OPERATIONS & INTELLIGENCE EXECUTIVE CYBER SECURITY REPORT

Inspira Health Network

October, 2018

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	12/31/2018
Threat Mitigation	MSS-APS-SSL		
Threat Mitigation	MSS-APS-PS		
Threat Mitigation	MSS-APFW		
Vulnerability Testing	MSS-VME	YES	12/31/2018
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 October, 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.

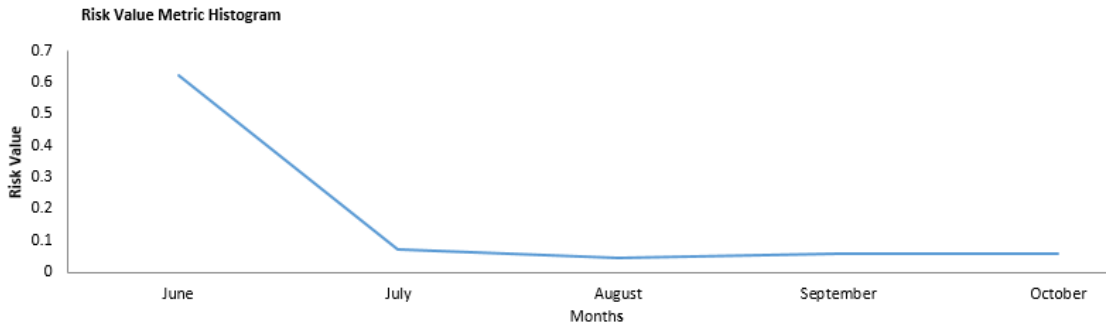
We at GLESEC measure RISK through a number of perspectives and using several of

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.

We determine that the risk condition for the Inspira Health Network for the month of August is high. This can be seen in the security indicator as indicated below.

Risk Indicator	**Service**	**Condition**	**Comments**
Risk Value Metric	MSS-VME	**HIGH**	3 high vulnerabilities are reported. Any one of these can cause an impact to the IHN.

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



For this period 56 hosts were discovered, of which 10 had at-least one vulnerability. Thus, the Risk Score Value changed very little. It remains very similar to previous month's one.

For GLESEC, it is important to know if these servers should be 100% operational throughout the day or if they experience a downtime at specific times.

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

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.

The total number of vulnerabilities for this period is 32 which represents can increase from September, which was 27; these are classified as follows:

- 3 high-risk vulnerabilities
- 16 for medium risk
- 12 for low risk

The number of vulnerabilities is similar to that of the previous month, with the difference that their vulnerable systems remained 10 for the month of October.

The details of your vulnerabilities are detailed in our monthly technical report

The vulnerabilities present in this month can be categorized as:

- 22 in General
- 2 on web servers
- 2 in Miscellaneous
- 4 in service detection
- 1 in Windows

The most vulnerable hosts for this month are:

- 170.75.33.166
- 170.75.33.139
- 170.75.49.35

The vulnerabilities in the hosts are mostly:

- SSL vulnerabilities (SSL Medium Strength Cipher Suites Supported, SSL Version 2 and 3 Protocol Detection (this is the high severity one)
- SSL Certificate Cannot Be Trusted
- SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE))

The proper configuration of the certificates will mitigate all these vulnerabilities. These represent a medium risk, a malicious attacker could exploit the vulnerabilities to act as an intermediary, usurping the legitimate origin connection and intercepting the client's information.

The port considered most vulnerable for this period was 443 (HTTPS) and 4443 (alternative HTTPS). It is necessary to mitigate the vulnerabilities that are directed to these ports because they are generally exposed to the Internet.

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 this 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 Health Network was scanned for vulnerabilities.

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

The following table indicates the external vulnerability metric.

Total IP's Scanned	IP's Vulnerable
56	10

Risk Distribution				
Critical	High	Medium	Low	Total
0	3	16	12	31

According to the metrics:

RV= 0.065956221

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:

Vulnerable Hosts	Critical	High	Medium	Low	Total
170.75.33.166	0	1	4	3	8
170.75.33.139	0	1	3	2	6
170.75.49.35	0	1	3	2	6
170.75.32.15	0	0	2	2	4
170.75.33.159	0	0	1	1	2
170.75.33.160	0	0	1	1	2
170.75.48.100	1	0	1	0	2
170.75.33.124	0	0	0	1	1
170.75.33.167	0	0	1	0	1

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	4	4
170.75.33.102	2	
170.75.33.104	1	
170.75.33.108	2	
170.75.33.112	2	
170.75.33.117	1	
170.75.33.118	1	
170.75.33.122	1	
170.75.33.123	1	
170.75.33.124		1
170.75.33.128	3	
170.75.33.133	1	
170.75.33.136	6	
170.75.33.139	6	6
170.75.33.142	2	
170.75.33.159		2
170.75.33.160		2
170.75.33.166		8
170.75.33.167		1
170.75.33.169	2	
170.75.33.186	3	
170.75.33.58	5	
170.75.48.100	1	2
170.75.49.35	6	6

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	

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

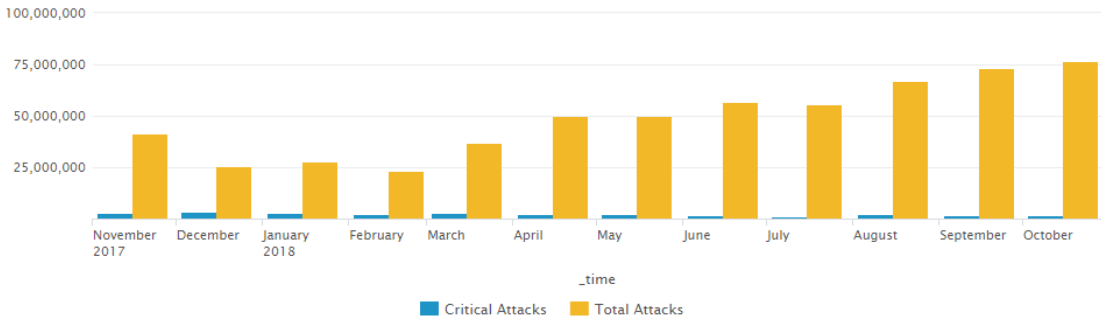
Based on the above the following table shows a matrix of the total external vulnerabilities by category.

Category	Critical	High	Medium	Low	Total
General	0	0	15	7	22
Service detection	0	3	0	1	4
Misc.	0	0	0	2	2
Web Servers	0	0	0	2	2
CISCO	1	0	0	0	1
Windows	0	0	1	0	1

THREATS

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

The Threats as reported by the MSS-APS, MSS-EPS, MSS-SIEM, MSS-EDR, and MSS-UTM for this month are Scanning, Access and Behavioral-DoS. All these threats were identified and dropped.



For the month we observed an increase in the activity of attacks from the previous month of approximately 4% and decrease in the critical attacks of the previous month of approximately
1%.

Most attacks are more than an hour and ten to thirty minutes long; they were directed to several ports, these attacks are usually reconnaissance scans. In the range of more than hour, most of the attacks are reconnaissance (anti-scanning),

followed by anomalies and access attempts.

The ports that receive the most activity are 445, 23 and 1433. Ports 1433 and 445 are targets for scanners, these ports correspond to SQL Server and Windows SMB Protocol, respectively. SMB is a protocol used by Windows to allow access to other computers part of a local network in Windows environments, however many worms and vulnerabilities target this specific port, and Microsoft recommended to close this port to internet connections. Port 23 is usually assigned to telnet service, telnet is a protocol used to access a remote host, the communication between the peers in this protocol is sent in plain text, for this reason this protocol is deprecated and SSH should be used instead. Any existing system in your organization that uses telnet should be configured to use SSH instead to reduce the risk of attacks targeting this protocol and filtering all the connections except for the authorized ones.

Most attacks seem to be reconnaissance (scanning). Approximately 90.4% of the attacks this month came from a scan that can be considered reconnaissance and is used by attackers to find open points in the network. Another of the categories that present attacks are Access with 6.9% and Behavioral-DoS with 2.2%.

The attacks are, for the most part, the Russian Federation (37.77%), Ukraine (19.30%) and United States (12.38%) as the three main sources. Among others, we could recognize TCP Scans and Ping Sweeps that belong to the Anti-Scanning category; and the TCP-SYN network floods that belong to the Behavioral-DoS category.

Based on the information gathered from the security countermeasures during these period **76,874,170** attacks on Inspira Health Network; **1,900,045** of which were considered critical were all stopped by the GLESEC managed security countermeasures.

