OPERATIONS & INTELLIGENCE EXECUTIVE CYBER SECURITY REPORT

Copa Airlines

September, 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		
Threat Mitigation	MSS-APS-SSL		
Threat Mitigation	MSS-APS-PS		
Threat Mitigation	MSS-APFW		
Vulnerability Testing	MSS-VME	YES	10/30/2018
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	YES	10/30/2018

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 September 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.

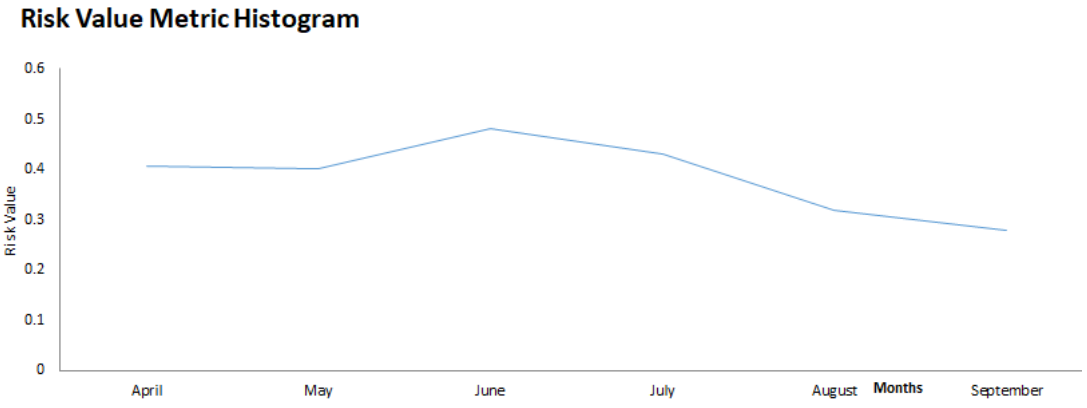
We at GLESEC measure RISK through a number of perspectives and using several of the TIP™ platform portfolio of services. The MSS-VM or Managed Vulnerability

Service provides us with one view, how weak are the systems of the organization. The MSS-BAS provides us a view of how weak is 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 Copa Airlines for the month of September is High. This can be seen in the security indicator as indicated below.

Risk Indicator	Service	Condition	Comments
Risk Value Metric	MSS-VME	HIGH	1 high vulnerability has been identified this month. Only one is enough to add up risk of negative impact to Copa Airlines

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



During this period, we can see that the risk value has decreased to 0.2893 since 1 medium and 1 high vulnerability were not present during the testing. It also happened that there was one vulnerable host less than the ones registered last month.

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 slightly decreased to 21 compared to the previous month (23), which are distributed as follows: 1 High, 17 Medium and 3 Low. No vulnerabilities of critical severity were discovered during the testing of this period.

The host that keeps showing a HIGH severity vulnerability for your organization is 201.218.212.9, which corresponds to a CISCO ASSA and accepts encrypted connections through SSL Version 2 and 3. Additional details of the severity of your systems are included in our monthly technical report.

The hosts most vulnerable for this period are:
201.218.212.9 with 11, 200.46.240.137 with 4, 201.218.212.35 with 2 and 34.199.239.56 with 1 vulnerability.

The most frequents vulnerability categories are:
General

- Vulnerability of disclosure of information on the implementation of the initialization vector of the SSL / TLS protocol (BEAST) with a total count of 5 systems affected.
- SSL Medium Strength Cipher Suites Supported with a total count of 3 systems affected.

Web servers

• F5 BIG-IP Cookie Remote Information Disclosure with a total count of 1 system affected.

The port considered most vulnerable for this period was 443 (HTTPS) followed by 500 (IPsec), 123 (NTP), this is due to the fact that many vulnerabilities were found related to the services that were heard and classified as medium 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 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 for Copa Airlines were scanned for vulnerabilities.

The following table indicates the external vulnerability metric.

