



OPERATIONS & INTELLIGENCE CYBER SECURITY REPORT

Inspira Health Network
February 2018

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

Info@glesec.com
www.glesec.com

CONFIDENTIAL

Table of Contents

About This Report	3
Scope of this Report	4
Executive Summary	5
Recommendations.....	13
Intelligence Section Per Service Module	14
Cyber Security Operations	35
Definitions	38

CONFIDENTIAL



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.



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		

CONFIDENTIAL



Executive Summary

This report corresponds to the period from February 01 to February 28, 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 / RIESGO
	VULNERABILITIES / VULNERABILIDADES • MSS-VM Service
	THREATS / AMENAZAS • MSS-APS; MSS-EPS; MSS-SIEM; MSS-EIR; MSS-UTM
	ASSETS / ACTIVOS • MSS-VM; MSS-EPS
	COMPLIANCE / CUMPLIMIENTO • MSS-EPS
	SECURITY VALIDATION / VALIDACION • MSS-BAS
	TRUSTED ACCESS / ACCESS CON CONFIABILIDAD • MSS-TAS

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

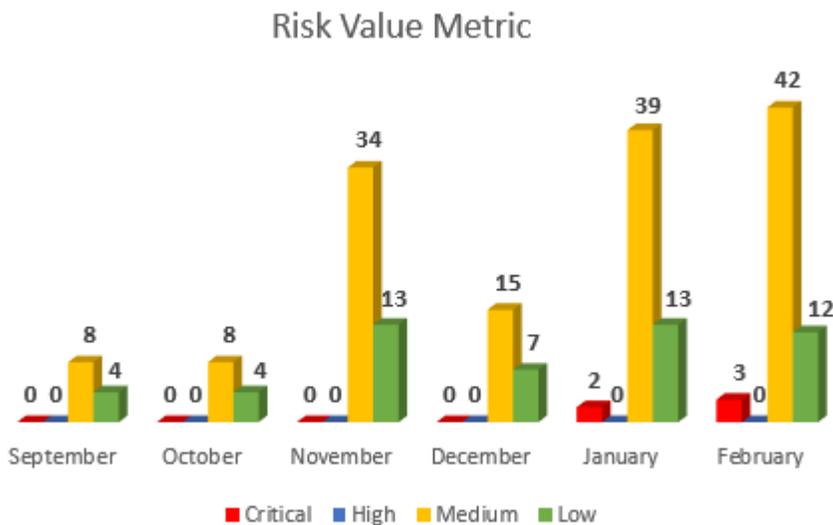
One of GLESEC's foundational columns is basing all its activities to support RISK determination and mitigation. What any organization should want to know is what is their level of RISK, and in this case in particular to cyber-security. Cyber-Security RISK has a direct impact to the business and as such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



Based on the contracted services, risk conditions are higher than last month, there is an increase of 1 critical and 3 medium vulnerabilities. This new critical one was found to be on a page under construction.



CONFIDENTIAL



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 have been 3 critical ,0 high ,42 medium and 12 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. It was also discovered one critical vulnerability on host 170.75.33.108, refer to recommendations section for more information on this. We have noticed an increase in medium vulnerabilities from December until this month; we strongly recommend to take action on these so that we see a lower amount in coming months.

There are many medium risk vulnerabilities which were found on many hosts, please refer to MMS-VM intelligence section for more detail about specific hosts. Medium risk vulnerabilities found were classified as SSL Medium Strength Cipher Suites Supported, SSL Certificate Cannot Be Trusted, SSL Certificate Expiry, SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability (POODLE), SSL RC4 Cipher Suites Supported (Bar Mitzvah), and SSL Certificate Signed Using Weak Hashing Algorithm. This means that attackers could take advantage of any of those and attempt to cause and negative impact to your Organization.

We recommend to take special attention to 170.75.32.15(CISCO ASA),



170.75.33.137 (shows internal FQDN through https), 170.75.33.140 (VM Horizon exposed) and any other specified at the recommendation section.

There was a reported incident on the 29th of December 2017, incident 1145, which has not been thoroughly solved. We recommend special attention on this one as well.

The most vulnerable ports for this period were 443 and 4443. This is because many vulnerabilities were found which are related to them and categorized as medium or critical risk.

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 Health Network were scanned for vulnerabilities.

The following table indicates the external vulnerability metric.



REPORT FOR:

Inspira Health Network

Total IP's Scanned		IP's Vulnerable		
49		18		
Risk Distribution				
Critical	High	Medium	Low	Total
3	0	42	12	57

According to the metrics:
 RV= 0.162406015

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
170.75.33.166	0		5	3	8
170.75.33.137	0		4	2	6
170.75.33.138	0		4	2	6
170.75.33.113	1		3	1	5
170.75.32.15	0		2	2	4
170.75.33.133	0		4	0	4
170.75.33.110	0		2	1	3
170.75.33.115	0		3	0	3
170.75.33.125	0		3	0	3
170.75.33.140	0		3	0	3

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
170.75.33.114	1	1
170.75.33.134	0	0
170.75.33.136	0	0
170.75.33.137	0	0
170.75.33.138	0	0
170.75.33.140	0	0
170.75.33.152	0	0
170.75.33.166	0	0
170.75.33.167	1	1
170.75.33.4	0	0
170.75.33.91	1	1
170.75.33.55	0	0
170.75.33.58	0	0

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

CONFIDENTIAL



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	

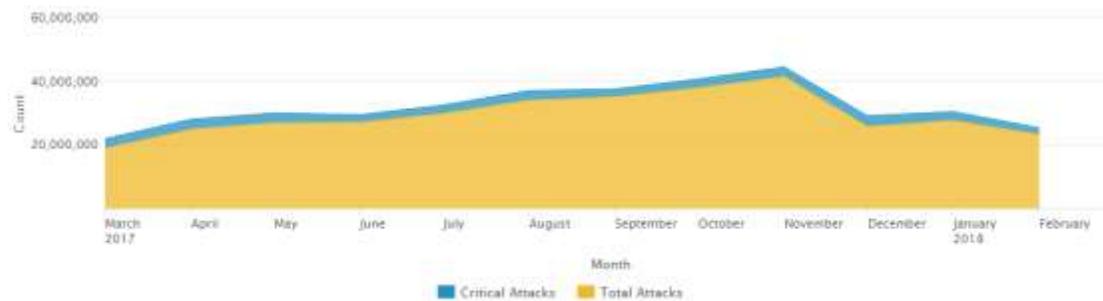
Based on the above the following table shows a matrix of the total external vulnerabilities by category.

plugin_family	critical	low	medium
General	0	5	38
Web Servers	1	3	1
Service detection	0	1	3
Misc	0	1	0
Windows	2	0	0

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).



CONFIDENTIAL



This month we are seeing a decrease in attack activity from prior month of about 9.8% and a decrease in critical attacks from prior month of about 38.8%.

Most of the attacks have a duration of more than one hour, are of type: Anti-scanning, anomalies, Invalid IP header or total length 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, this attacks were dropped.

We also found a considerable amount of attacks to an unregistered port (8545) and port 1433 (MS-SQL-SERVER) most of this attacks are part of horizontal TCP scans, port 8545 is filtered. If no particular internal rule specifies that this ports should be reachable from the outside, they should not, as part of the least privilege principle

Most of the attacks seem to be of reconnaissance (scanning). About 78% 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. 43% of total attacks this month followed by USA and Chile, as the three top sources.

Based on the information gathered from the security countermeasures during this period 23,229,010 attacks on Inspira; 2,038,859 of which were considered critical were all stopped by the GLESEC managed security countermeasures.

Inspira receives an average of 25,427,168 total attacks and 2,406,731 critical attacks on a monthly basis. This equates to an average of 861,938 total daily attacks and 81,584 critical daily attacks.

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 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. The MSS-VM (E/I), MSS-EPS conduct weekly testing.

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

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 user 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

Note: we recommend an upgrade on the Inspira Health Network Bridgeton and Elmer DefensePro.