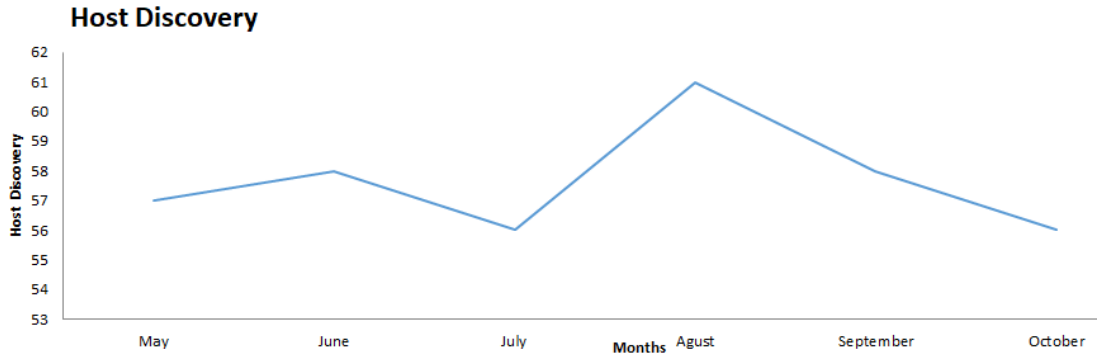
Inspira Health Network receives an average of 45,110,053 total attacks and 1,602,271 critical attacks on a monthly basis. This equates to an average of 2,157,209 total daily attacks and 76,622 critical daily attacks.

ASSETS

The MSS-VM (E/I), MSS-EPS conducts weekly testing. The MSS-VM (E/I) identify network assets while the MSS-EPS identify applications. Depending on the contracted services is the listing that can be provided of system or application assets.

We believe that we cannot protect what we don't know and to know the assets (systems and applications) is critical to having a sound cyber security practice. Therefore we encourage you to verify the information that we provide and let us know if anything is suspicious or just not right. We can work with your organization to create a baseline that can be used to identify deviations. Please contact our GOC for assistance in this matter.

The following histogram shows the past six-month total of number of systems discovered in the perimeter of your organization.



Knowing what is in your network is extremely important. The scans for this period showed 56 hosts discovered, we were unable to reach host: 170.75.33.138, 170.75.33.137, 170.75.33.129, 170.75.33.106, 170.75.33.104

All hosts analyzed during this period correspond to the IPs ranges provided to us from your organization.

COMPLIANCE

The MSS-EPS or Managed End Point Security Service is a Compliance and Remediation Service. For compliance we understand the testing, monitoring and alerting of deviations of the parameters of all "hosts" and "servers" in the organization from established baselines. These baselines can be created to support specific outside requirements or internal best-practice guidelines. The MSS-EPS can monitor deviations to these baselines and also "enforce" compliance with these.

The services that provide us with information for this section have not been contracted

CYBER SECURITY VALIDATION

Security Validation implies the validation of the entire security by conducting testing with simulated attacks. This is conducted with the Managed Breach Attack Simulation Service (MSS-BAS). The MSS-BAS is a collection of advanced pre-exploitation, post- exploitation and awareness testing services. The testing is on real targets based on simulated attacks; therefore these provide conclusive (no false positive) results. The different attack vectors test the organization's configurations, countermeasures, implementations and ability to respond in a continuous fashion producing valuable intelligence and recommendations.

The services that provide us with information for this section have not been contracted.

TRUSTED ACCESS

The new IT model brings with it a greater attack surface, comprised by employees that use their own devices for work, while working remotely. The proliferation of cloud applications for nearly every business need has also contributed to increased technical complexity. These days, attackers can expose much different vulnerability in multiple vectors — in a single attack. Traditional security is designed to address separate, siloes attacks, making these solutions ineffective against modern threats. These new threats center on gaining remote access to your apps and data — whether it's with stolen passwords or exploited known vulnerabilities targeting your users, their out-of- date devices, cloud applications and remote access software.

The Managed Trusted Access Service (MSS-TAS) is a holistic security service to (a) ensure that the users' access is trusted (valid user) and (b) the devices used by the user to authenticate meet the organization's security standards.

The services that provide us with information for this section have not been contracted.

Recommendations

GLESEC recommends for Inspira Health Network to address the following:

1. Take action on every recommendation mentioned on this section

2. Many of the vulnerabilities present in the scanned devices, correspond to the use of SSL protocols, SSL has been deprecated in favor of TLS, also, SSL has many well documented vulnerabilities such as POODLE and Bar Mitzvah. The recommended practice is to implement TLS version 1.1 or higher that is the most secure implementation as of today.

    - The most frequent vulnerability is the SSL Medium Strength Cipher Suites Supported, avoid the use of keys less than 112 bits, or that uses the 3DES encryption set.

3. During this month, multiple ports were target of attacks; but 2 ports were specifically targeted: port 1433 and 445(SMB).

    - HTTPS is the secure extension of the HTTP protocol, widely used for Internet connections. Modern standards recommend the implementation of TLS instead of SSL for authentication. Many of the vulnerabilities discovered, could be exploited through this port.

    - Port 445 is used by the SMB protocol, which has been recognized as vulnerable. Is recommended to verify if there are any systems with this port open to internet connections and filter the connections.

4. Take into consideration the recommendations made on the incident reports.

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

Intelligence Section Per Service Module

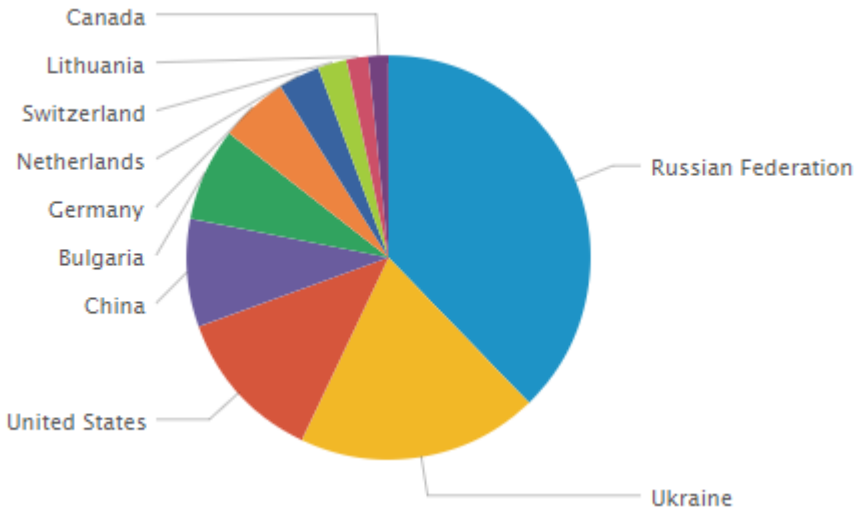
MANAGED ATTACK PROTECTION SERVICE (MSS-APS) SECURITY INTELLIGENCE SECTION

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.

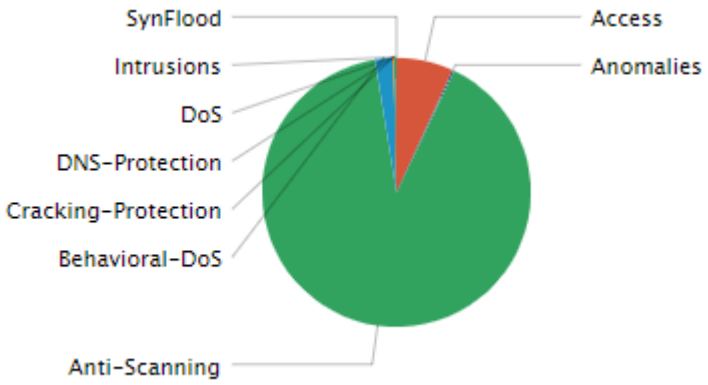
The purpose of this section is to highlight intelligence gathered from the services under contract as well as outside sources such honeypots, known malicious sources, vulnerability databases, relationships with CERT and CSIRT teams that GLESEC possesses, together with various other threat feeds.

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.

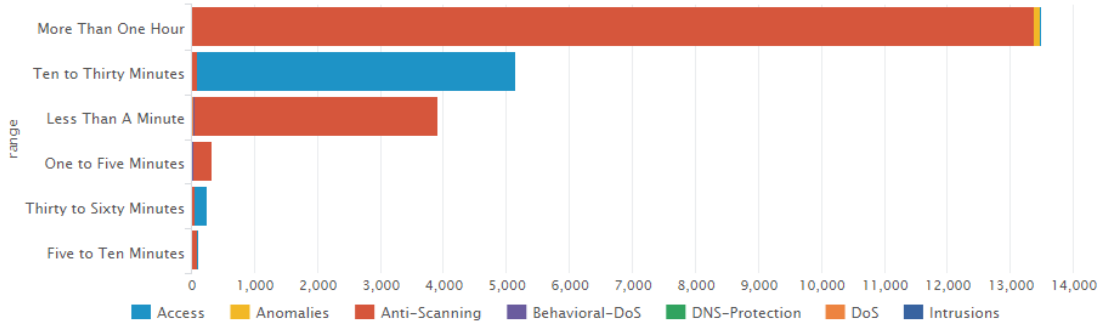


The distribution of attacks per type can be seen in the following diagram.



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	285.03	291867.12
Anti-Scanning	222.09	227420.94
Behavioral-DoS	130.82	133958.65
DNS-Protection	8.68	8884.02
Anomalies	4.03	4128.73
DoS	1.15	1181.27
Intrusions	0.72	735.63
SynFlood	0.07	75.07
Cracking-Protection	0.00	0.00
Total Bandwidth in Gbps/Mbps	652.59	668251.43

*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.