Total IP's Scanned	IP's Vulnerable
11	7

Risk Distribution				
Critical	High	Medium	Low	Total
0	1	17	3	21

According to the metrics:

RV= 0.289393939

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-ip	Critical	High	Medium	Low
201.218.212.9		1	8	2
200.46.240.137		0	4	0
201.218.212.35		0	2	0
34.199.239.56		0	0	1
52.3.92.27		0	1	0
52.72.43.239		0	1	0
200.46.241.161		0	1	0

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

host-ip	Previous Month	Current Month
200.46.240.137	4	4
200.46.241.161	1	1
201.218.212.35	2	2
201.218.212.9	11	11
34.199.239.56	1	1
52.3.92.27	1	1
52.72.43.239	1	1
52.86.152.128	2	

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

Vulnerability Categories

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

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

Based on the above the following table shows a matrix of the total External

vulnerabilities by category.

Category	Critical	High	Medium	Low	Total
General		0	14	2	16
Web Servers		0	2	1	3
Misc.		0	1	0	1
Service detection		1	0	0	1

THREATS

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

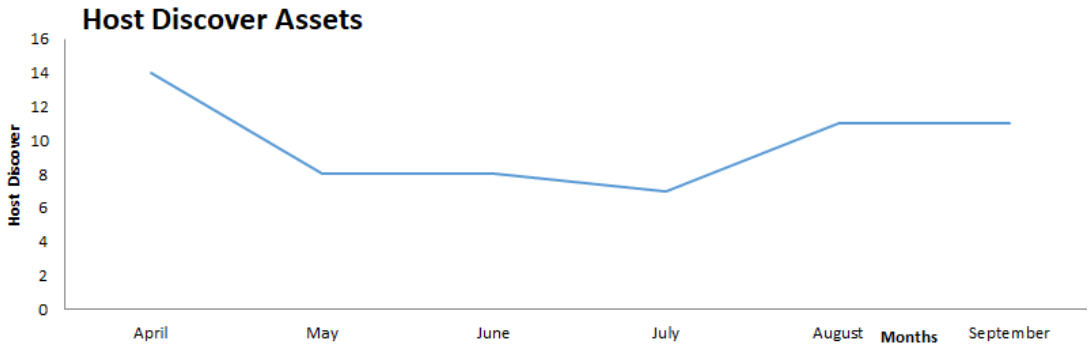
The services that provide us with information for this section have not been contracted.

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 Host Discovery histogram below represents the changes in the Host Discovery inspections over the past six months



For the COPA AIRLINES client, the total number of hosts scanned remained the same as the month of August 11 hosts; of which 7 were found to be vulnerable.

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.

During previous month, Member-Client Copa Airlines had a successful access rate of 91.7%, we were able to register 322 denied authentications, 269 accidentally denied authentications that were denied because of user error, 27 purposely denied authentication, the user took action to deny these authentications either in the Duo prompt or the Duo Mobile, 20 blocked authentications that were denied because of policy or system rules. It is also worth mentioning that from the total of 436 users there were 245 inactive accounts.

Recommendations

GLESEC recommends for Copa Airlines to address the following

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

2. Invalid certificates should be corrected so that they are trusted, even more so when the service is exposed to the internet.

3. SSL Certificate Chain contains RSA keys less than 2048 bits should be corrected.

4. SSL medium Strength cipher suites should not be allowed for SSL connections. This is corrected by Enabling TLS 1.2 or higher and disabling all previous vulnerable versions.

5. We recommend applying the most recent patches for your endpoints, since we have identified that 75% of the devices used for the TAS service have outdated software installed.

6. It is recommended to attend to host with IP 201.218.212.9, which is presenting an Internet Key Exchange (IKE) vulnerability Aggressive Mode with Pre-Shared Key. The following is recommended:

    - Disable aggressive mode if it is compatible.
    - Do not use the pre-shared key for authentication if possible.
    - If the use of the pre-shared key cannot be avoided, use very strong keys.

In our Technical Report monthly you will find more information about the affected hosts of the mentioned vulnerabilities.

Alert: All mentioned vulnerabilities have exploits available and are on the internet can be downloaded and used against you.