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.
5. Old versions of software are vulnerable to many known exploits, malicious code can be hidden within files that should be allowed because they are of regular usage, and bypass many security measures. It is important to keep the software updated with the latest patches to prevent attackers from using these exploits, this process can be done manually or automated using an endpoint manager to check and enforce compliance policies. Contact your GLESEC representative for assistance with this.

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



Intelligence Section Per Service Module

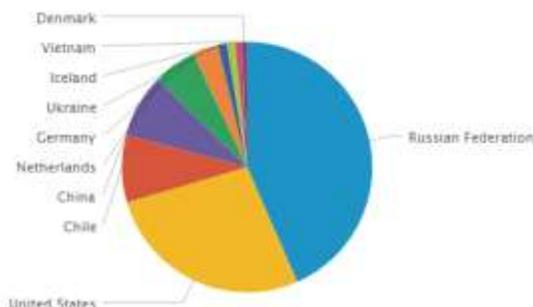
MANAGED ATTACK PROTECTION SERVICE (MSS-APS) SECURITY INTELLIGENCE SECTION

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.

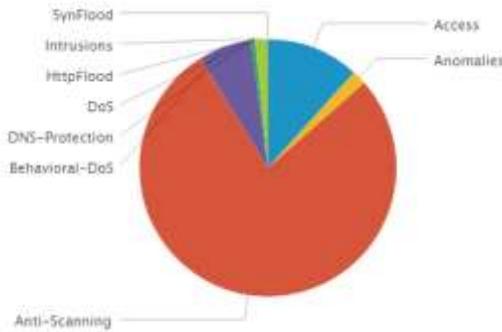
The purpose of this section is to highlight intelligence gathered from the services under contract as well as outside sources such honeypots, known malicious sources, vulnerability databases, relationships with CERT and CSIRT teams that GLESEC possesses, together with various other threat feeds.

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.

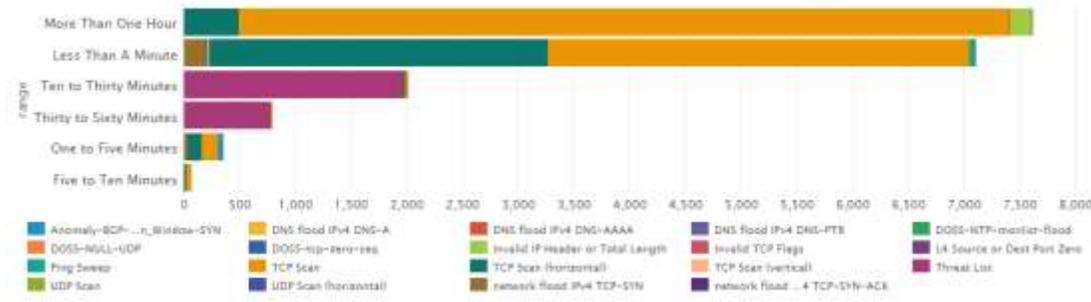


The distribution of attacks per type can be seen in the following diagram.



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	133.67	136874.51
Behavioral-DoS	76.12	77944.25
Anti-Scanning	60.12	61562.36
Intrusions	20.15	20629.71
DNS-Protection	10.32	10555.19
Anomalies	7.24	7412.85
DoS	0.08	80.43
SynFlood	0.08	77.54
HttpFlood	0.00	0.00
Total Bandwidth in Gbps/Mbps	307.78	315152.06

*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

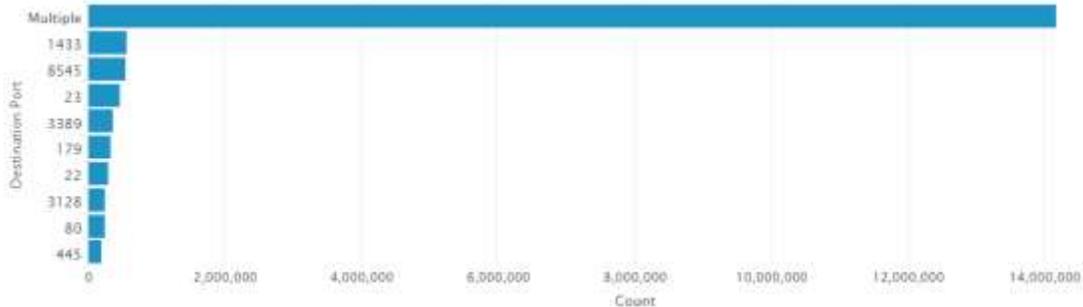
The advanced intrusion detection and prevention capabilities offered by the DefensePro IPS NBA, DoS and Reputation Service provides maximum protection for

CONFIDENTIAL



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.

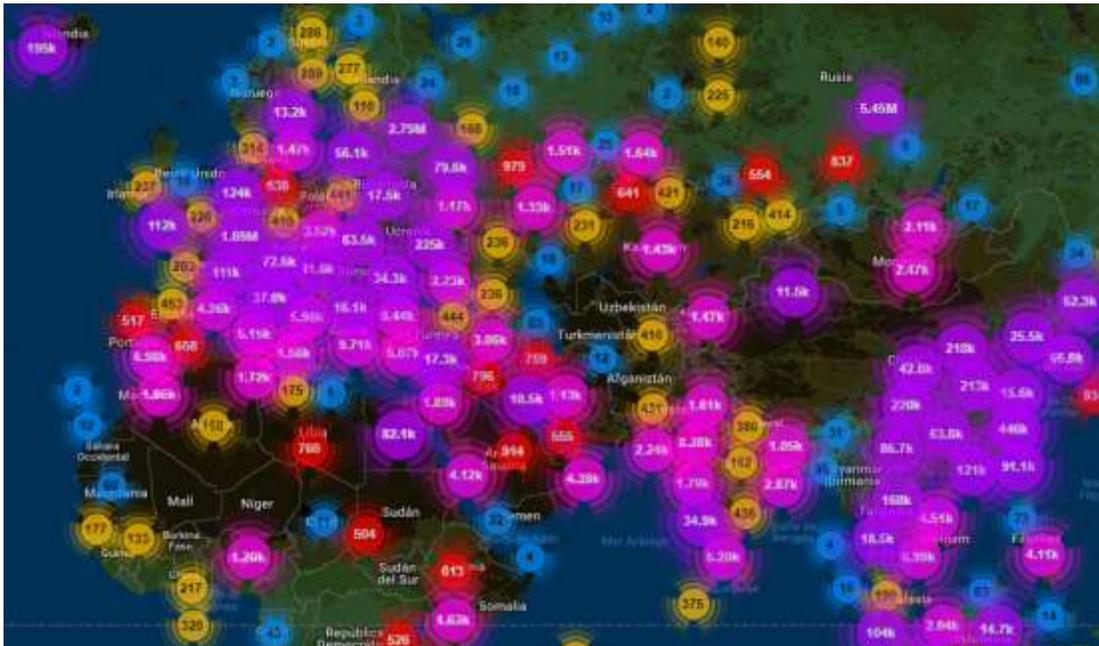


Port number information utilized is based on IANA Service Name and Transport Protocol Port Number Registry and additional outside sources are used to illustrate the relationship to commonly exploited attacks vectors.

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.