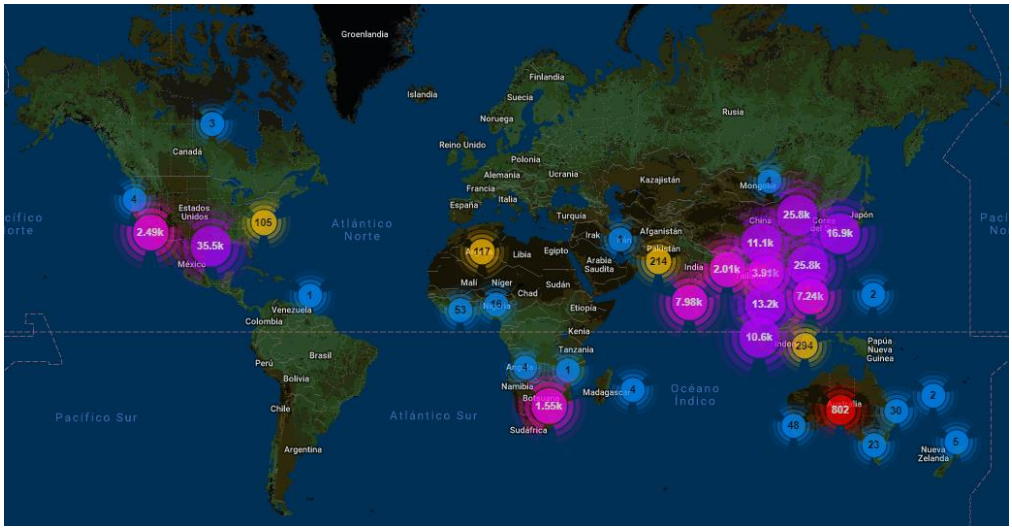
Port Activity

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.

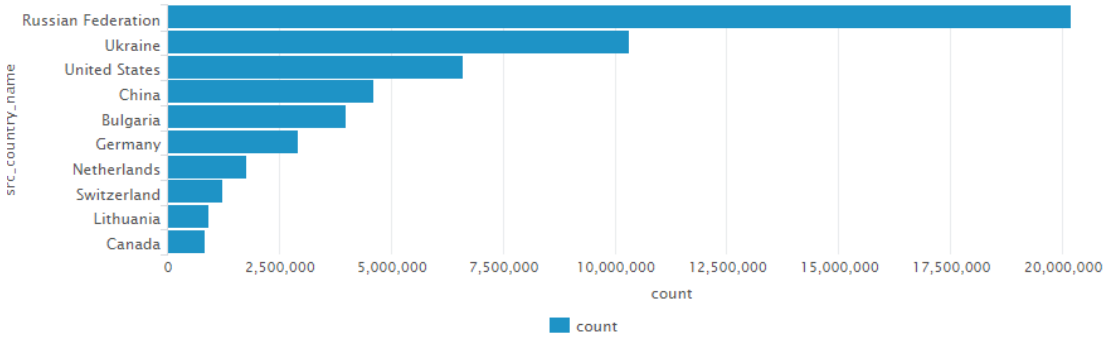
The DefensePro assisted in preventing attacks directed at network and server level which were directed at well-known port numbers as seen in the following diagram.

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.

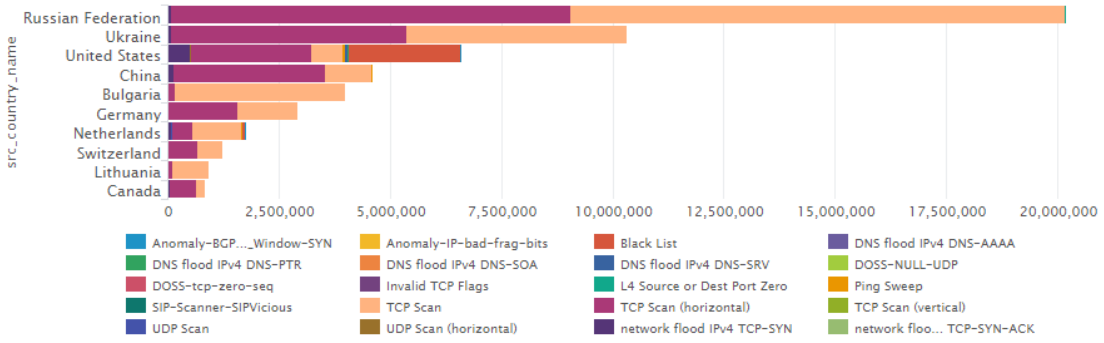
The vast majority of attacks on Inspira Health Network originated geographically from the following countries as seen in the attached diagram. Some results do not include location information that allows map plotting.



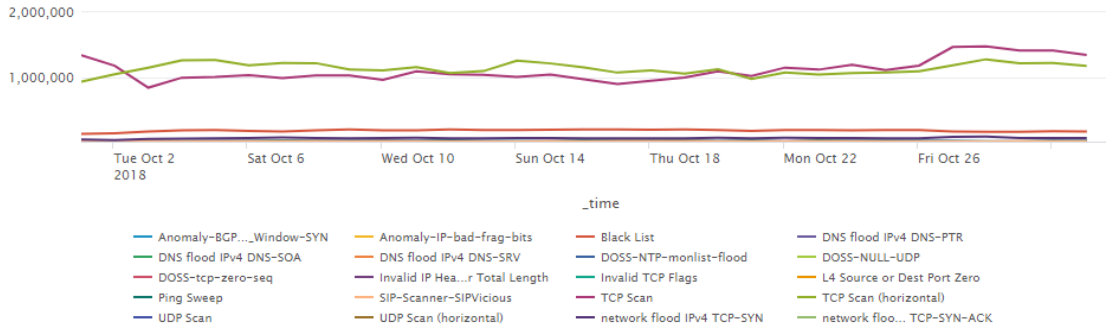
Graph: Top 10 Attacking Countries Blocked
This report provides the count of total attacks blocked by country.



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



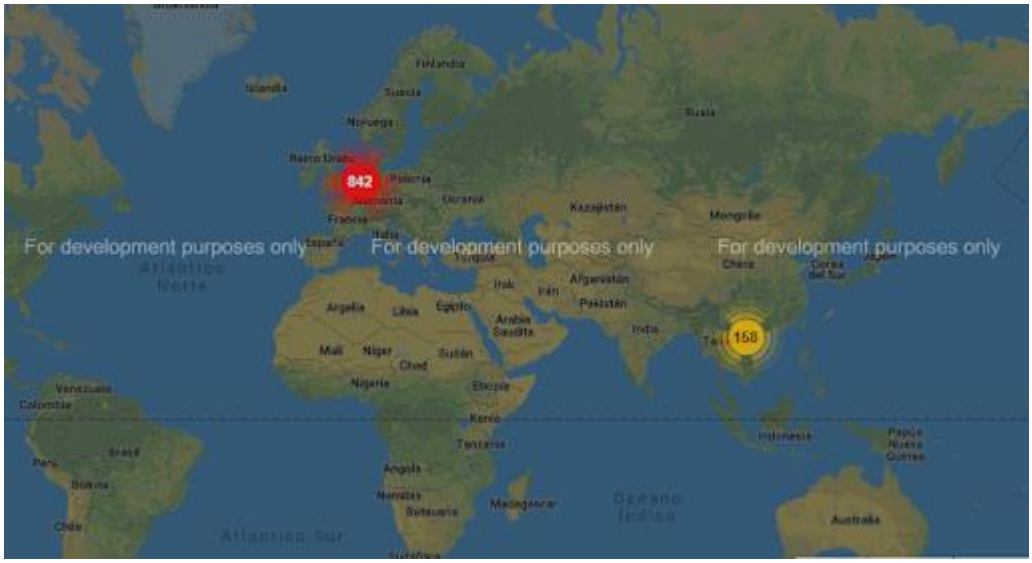
Graph: Attacks Types Blocked by Week
This report provides the count of attacks blocked by week