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

Intelligence Section Per Service Module

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

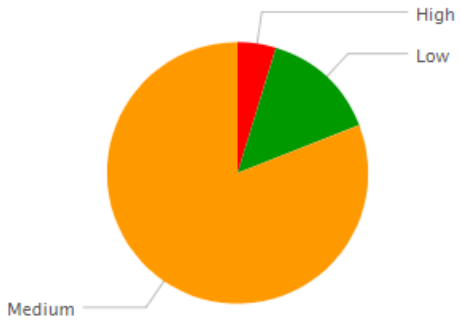
The score of vulnerability is determined by its risk factor; Critical, High, Medium or Low, as well as its value in the Common Vulnerability Scoring System (CVSS). The CVSS "base score" represents the innate risk characteristic of each vulnerability. CVSS is a vulnerability scoring system designed to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

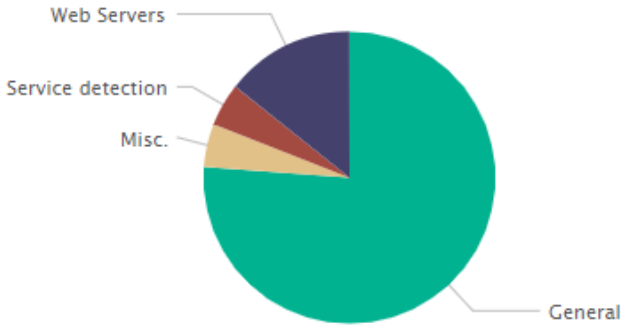
Low risk if they have a CVSS base score of 0.0 – 3.9
Medium risk if they have a CVSS base score of 4.0 – 6.9
High risk if they have a CVSS base score of 7.0 – 10.0

Vulnerability Information

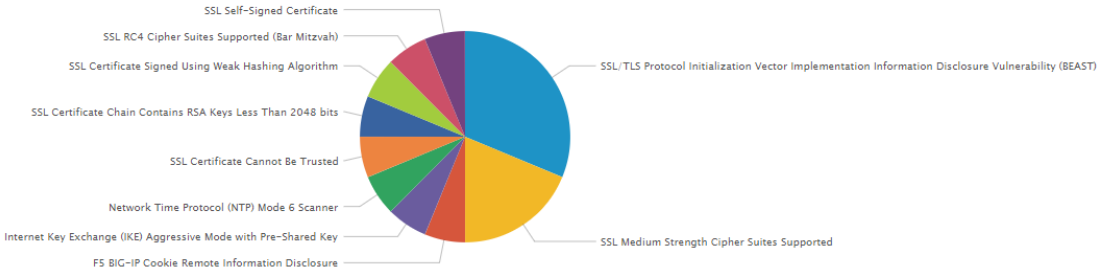
Graph: Risk Distribution
This report depicts the risk distribution of vulnerabilities discovered this report period



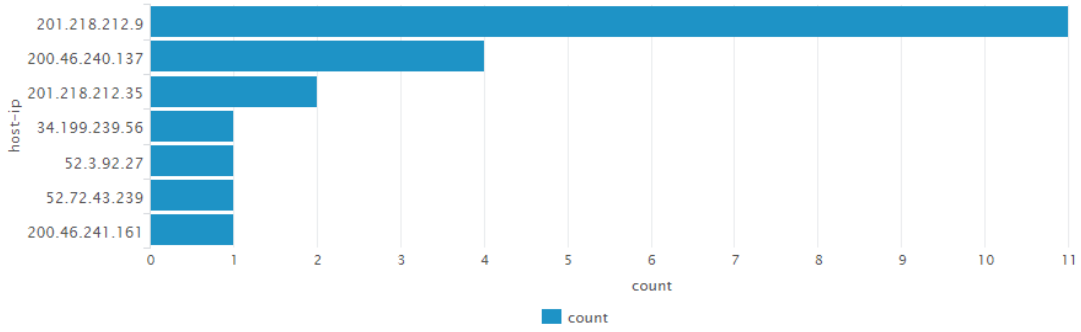
Graph: Most Frequent Vulnerability Category
This report depicts the most frequent vulnerabilities by category discovered this report period