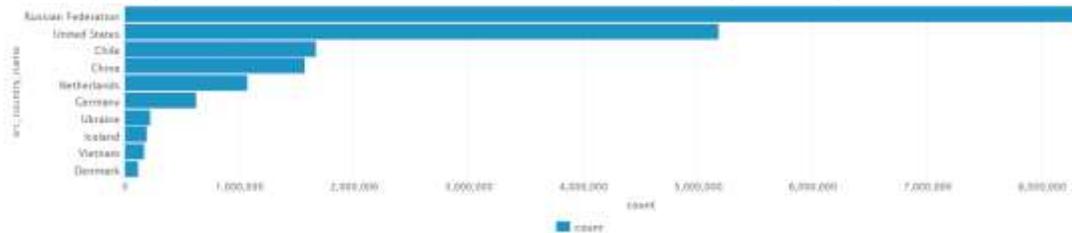
CONFIDENTIAL





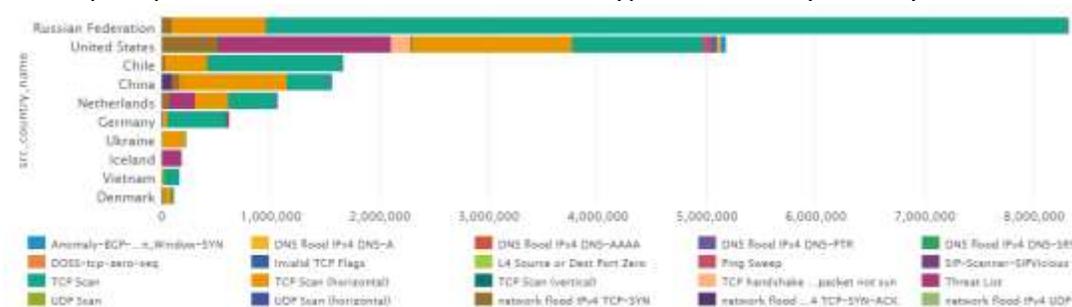
Graph: Top 10 Attacking Countries Blocked

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

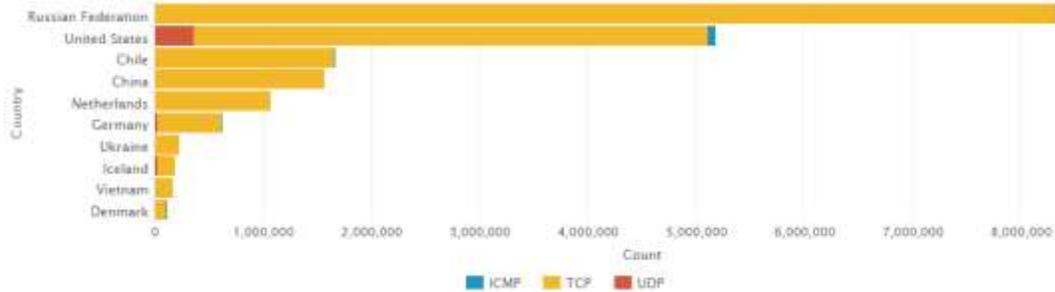


Graph: Top 10 Attacking Countries Blocked by Protocol

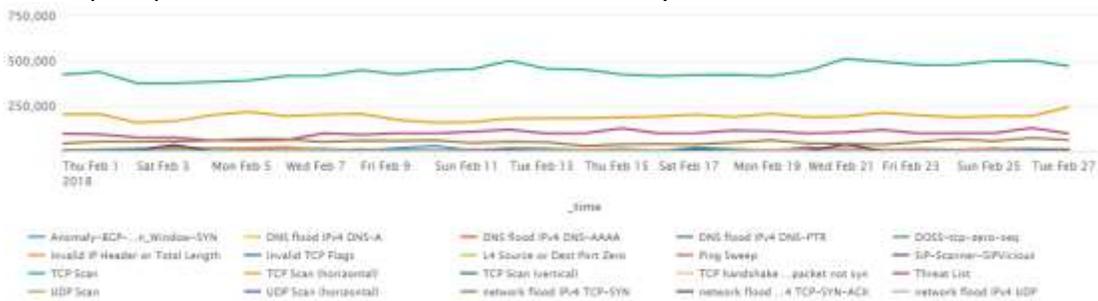
This report provides the count of attack protocols blocked by country

CONFIDENTIAL

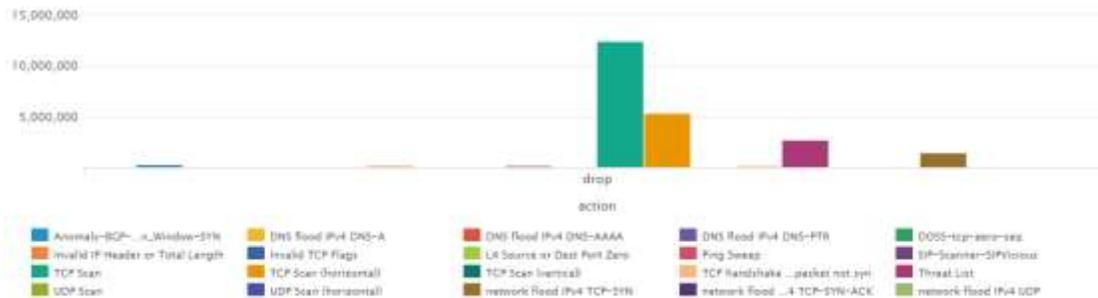




Graph: Attacks Types Blocked by Week
 This report provides the count of attacks blocked by week



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

CONFIDENTIAL



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.

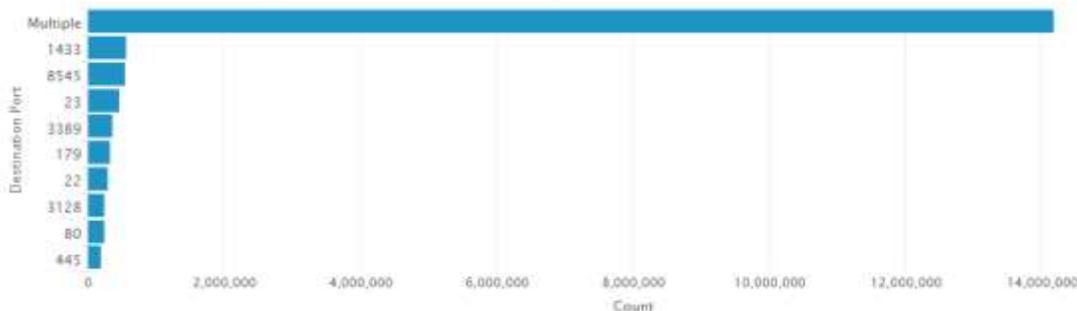
OWASP Top 10 lists A1-Injection as the greatest threat and defines this category as:

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.

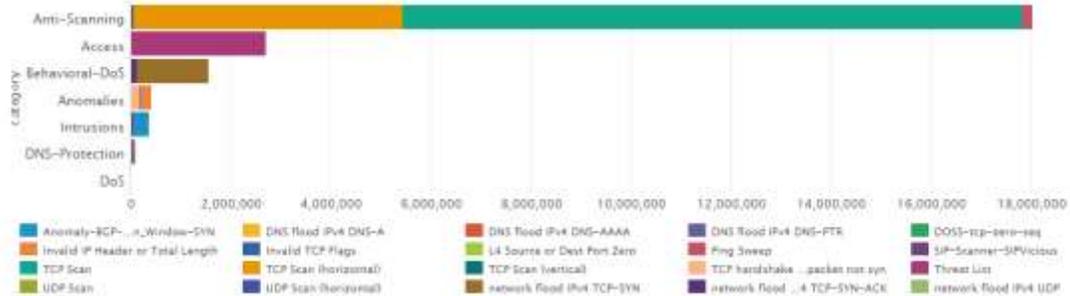
Graph: Attacks Blocked by Destination Port

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.