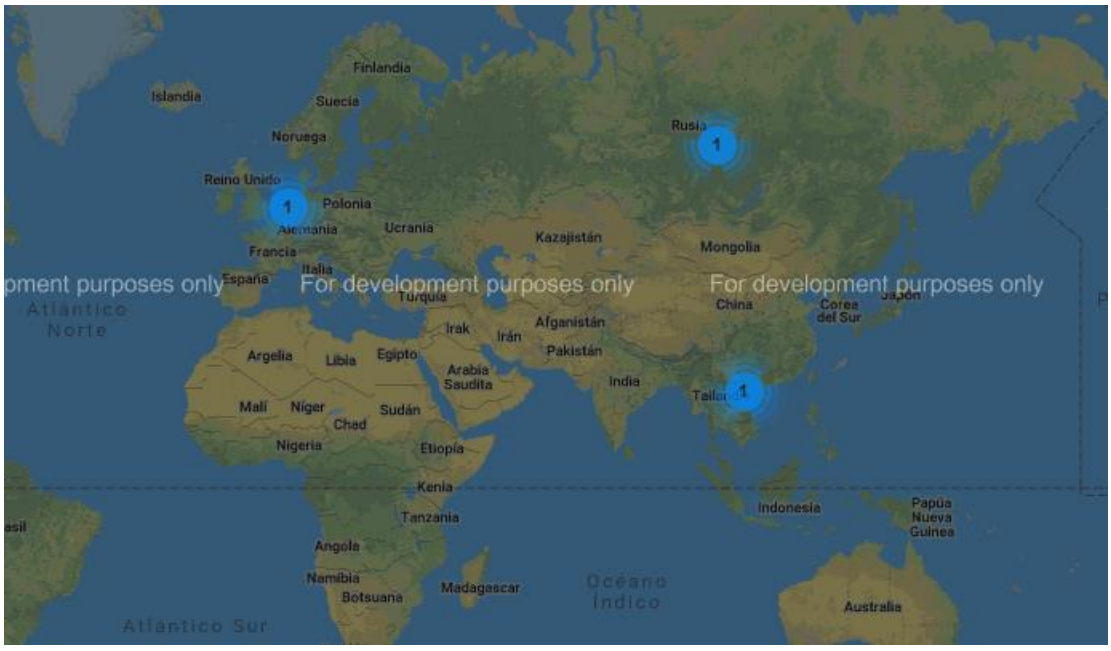
Known Threat Source Information

Of the attacks on Inspira Health Network are from known threat sources that have been compiled and correlated with attack source IPs gathered from the DefensePro attack logs and 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 **856,785** attacks on Inspira Health Network from the DNS Blacklist were obtained by correlating values from the Project Honey Pot Database. Some results do not include location information that allows map plotting.

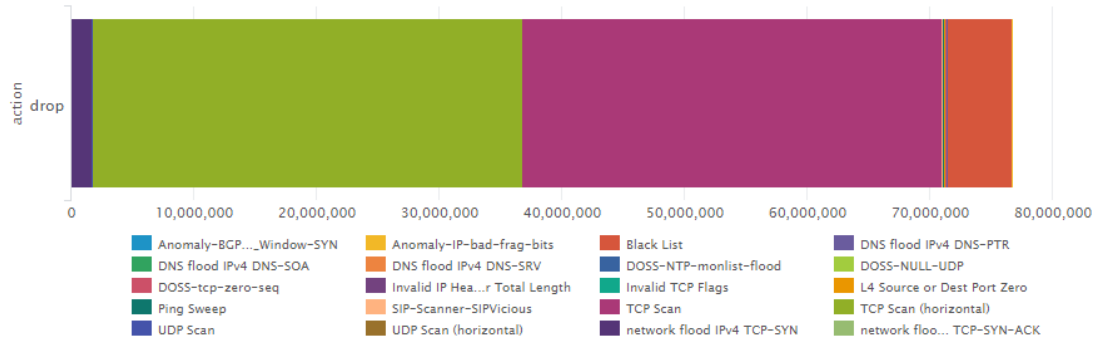


Map of geographic distribution of **856,785** attacks on Inspira Health Network from known threat sources obtained by correlating values from AlienVault Labs; Emerging Threats; Zeus, Spyeye, and Palevo Tracker. Some results do not include location information that allows map plotting



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

rule.



Port Information

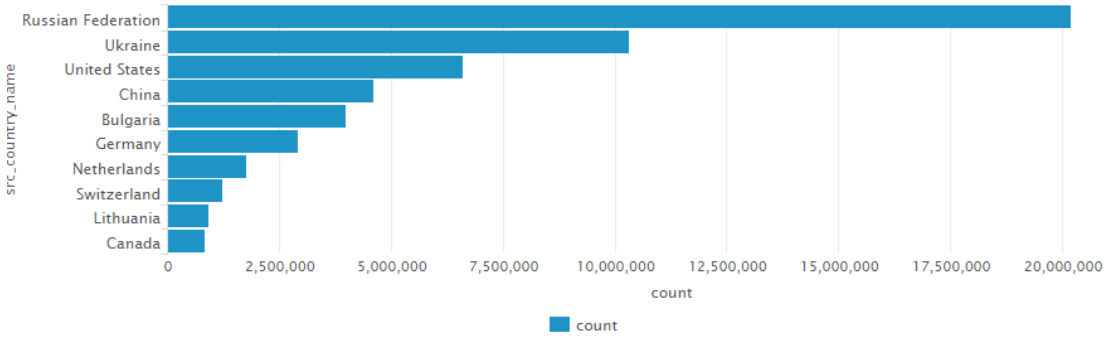
Port Information: Port 80 (http), Port 1443 (ms-sql), Port 8080 (https-alt), Port 3306 (mysql) commonly scanned in order to attack web servers. SQL injection is currently the most common form of web site attack in that web forms are very common, often they are not coded properly and the hacking tools 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.

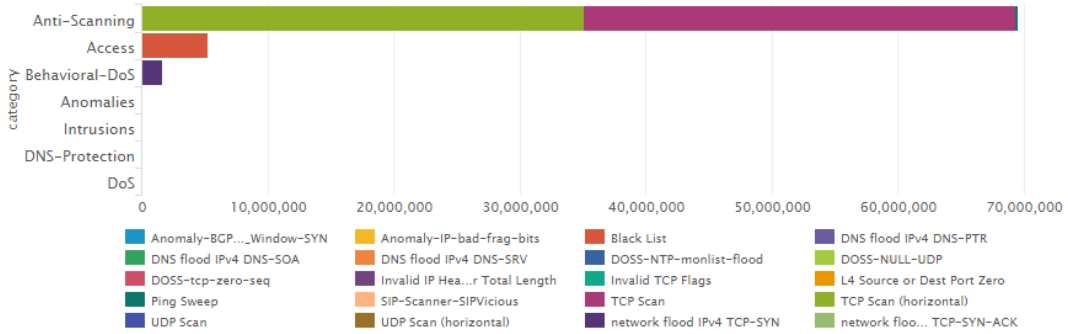
A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete),

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.

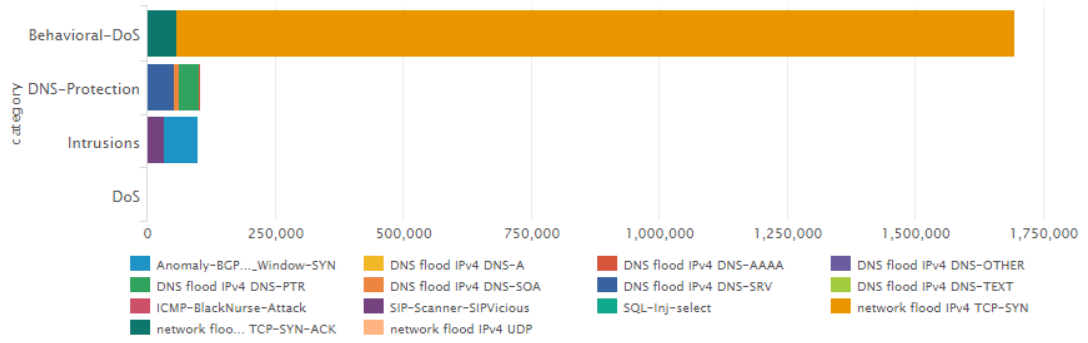
Graph: Attacks Blocked by Destination Port
This report provides information on the total number of attacks blocked that were attempted on which port and for how many times.



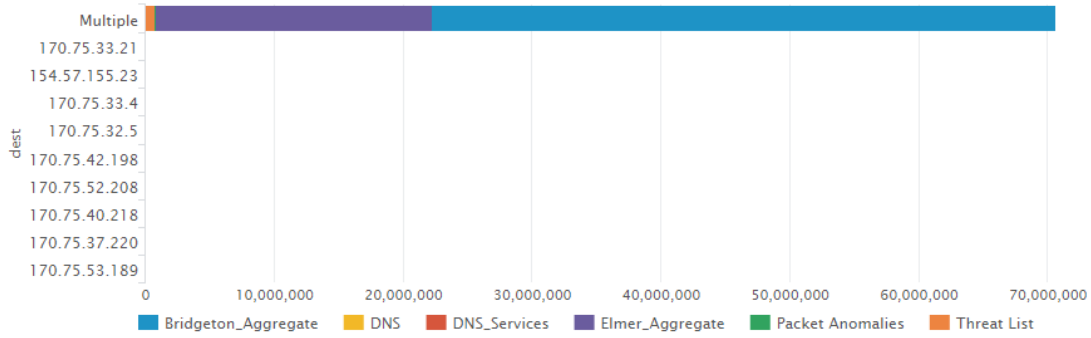
Graph: Attacks Blocked By Threat Category
This report lists the attacks blocked per Attack Category, listing the attack name.



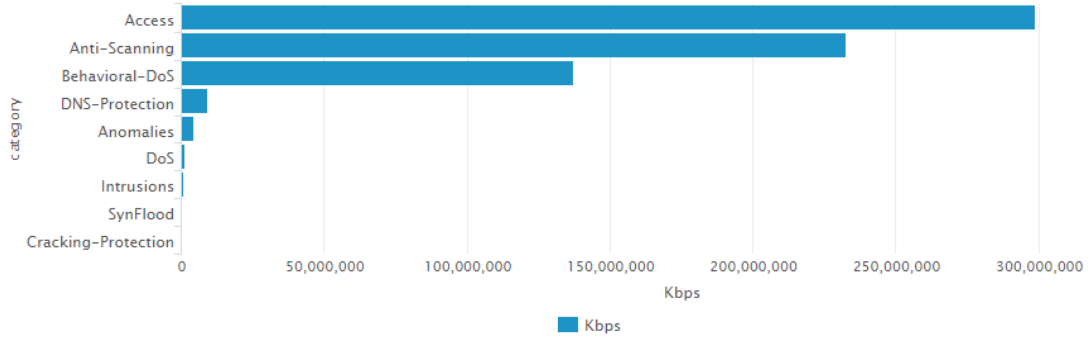
Graph: Critical Attacks Blocked
This report provides Critical Attacks information, attack name, network security rule along with the number of times the attack was launched.