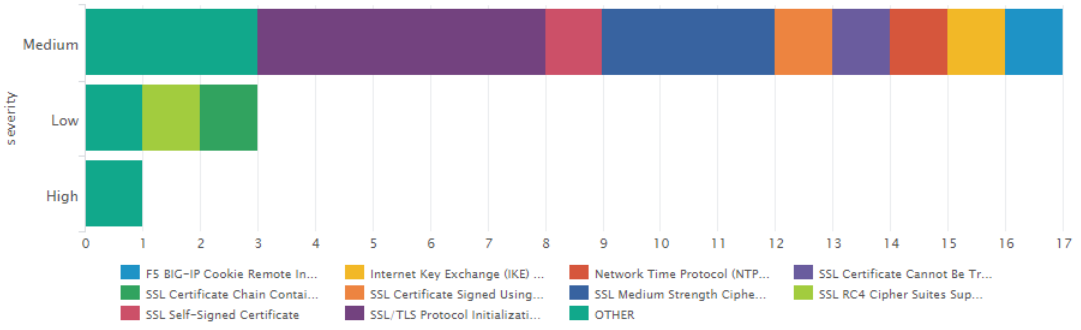
Graph: Most Frequent Vulnerability Name
This report depicts the most frequent vulnerabilities discovered this report period



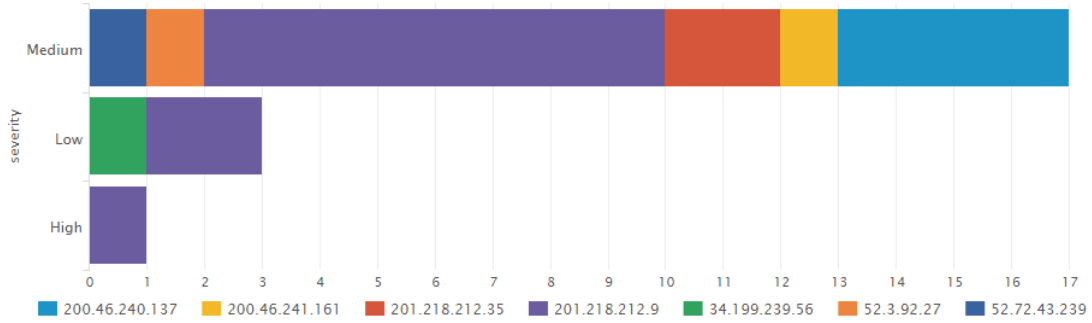
Graph: Most Vulnerable Host
This report depicts the most vulnerable hosts discovered in this report period



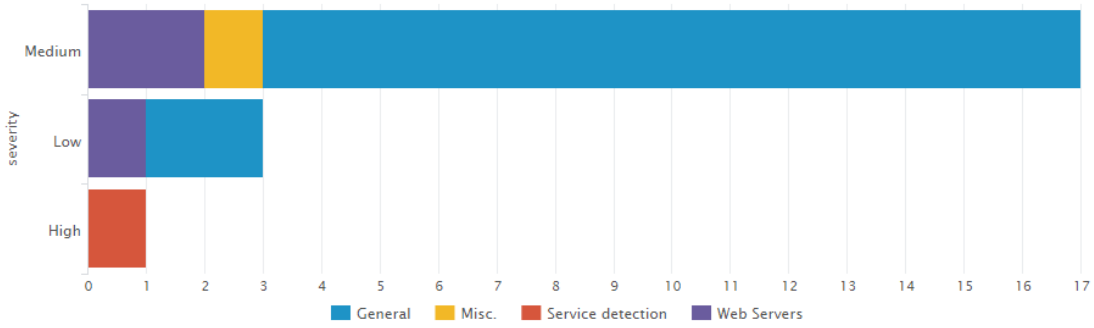
Graph: Vulnerability Risk by Vulnerability Name
This report illustrates the vulnerability risk and count by vulnerability name discovered this report period



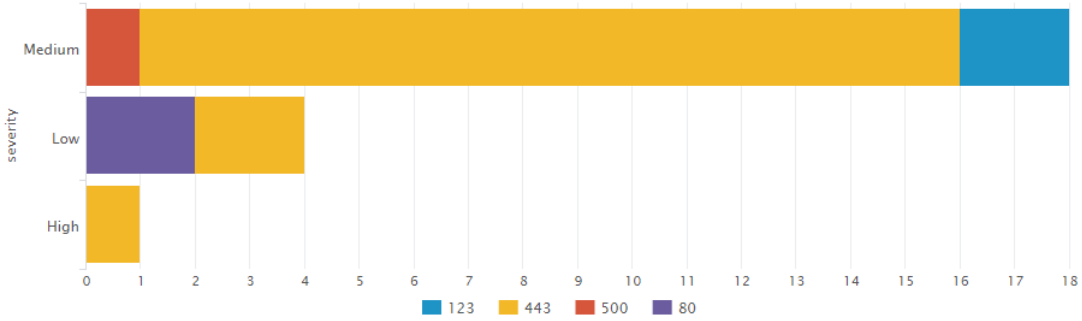
Graph: Vulnerability Risk by Host
This report illustrates the vulnerability risk and count by category discovered this report period