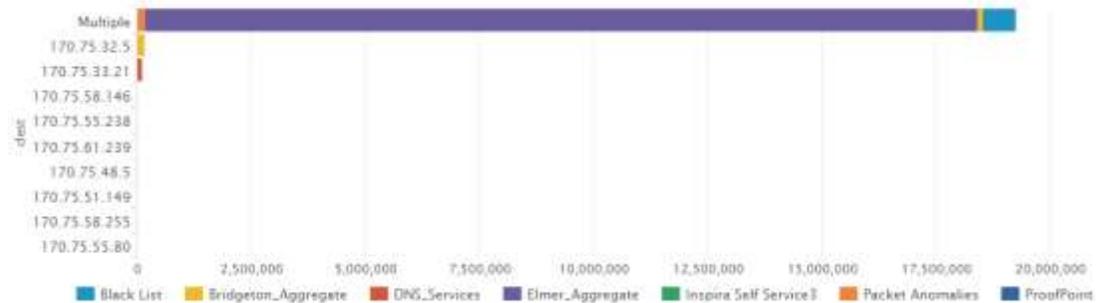
Graph: Critical Attacks Blocked

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

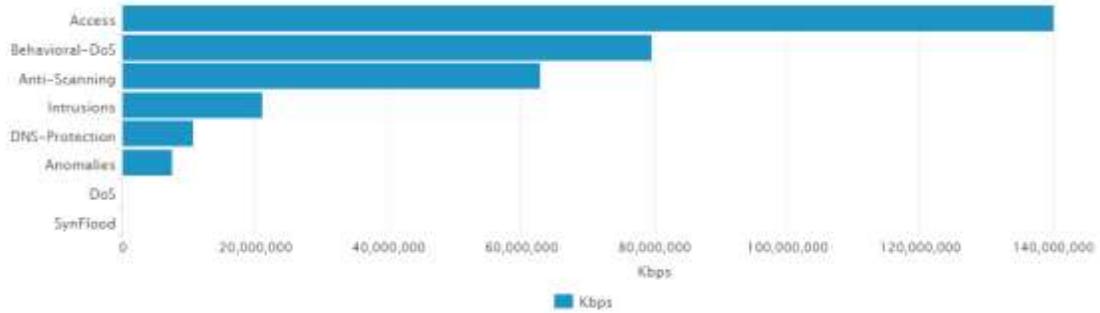
This report shows the attack categories based on the BW of the attacks sharing the same category including Kbps.

CONFIDENTIAL



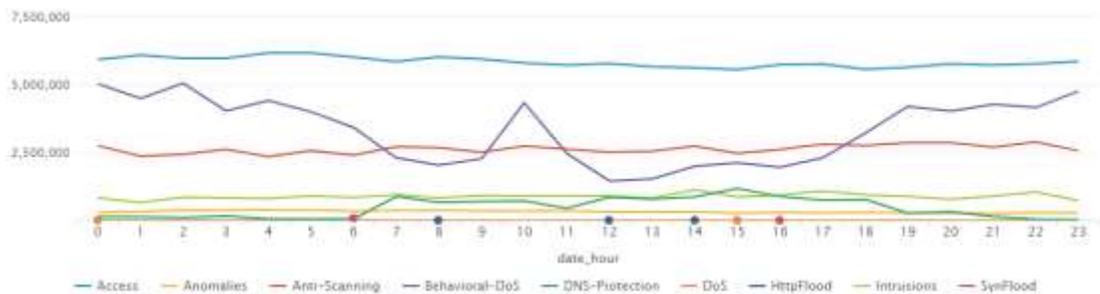
REPORT FOR:

Inspira Health Network



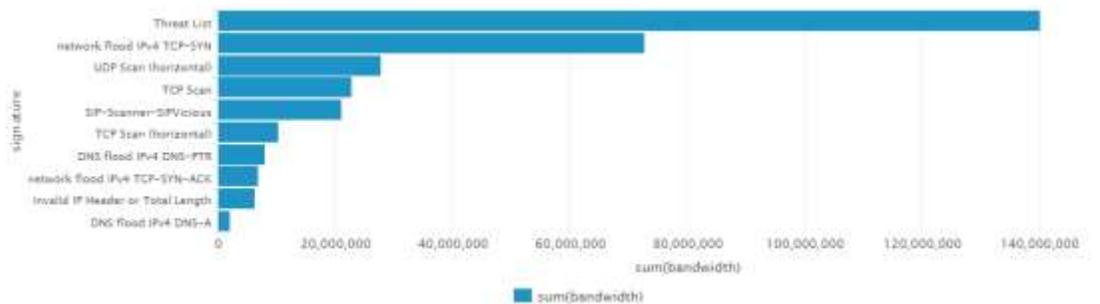
Graph: Bandwidth by Blocked Threat Category by Hour of Day

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



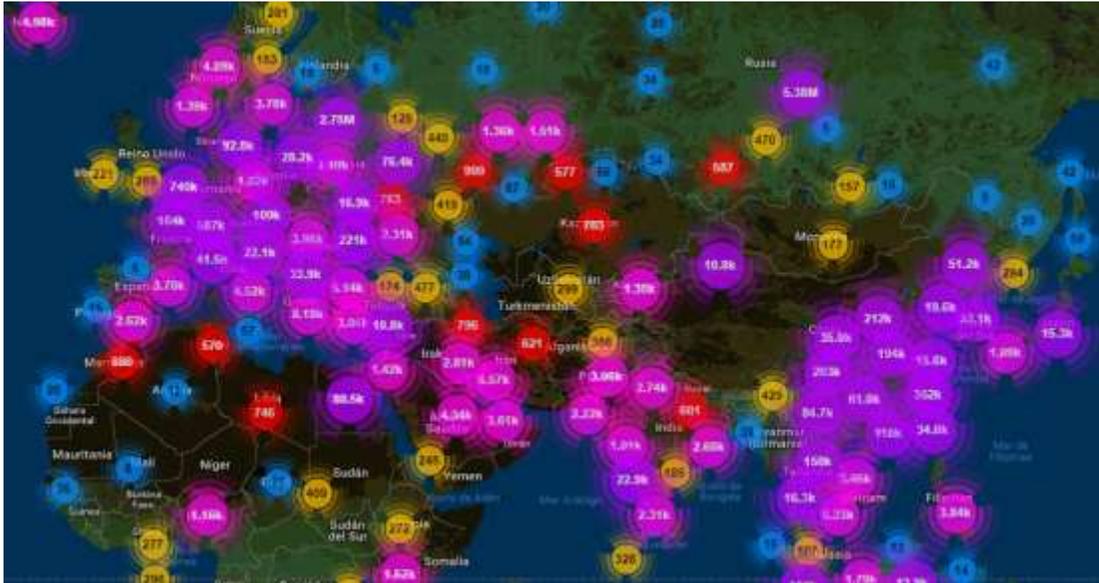
attack including Kbits.

Scanning Information

The following map displays geographic distribution of 18,045,887 attacks on Inspira from scanning sources. Some results do not include location information that allows map plotting.

CONFIDENTIAL

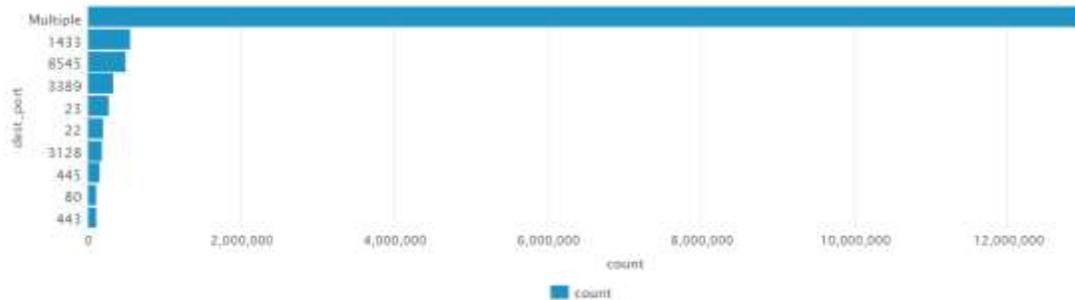




Network-wide Anti Scanning protections dropped enumeration attempts which otherwise thwart any effort for threat modeling, commonplace after the information gathering phase of a targeted or planned attack.

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.