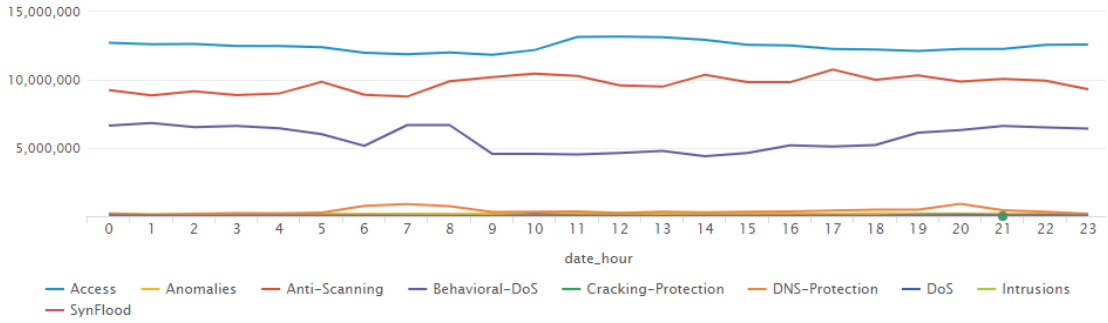
Graph: Top Attacked Destinations Blocked
This report provides information on the system IPs, which were the destination of the attacks for most number of times along with the network security rule.



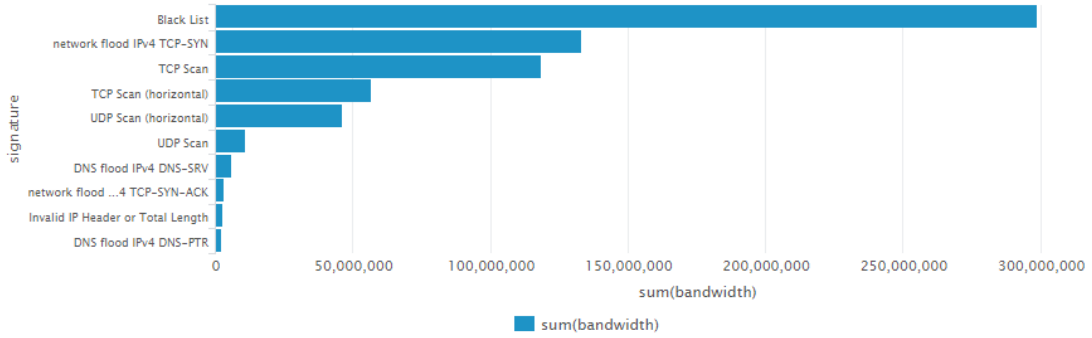
Graph: Attack Categories Blocked by Bandwidth
This report shows the attack categories based on the BW of the attacks sharing the same category including Kbps.



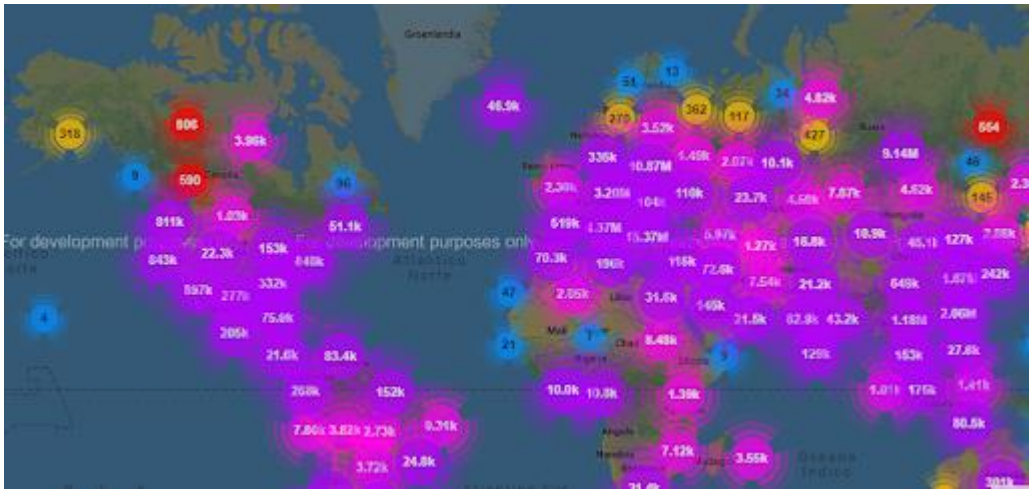
Graph: Bandwidth by Blocked Threat Category by Hour of Day
This report shows the most bandwidth consuming threat categories based on the bandwidth of the attacks sharing the same threat category for each hour of day.



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

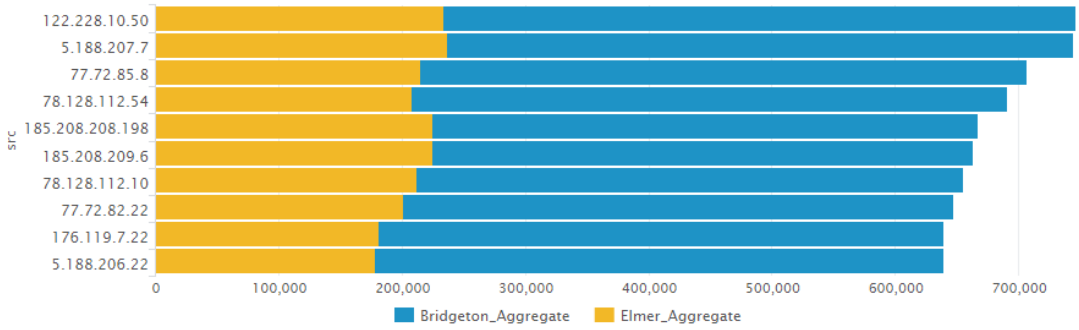


<u>Scanning Information</u>
The following map displays geographic distribution of **69,664,822** attacks on Inspira Health Network from scanning sources. Some results do not include location information that allows map plotting.



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 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.



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>

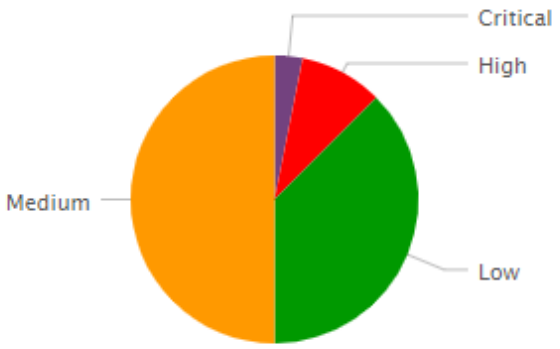
The score of a vulnerability is determined by its risk factor; Critical, High, Medium or Low, as well as its value in the Common Vulnerability Scoring System (CVSS). The CVSS "base score" represents the innate risk characteristic of each vulnerability. CVSS is a vulnerability scoring system designed 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:

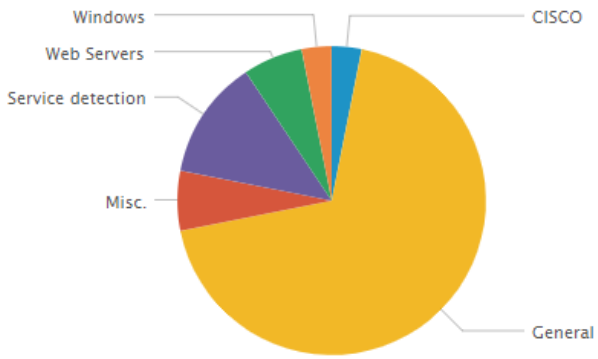
Low risk if they have a CVSS base score of 0.0 – 3.9
Medium risk if they have a CVSS base score of 4.0 – 6.9
High risk if they have a CVSS base score of 7.0 – 10.0

