 0m 0s	100.000%	100.000%

State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
PING	99.989% (99.989%)	0.000% (0.000%)	0.000% (0.000%)	0.011% (0.011%)	0.000%
Average	99.989% (99.989%)	0.000% (0.000%)	0.000% (0.000%)	0.011% (0.011%)	0.000%

The DefensePro Elmer was considered up and available 100% during this report period.

Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	31d 0h 0m 0s	100.000%	100.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	31d 0h 0m 0s	100.000%	100.000%
DOWN	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	31d 0h 0m 0s	100.000%	100.000%

State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
PING	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%

MONITORING PERFORMANCE OF COUNTERMEASURES

In this section we monitor and report on the response time from GLESEC IDCs to the countermeasures under GLESEC management.

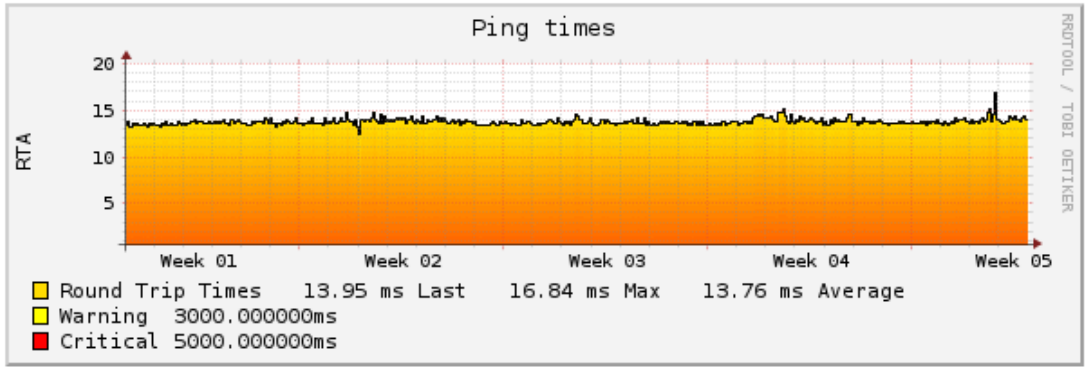
Round trip ping times averaged 13.76 ms from the GLESEC GOC to Inspira Health Network with 0 % average packet loss.

Service overview for "Bridgeton_DefensePro_516"

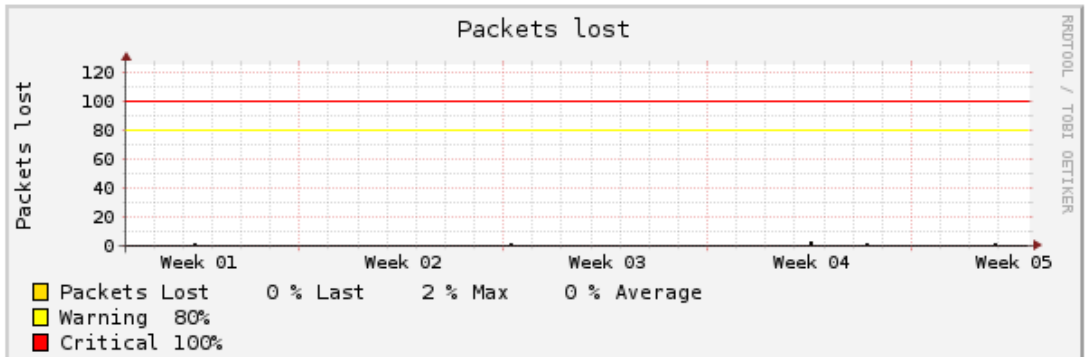
Host: Bridgeton DefensePro 516 **Service:** Host Perfdata