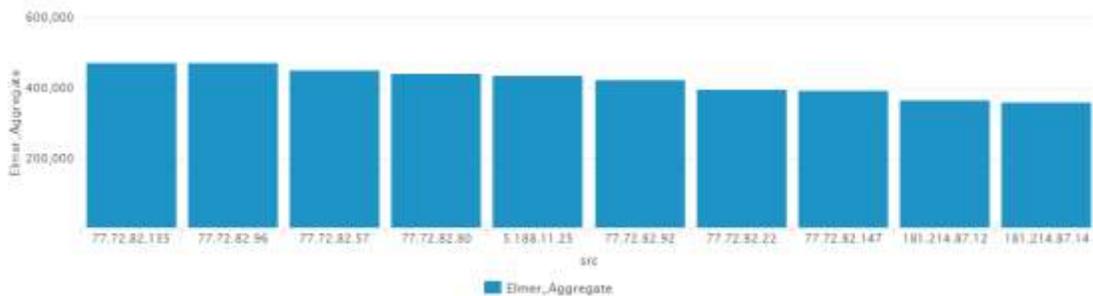
CONFIDENTIAL





Graph: Top Scanners Blocked (Source IP Addressed)

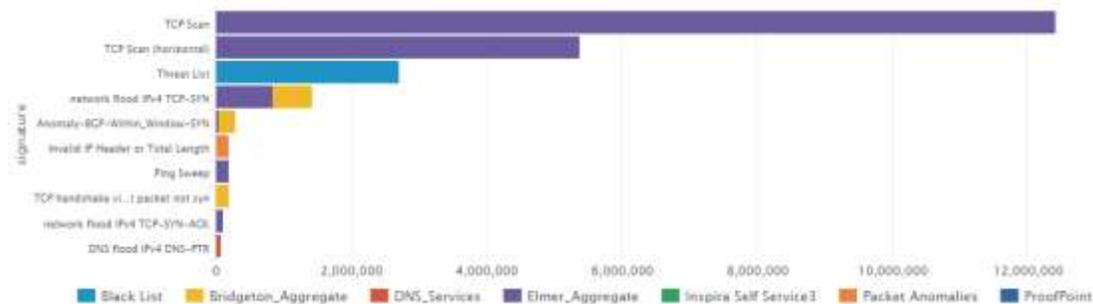
This report shows historical view of the Top source IP addresses that have scanned the network-by-network scanning activities along with the network security rule.



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

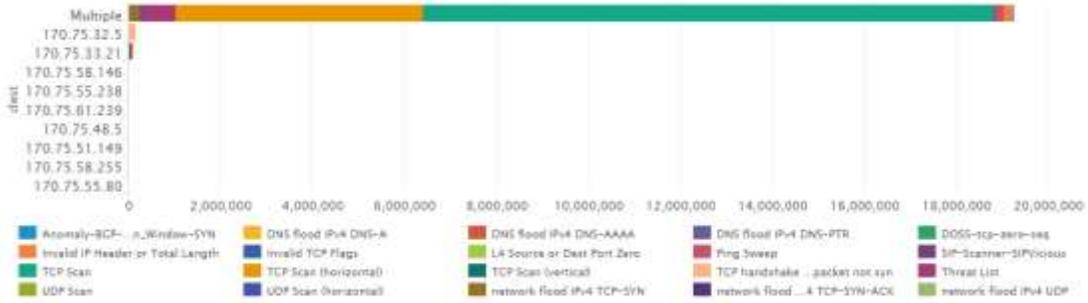
This report provides information on the top attacks targeted at destinations that were blocked on the DP IPS. In this report the destination on which the attack was targeted, attack name, and count are shown.

CONFIDENTIAL



REPORT FOR:

Inspira Health Network



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

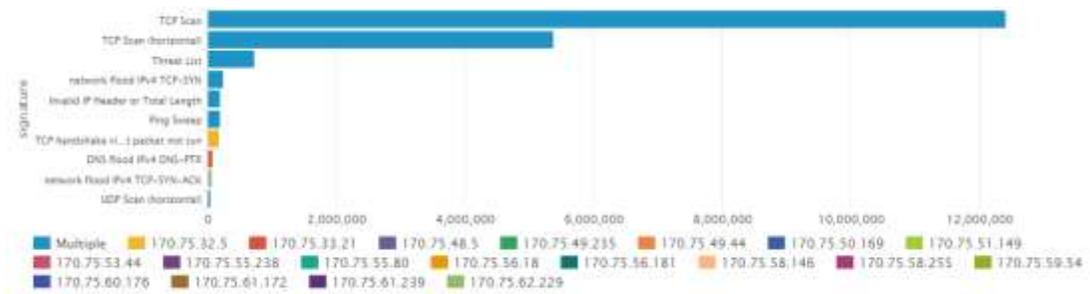
This report provides information on the attacks attempted for the most number of times on the destination's protected system IPs.

CONFIDENTIAL



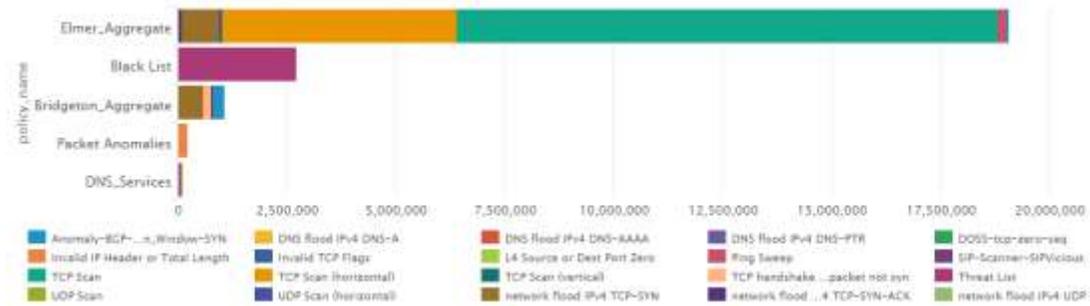
REPORT FOR:

Inspira Health Network



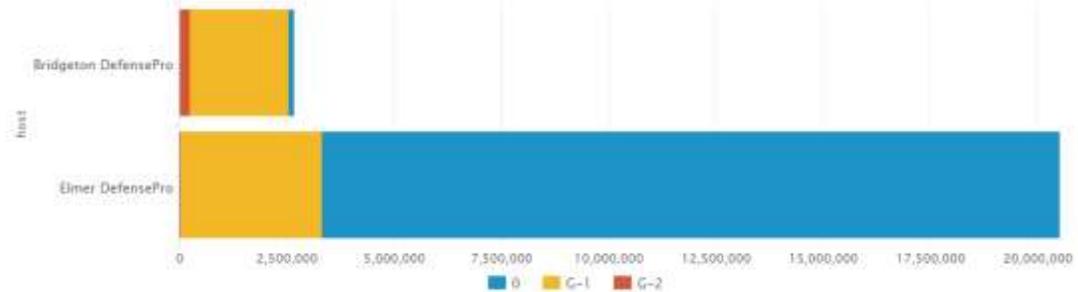
Graph: Attacks Blocked by Network Security Rule

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.

CONFIDENTIAL



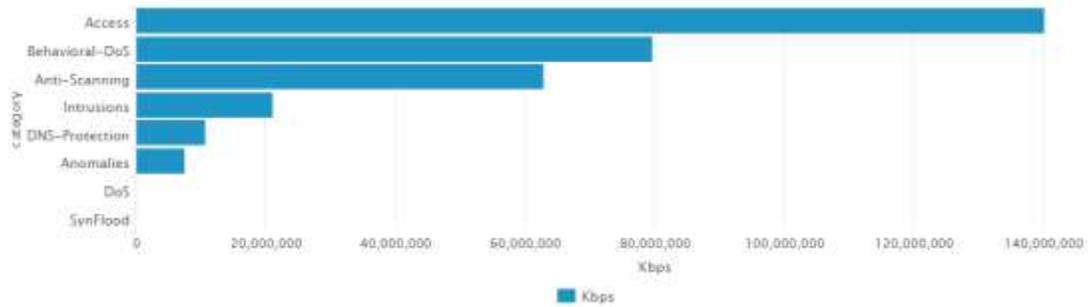
REPORT FOR:

Inspira Health Network

Category :	Gbps :	Mbps :
Access	133.67	136874.91
Behavioral-DoS	76.12	77944.29
Anti-Scanning	60.12	61562.36
Intrusions	20.10	20629.71
DNS-Protection	10.22	10565.19
Anomalies	7.14	7412.85
DoS	0.08	86.43
SynFlood	0.08	77.54
HitzFlood	0.00	0.00
Total Bandwidth in Gbps/Mbps	307.70	315152.88

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.