Vulnerability Information

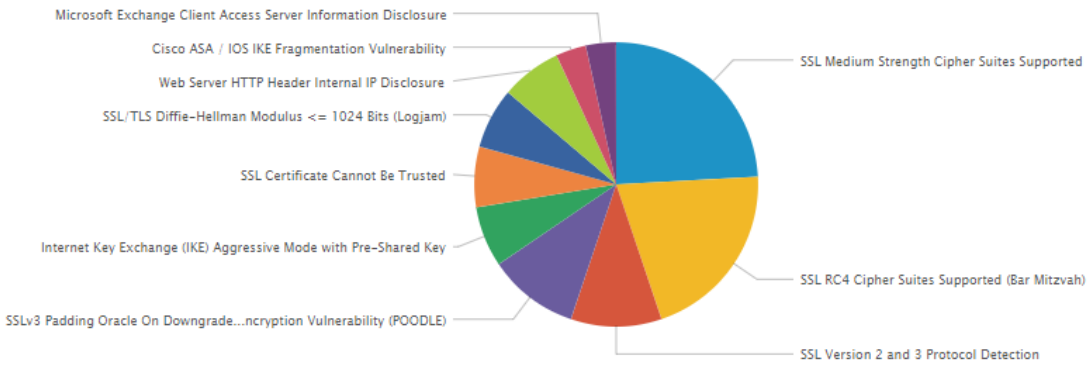
Graph: Risk Distribution
This report depicts the risk distribution of vulnerabilities discovered this report period



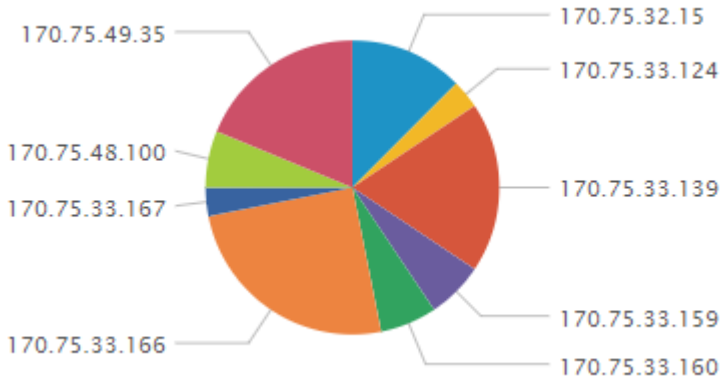
Graph: Most Frequent Vulnerability Category
This report depicts the most frequent vulnerabilities by category discovered this report period



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

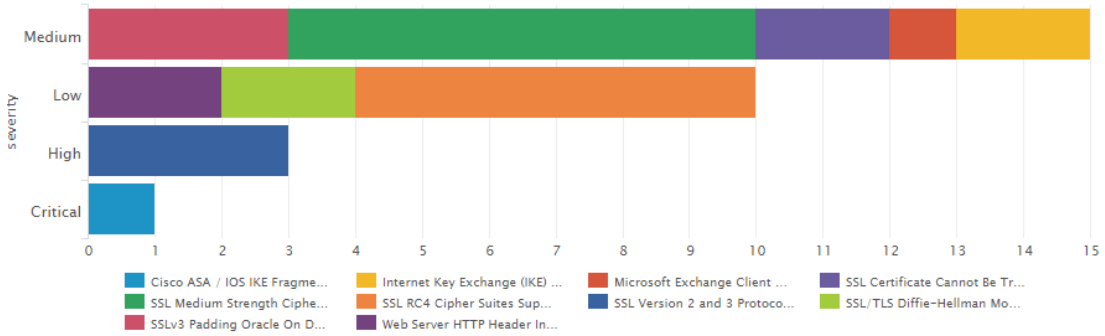


Graph: Most Vulnerable Host
This report depicts the most vulnerable hosts discovered this report period

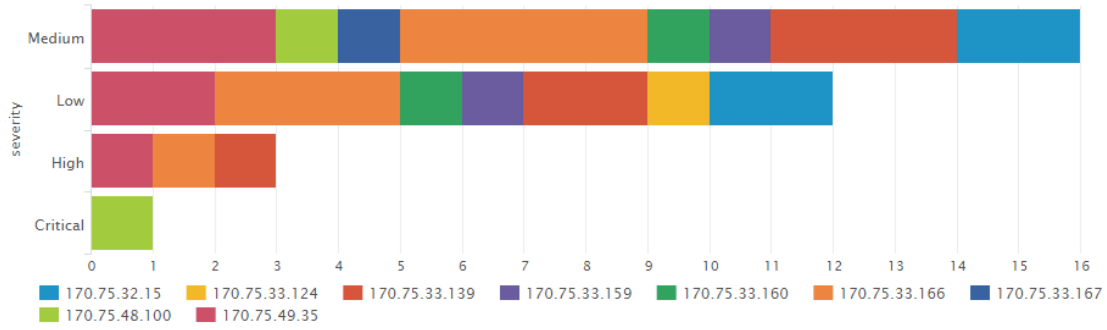


Graph: Vulnerability Risk by Vulnerability Name
This report illustrates the vulnerability risk and count by vulnerability name discovered this report period

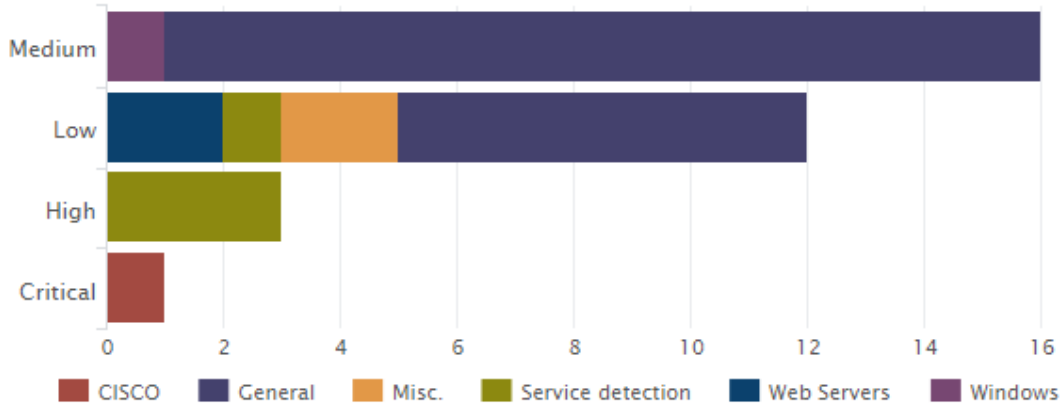
USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355



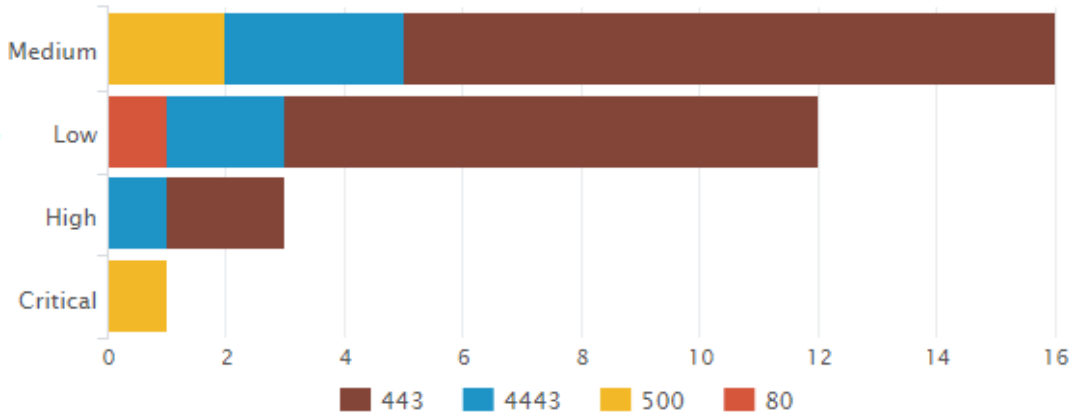
Graph: Vulnerability Risk by Host
This report illustrates the vulnerability risk and count by category discovered this report period



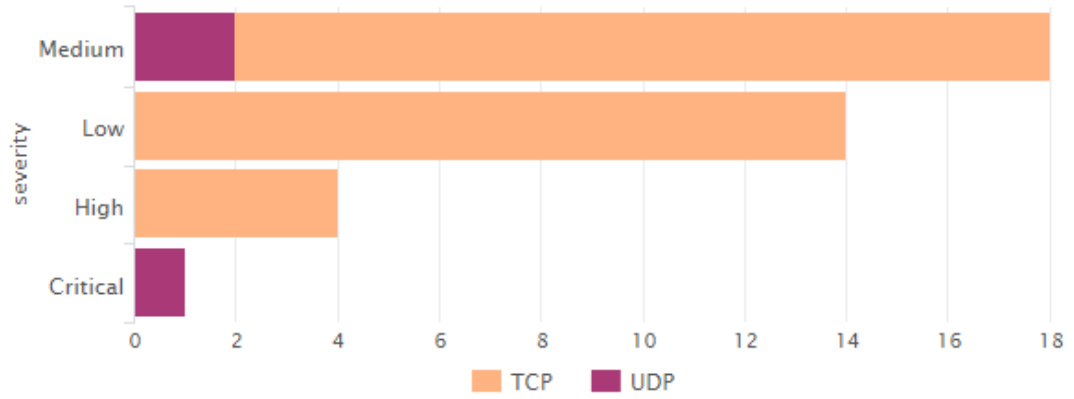
Graph: Vulnerability Risk by Category
This report illustrates the vulnerability risk and count by category discovered this report period