Custom time range 01.01.18 0:00 - 01.02.18 0:00

Datasource: Round Trip Times

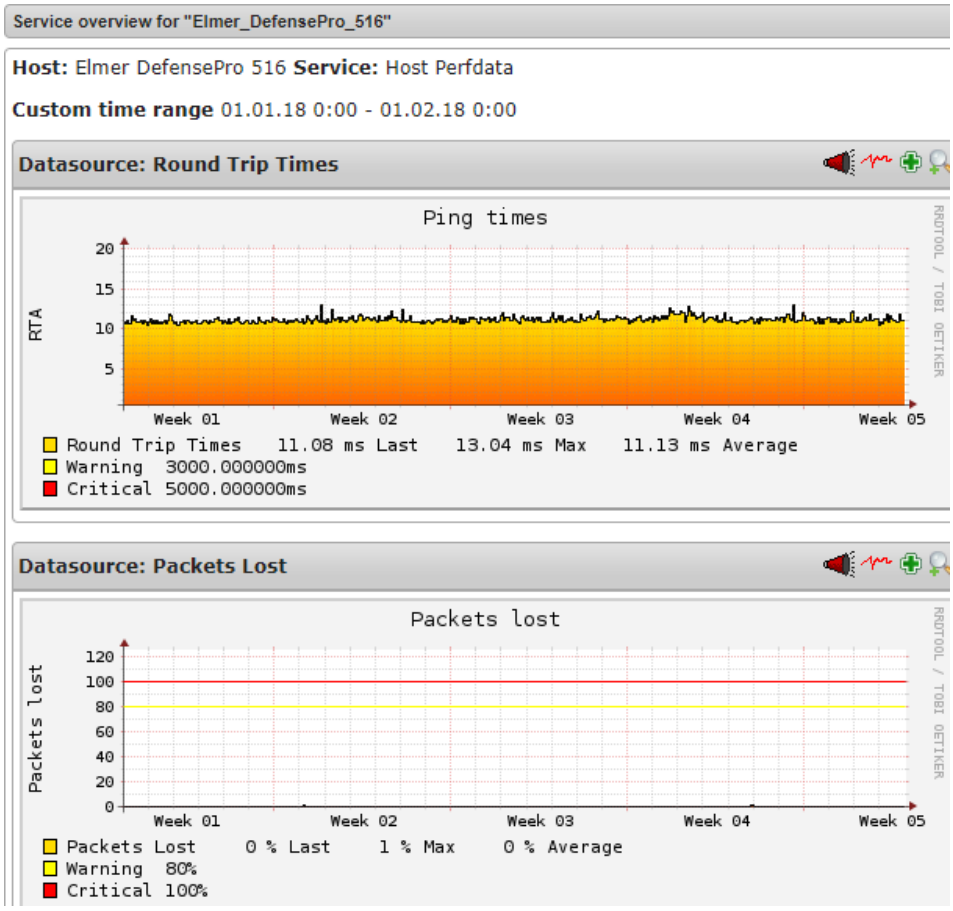


Datasource: Packets Lost



Inspira Health Network DefensePro Elmer Host Performance
Round trip ping times averaged 13.04 ms from the GLESEC GOC to Inspira Health Network with 0 % average packet loss.

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355



TICKET ACTIVITY

In this section we report on all the change management and incidents tickets for the month.

Incidents Reported to the client

Ticket#	Title	Priority
2018020710000011	Incident Notification-1154(IHN)	2 high

Definitions

A more complete list is available on the GMP portal

High Vulnerabilities are defined as being in one or more of the following categories: Backdoors, full Read/Write access to files, remote Command Execution, Potential Trojan Horses, or critical Information Disclosure (e.g. passwords).

Medium Vulnerabilities describes vulnerabilities that either expose sensitive data, directory browsing and traversal, disclosure of security controls, facilitate unauthorized use of services or denial of service to an attacker.

Low Vulnerabilities describes vulnerabilities that allow preliminary or sensitive information gathering for an attacker or pose risks that are not entirely security related but maybe used in social engineering or similar attacks.

SMB/NetBIOS vulnerabilities could allow remote code execution on affected systems. An attacker who successfully exploits these vulnerabilities could install programs; view, change, or delete data; or create new accounts with full user rights. Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.

Simple Network vulnerabilities affect protocols like NTP, ICMP and common network applications like SharePoint among others. This is not meant to be a comprehensive list.

Authentication and encryption are two intertwined technologies that help to insure that your data remains secure. Authentication is the process of insuring that both ends of the connection are in fact “who” they say they are. This applies not only to the entity trying to access a service (such as an end user) but to the entity providing the service, as well (such as a file server or Web site). Encryption helps to insure that the information within a session is not compromised. This includes not only reading the information within a data stream, but altering it, as well.

While authentication and encryption each has its own responsibilities in securing a communication session, maximum protection can only be achieved when the two are combined. For this reason, many security protocols contain both authentication and encryption specifications.

Authentication and encryption are two intertwined technologies that help to insure that your data remains secure. Authentication is the process of insuring that both ends of the connection are in fact “who” they say they are. This applies not only to the entity trying to access a service (such as an end user) but to the entity providing the service, as well (such as a file server or Web site). Encryption helps to insure that the information within a session is not compromised. This includes not only reading the information within a data stream, but altering it, as well.

While authentication and encryption each has its own responsibilities in securing a communication session, maximum protection can only be achieved when the two are combined. For this reason, many security protocols contain both authentication and encryption specifications.

USA-ARGENTINA-PANAMA
México-Perú-Brasil- Chile

Tel: +1 609-651-4246
Tel: +507-836-5355

Info@glesec.com
www.glesec.com