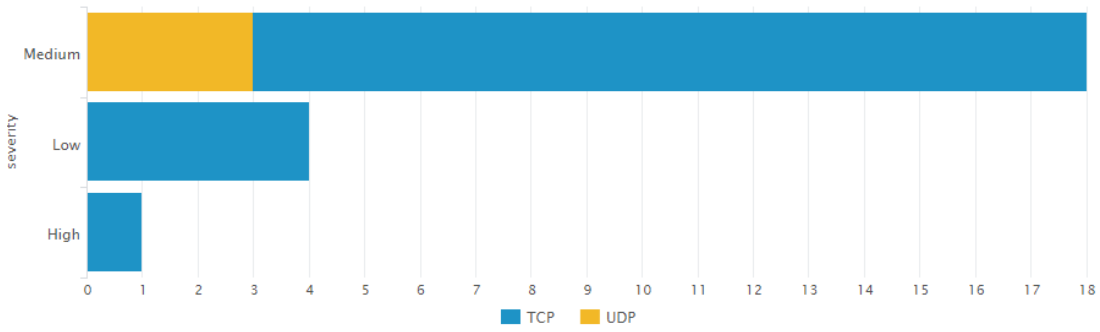
Graph: Vulnerability Risk by Category
This report illustrates the vulnerability risk and count by category discovered this report period



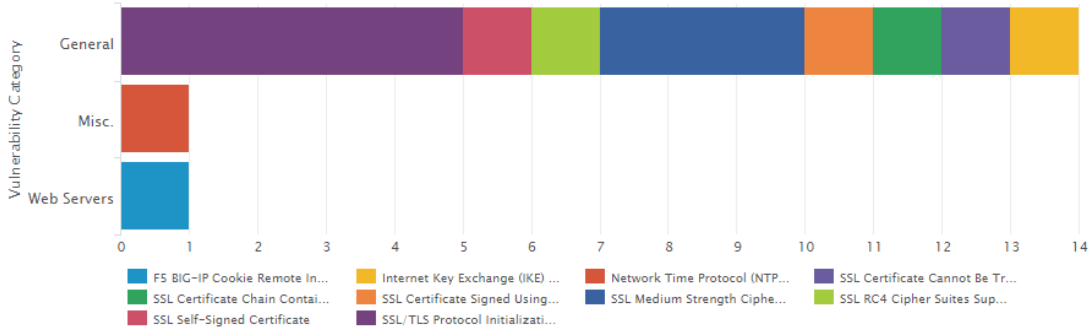
Graph: Vulnerability Risk by Port
This report illustrates the vulnerability risk and count by port discovered this report period



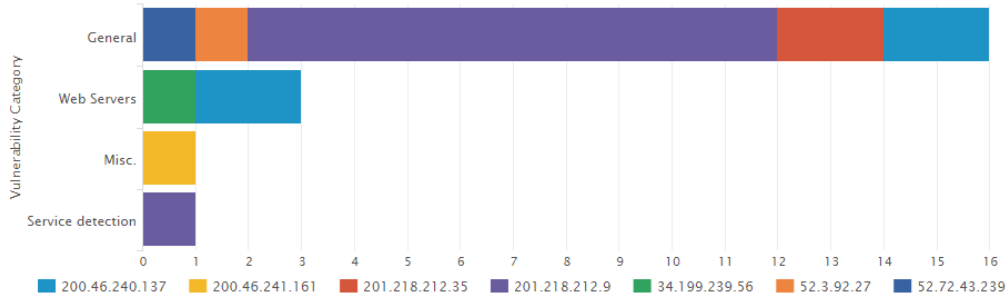
Graph: Vulnerability Risk by Protocol
This report illustrates the vulnerability risk and count by protocol discovered this report period