CONFIDENTIAL



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/>.

Vulnerability Score

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

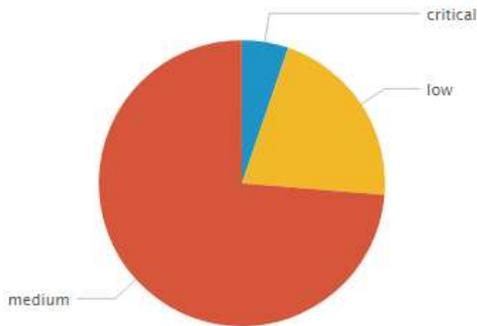
Medium risk if they have a CVSS base score of 4.0 – 6.9

High risk if they have a CVSS base score of 7.0 – 10.0

Vulnerability Information

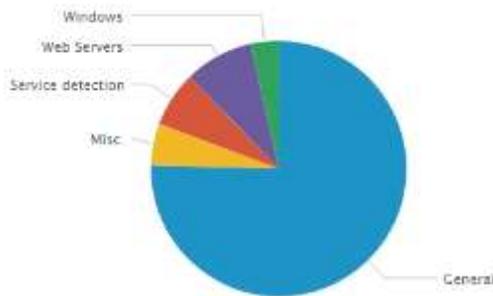
Graph: Risk Distribution

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



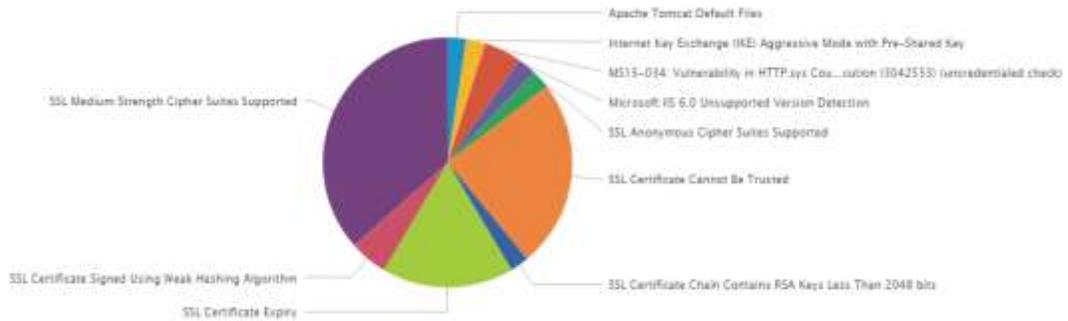
Graph: Most Frequent Vulnerability Name

This report depicts the most frequent vulnerabilities discovered this report period



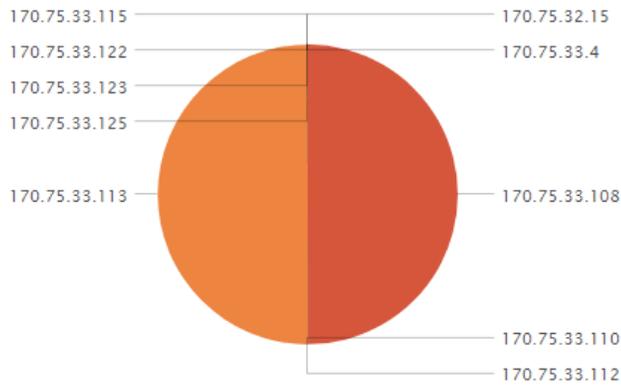
REPORT FOR:

Inspira Health Network



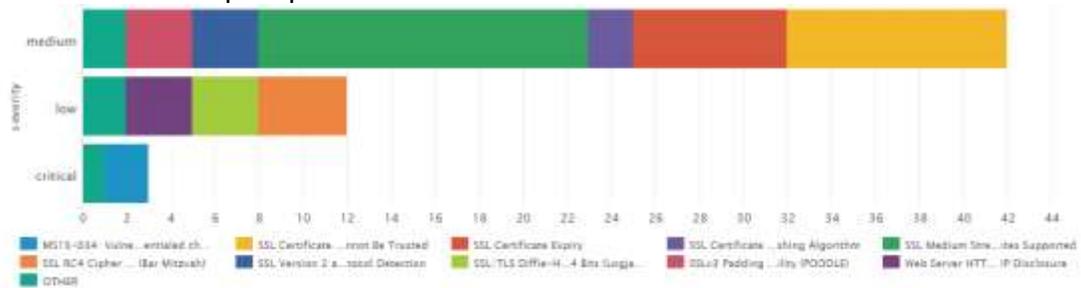
Graph: Most Vulnerable Host

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

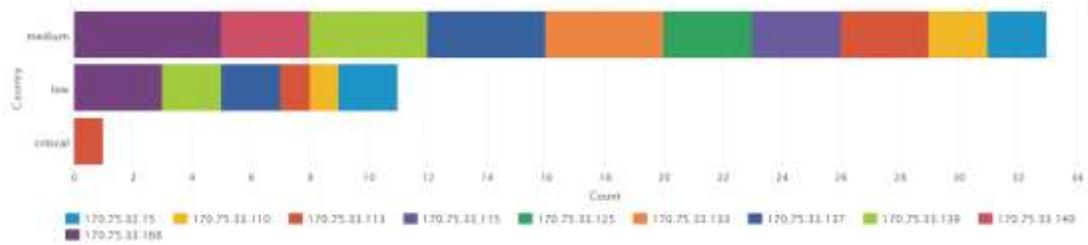


Graph: Vulnerability Risk by Host

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

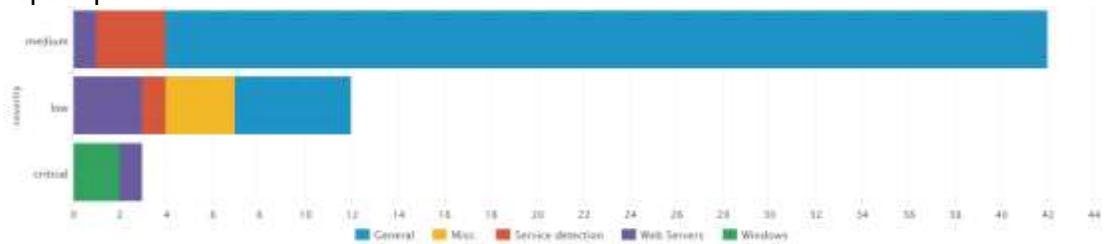
CONFIDENTIAL





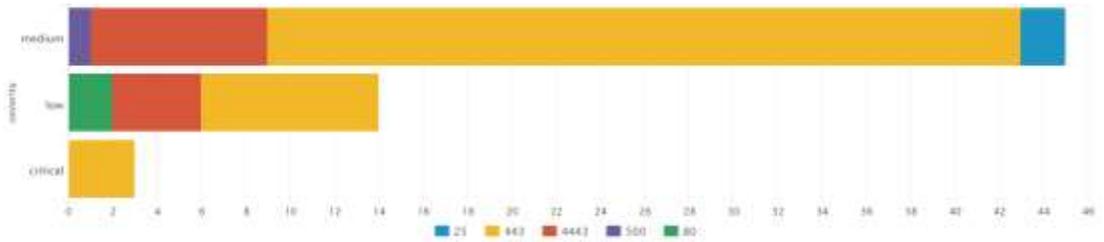
Graph: Vulnerability Risk by Category

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

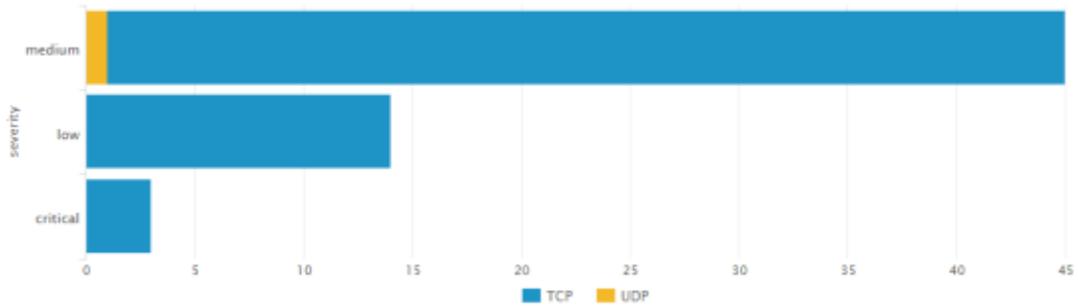


Graph: Vulnerability Risk by Protocol

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

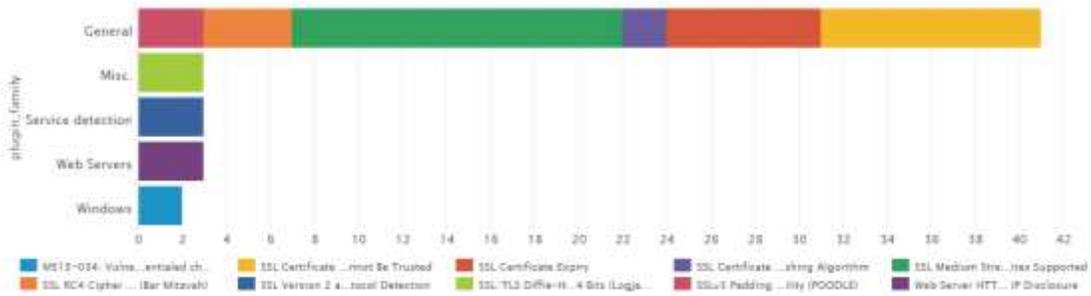
CONFIDENTIAL





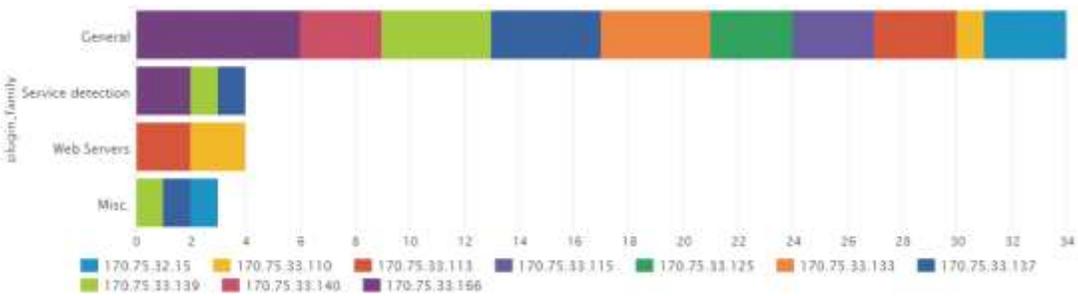
Graph: Vulnerability Category by Vulnerability Name

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

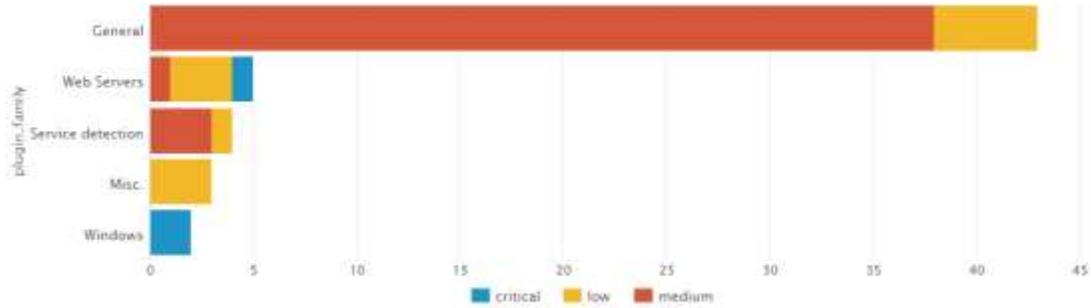


Graph: Vulnerability Category by Risk

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

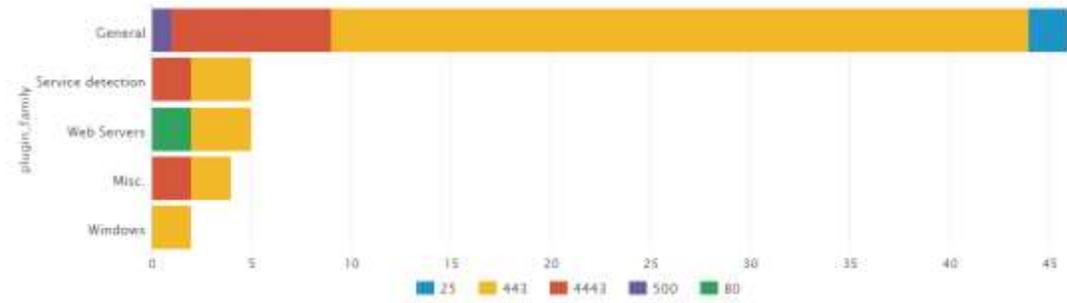
CONFIDENTIAL





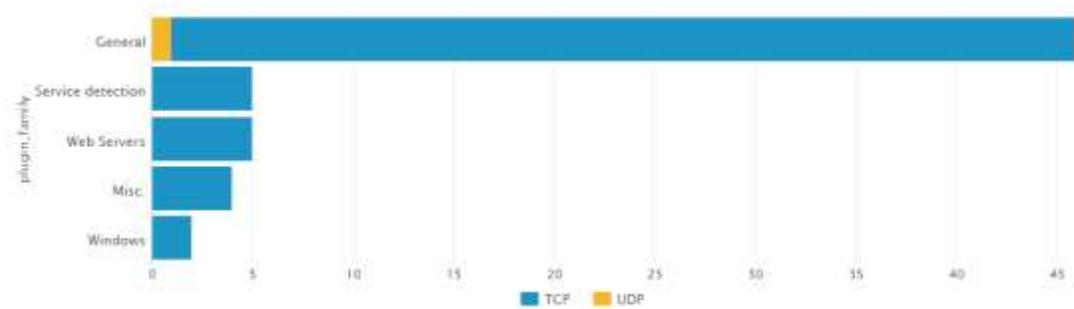
Graph: Vulnerability Category by Port

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

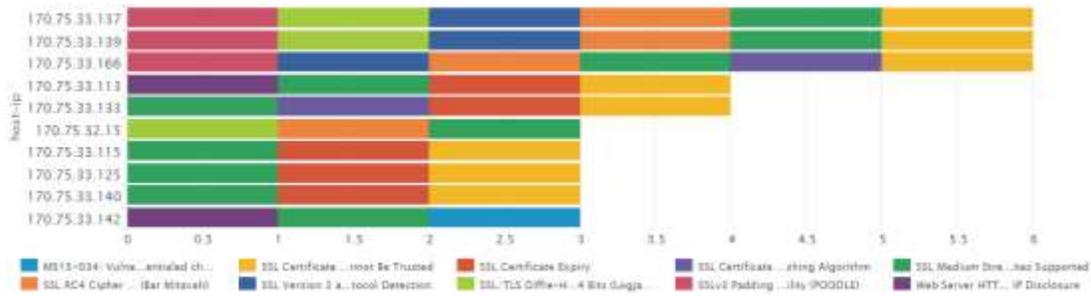
This report illustrates the vulnerability name and count by hosts discovered this report period

CONFIDENTIAL



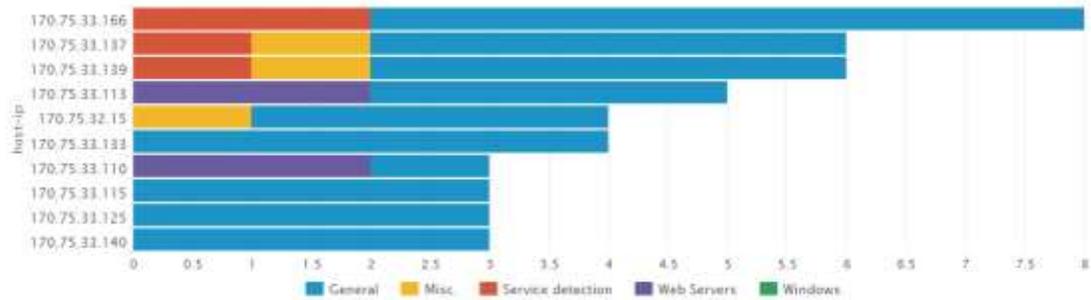
REPORT FOR:

Inspira Health Network



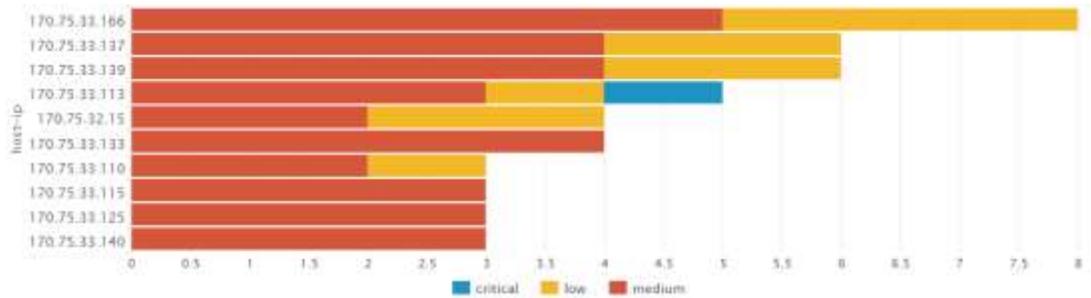
Graph: Host by Vulnerability Category

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

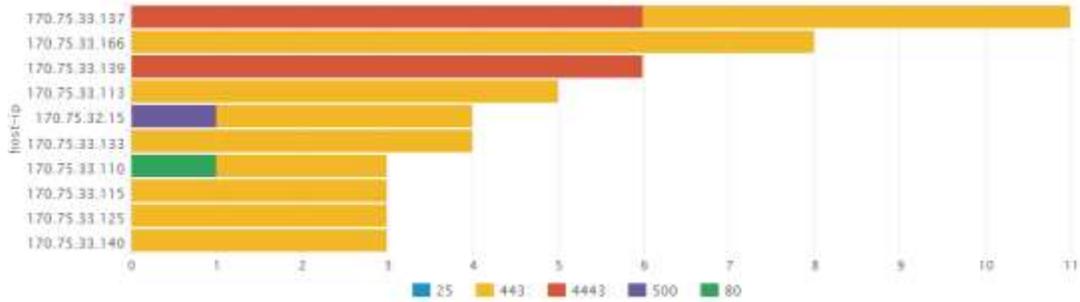
This report illustrates the port and count by hosts discovered this report period

CONFIDENTIAL



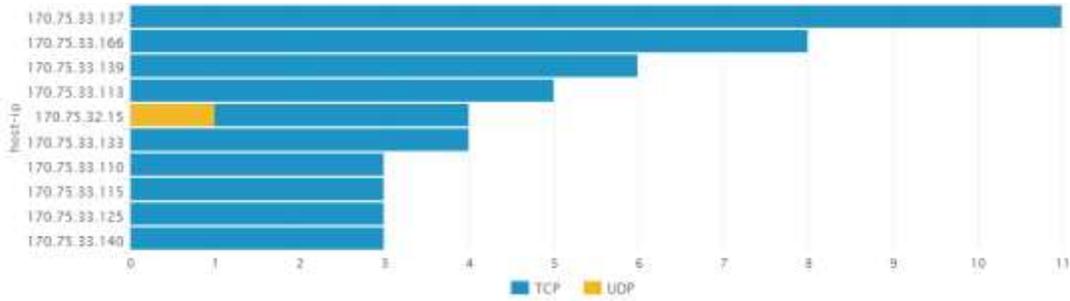
REPORT FOR:

Inspira Health Network



Graph: Host by Protocol

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



CONFIDENTIAL



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	28d 0h 0m 0s	100.000%	100.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	28d 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	28d 0h 0m 0s	100.000%	100.000%

State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
PHG	99.988% (99.988%)	0.000% (0.000%)	0.000% (0.000%)	0.012% (0.012%)	0.000%
Average	99.988% (99.988%)	0.000% (0.000%)	0.000% (0.000%)	0.012% (0.012%)	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	28d 0h 0m 0s	100.000%	100.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	28d 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	28d 0h 0m 0s	100.000%	100.000%

State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
PHG	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.

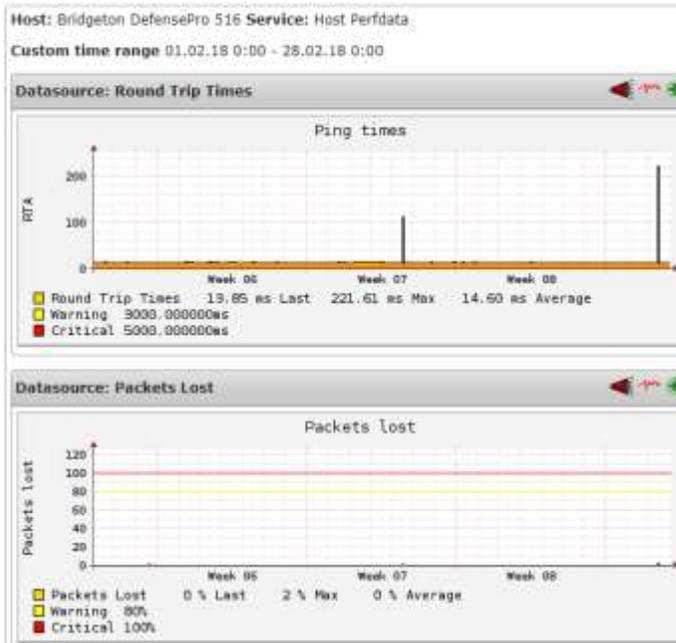
CONFIDENTIAL



REPORT FOR:

Inspira Health Network

Round trip ping times averaged 14.60 ms from the GLESEC GOC to Inspira Health Network with 0 % average packet loss.



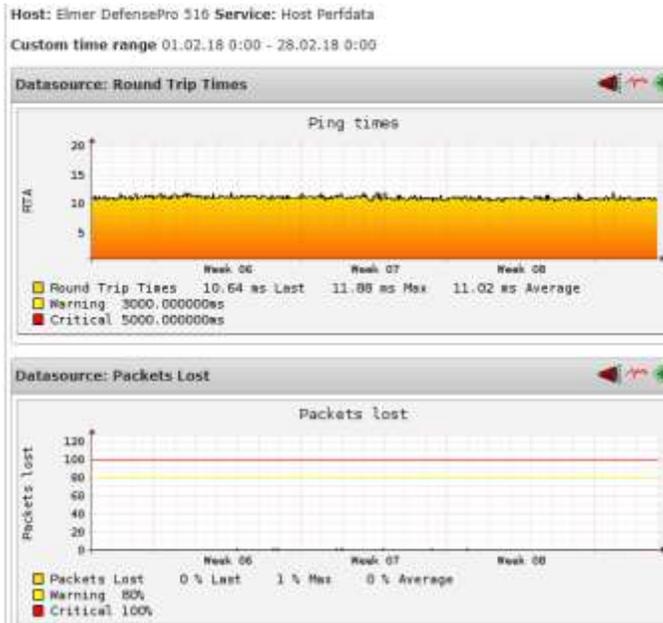
Inspira Health Network DefensePro Elmer Host Performance
Round trip ping times averaged 11.02 ms from the GLESEC GOC to Inspira Health Network with 0 % average packet loss.

CONFIDENTIAL



REPORT FOR:

Inspira Health Network



TICKET ACTIVITY

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

Monthly Reports IHN 2018-02-01 00:00:00-2018-02-2[..]

Number	Ticket#	Title
1	2018021610000218	RE: [EXT] Re: FW: I think we're being attacked...
2	2018020710000011	Incident Notification-1154(IHN)

CONFIDENTIAL



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