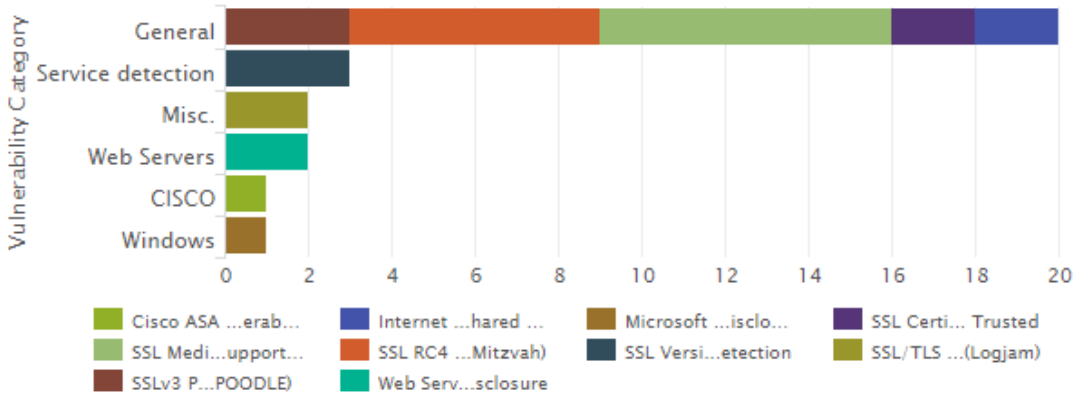
Graph: Vulnerability Risk by Port
This report illustrates the vulnerability risk and count by port discovered this report period



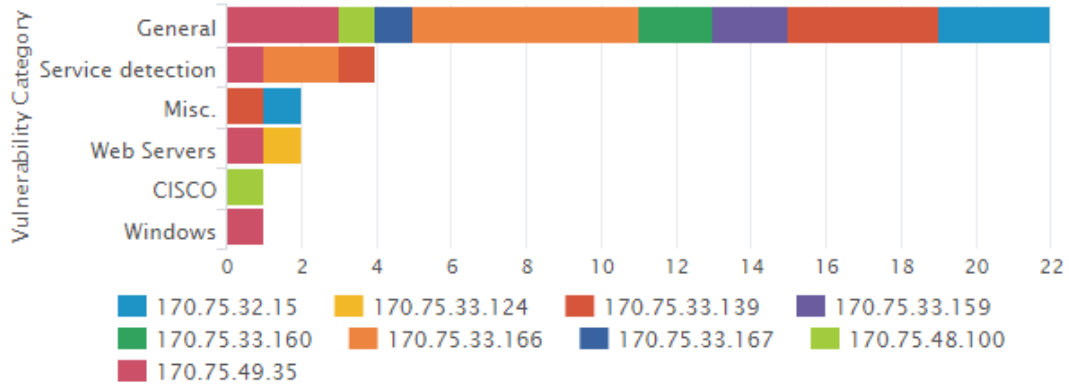
Graph: Vulnerability Risk by Protocol
This report illustrates the vulnerability risk and count by protocol discovered this report period.



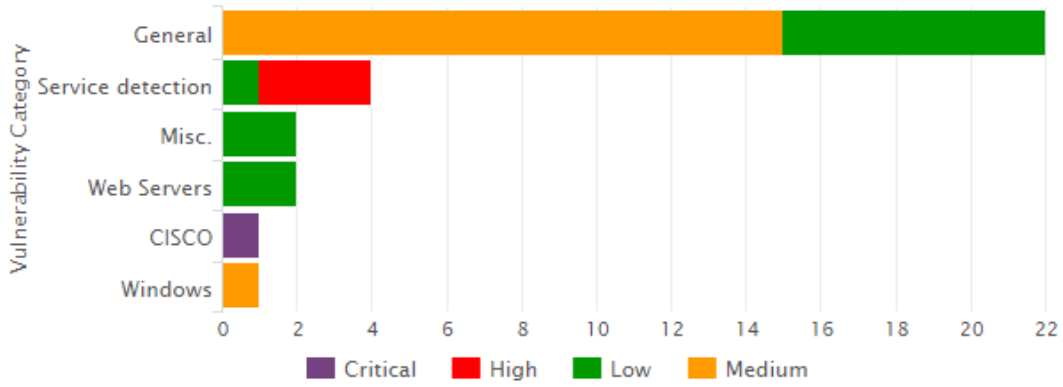
Graph: Vulnerability Category by Vulnerability Name
This report illustrates the vulnerability category and count by vulnerability name discovered this report period



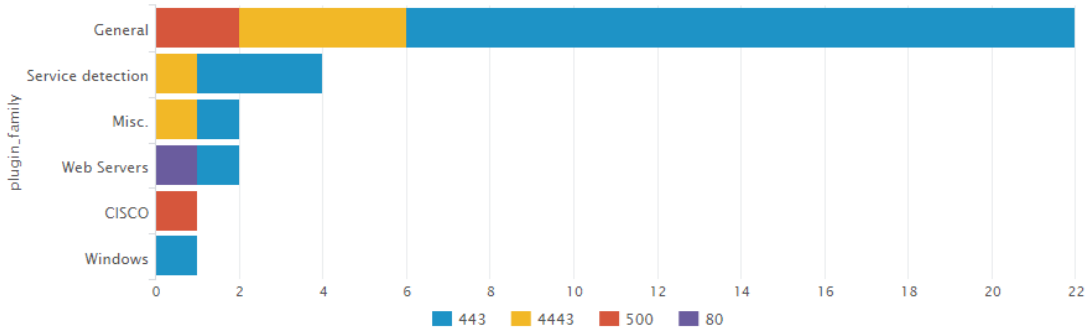
Graph: Vulnerability Category by Host
This report illustrates the vulnerability category and count by host discovered this report period



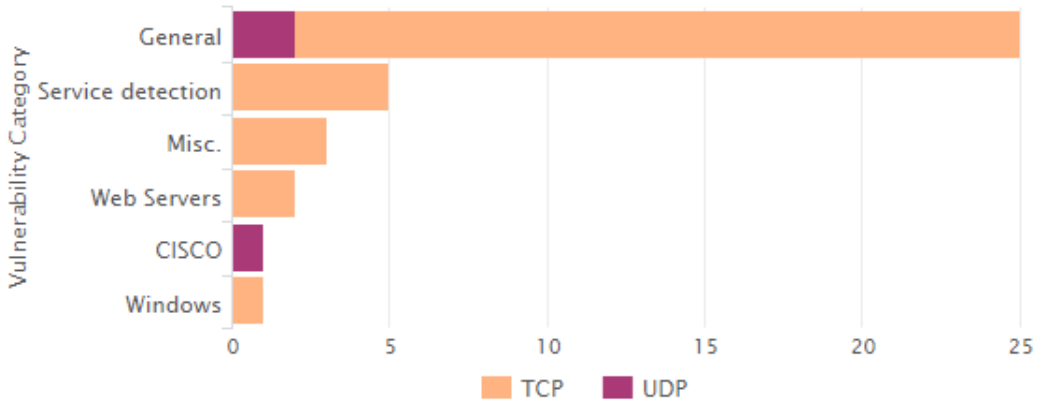
Graph: Vulnerability Category by Risk
This report illustrates the vulnerability category and count by risk discovered this report period



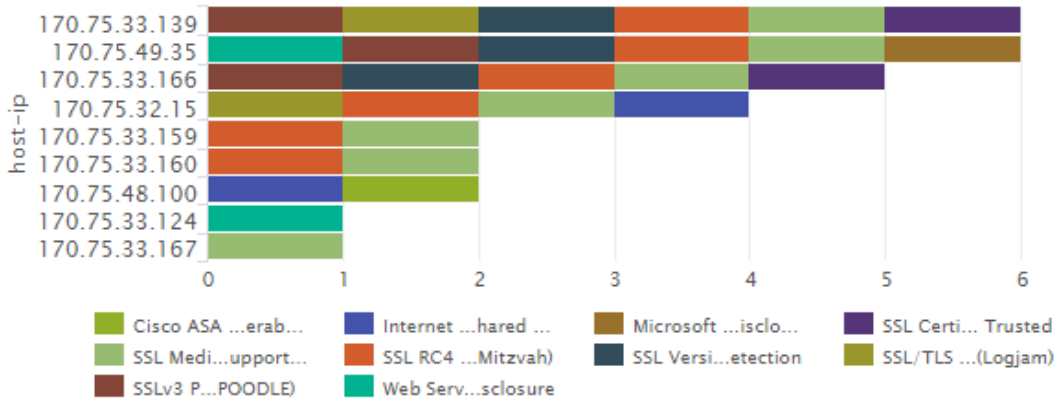
Graph: Vulnerability Category by Port
This report illustrates the vulnerability category and count by port discovered this report period