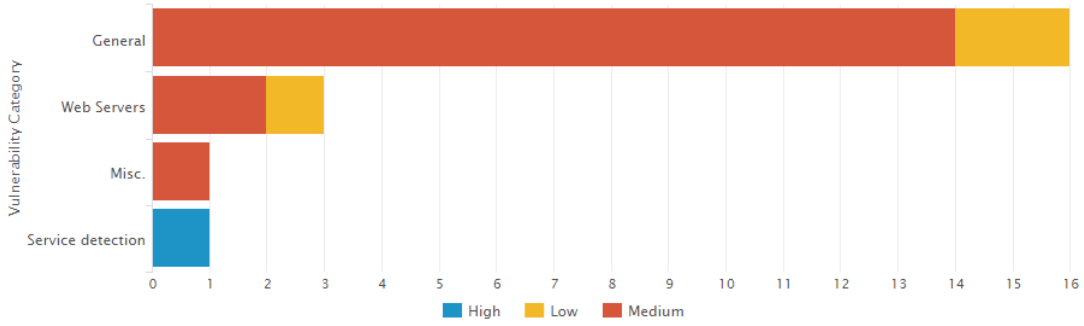
Graph: Vulnerability Category by Vulnerability Name
This report illustrates the vulnerability category and count by vulnerability name discovered this report period



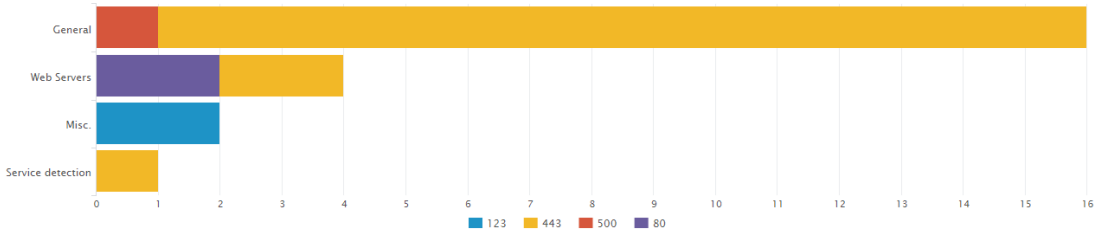
Graph: Vulnerability Category by Host
This report illustrates the vulnerability category and count by host discovered this report period



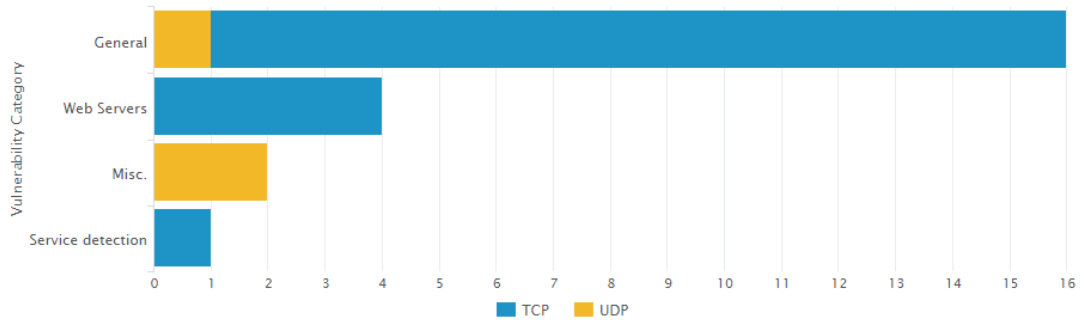
Graph: Vulnerability Category by Risk
This report illustrates the vulnerability category and count by risk discovered this report period



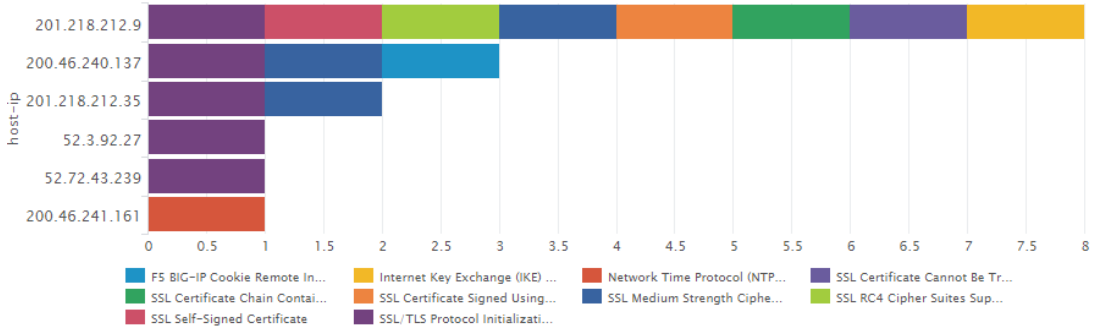
Graph: Vulnerability Category by Port
This report illustrates the vulnerability category and count by port discovered this report period