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

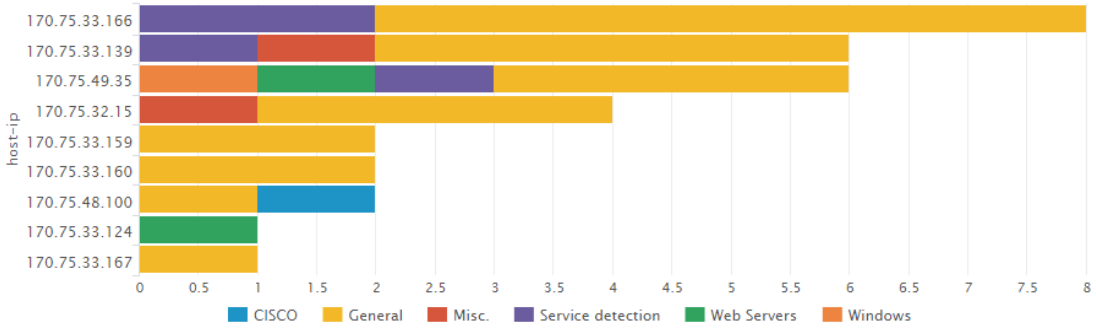


Graph: Host by Vulnerability Name
This report illustrates the vulnerability name and count by hosts discovered this report period

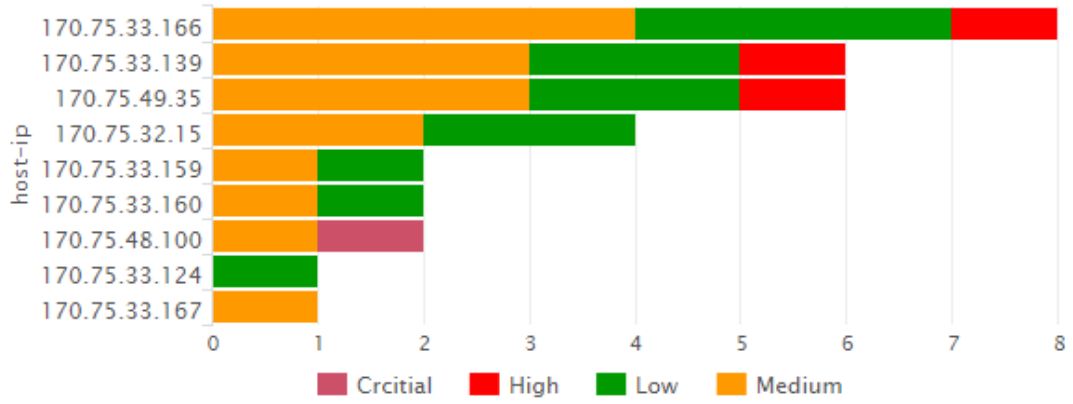


Graph: Host by Vulnerability Category
This report illustrates the vulnerability category and count by hosts discovered this report period

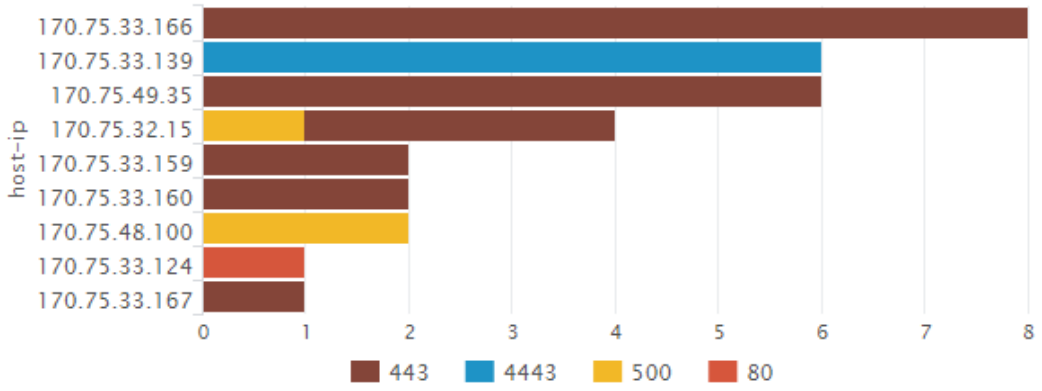
USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355



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



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.

PROFESSIONAL SERVICES ACTIVITY

Below we outline the usage of the consulting retainer of professional services activity for the corresponding month. In this we show the total billable and non-billable hours, the contracted retainer, the total hours used in the month and the hours above the retainer.

Billable consulting hours	Non-billable consulting hours	Contracted retainer hours	Total Hours utilized	Hours above retainer
0	0	2	0	0

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	99.967% (99.967%)	0.000% (0.000%)	0.000% (0.000%)	0.033% (0.033%)	0.000%
Average	99.967% (99.967%)	0.000% (0.000%)	0.000% (0.000%)	0.033% (0.033%)	0.000%

The DefensePro Elmer was considered up and available 99.68% during this report period.

Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	30d 23h 37m 50s	99.950%	99.950%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	30d 23h 37m 50s	99.950%	99.950%
DOWN	Unscheduled	0d 0h 22m 10s	0.050%	0.050%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 22m 10s	0.050%	0.050%
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%

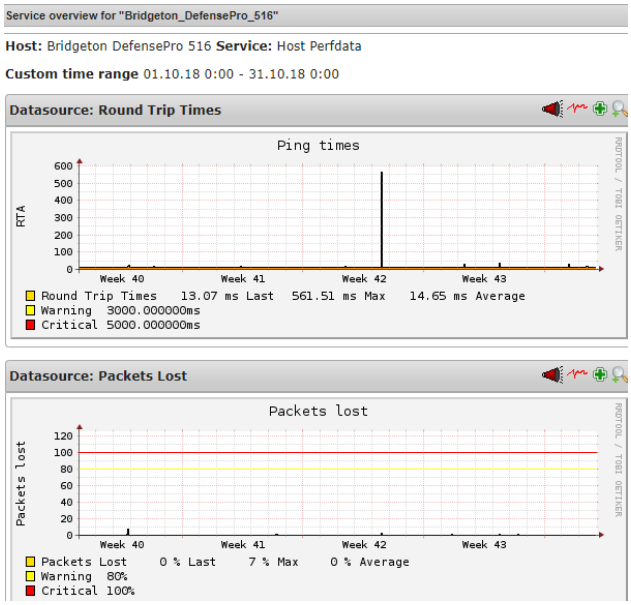
State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
PING	99.886% (99.886%)	0.000% (0.000%)	0.000% (0.000%)	0.114% (0.114%)	0.000%
Average	99.886% (99.886%)	0.000% (0.000%)	0.000% (0.000%)	0.114% (0.114%)	0.000%

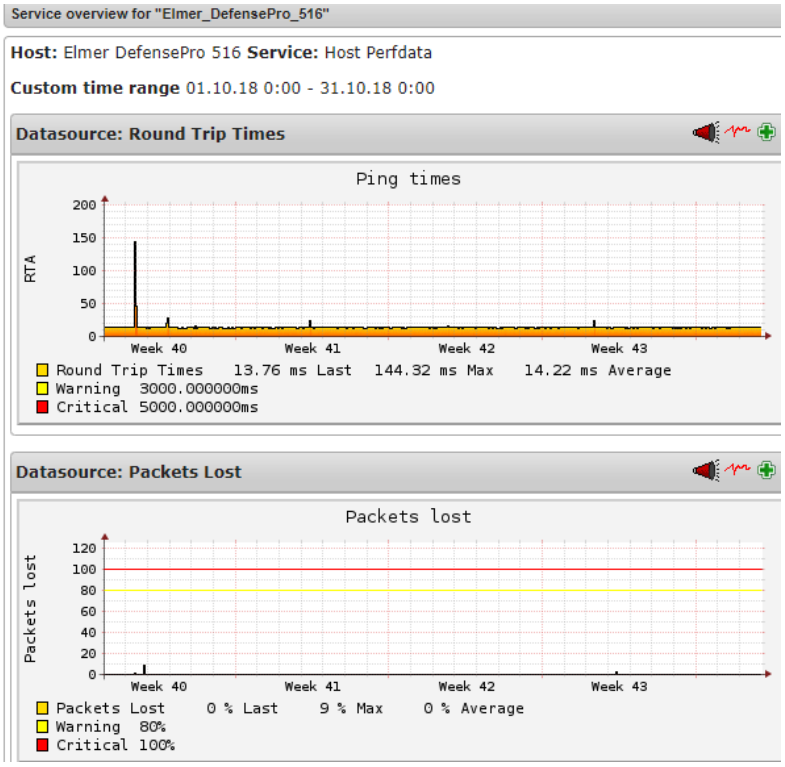
MONITORING PERFORMANCE OF COUNTERMEASURES

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 14.65 ms from the GLESEC GOC to Inspira Health Network with 0 % average packet loss.



Inspira Health Network DefensePro Elmer Host Performance
Round trip ping times averaged 14.22 ms from the GLESEC GOC to Inspira Health Network with 0 % average packet loss.



TICKET ACTIVITY

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

Monthly Reports IHN 2018-10-01 00:00:00-2018-10-3[..]

Number	Ticket#	Title
1	2018102610000041	TLP AMBER INSPIRA INCIDENT REPORT 1227
2	2018100910000047	Monthly Operations & Intelligence Report September 2018
3	2018100810000021	RE: [EXT] ANSWER FOR INCIDENT REPORT 1213
4	2018100710000032	Received data (syslog) Elmer
5	2018100210000292	Elmer connectivity

Since September 19, all the traffic from Elmer was redirected to Bridgeton, the client notified us that this was due to some changes they were doing in their network. On October 7th at 10:24 a.m. we began to receive data from Elmer normally.

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