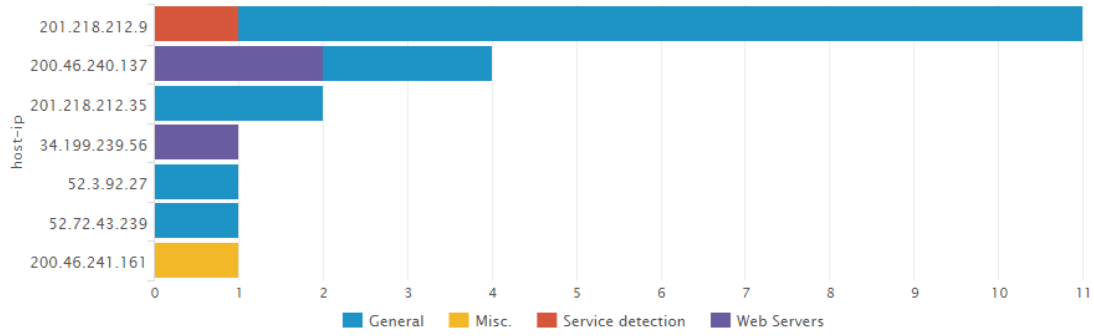
Graph: Vulnerability Category by Protocol
This report illustrates the vulnerability category and count by protocol discovered this report period



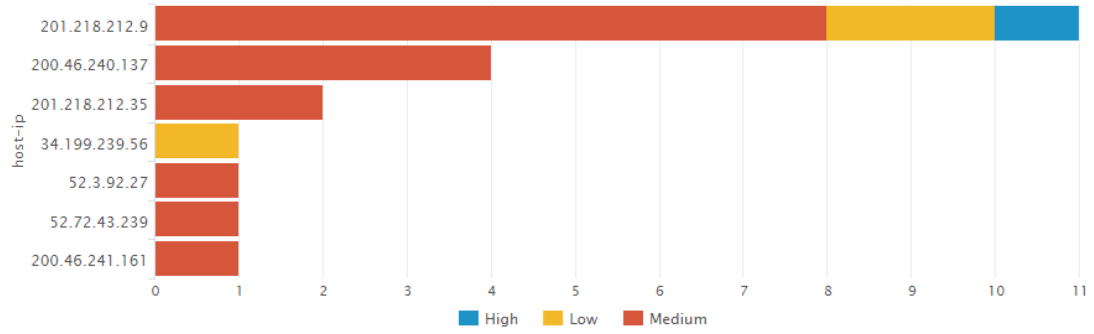
Graph: Host by Vulnerability Name
This report illustrates the vulnerability name and count by hosts discovered this report period



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

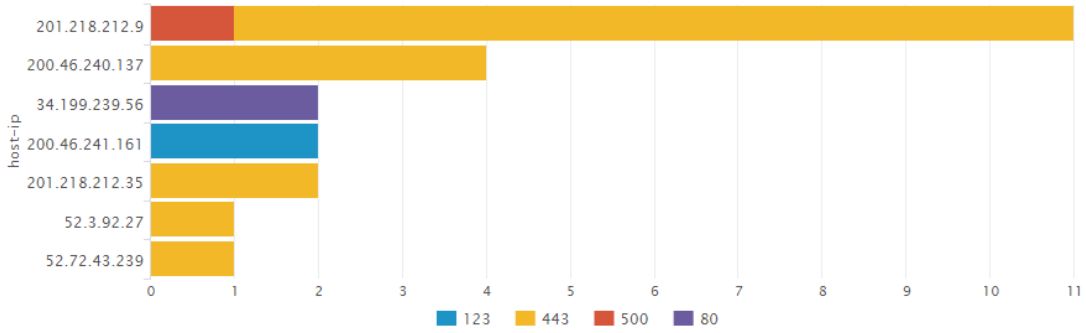


Graph: Host by Vulnerability Risk
This report illustrates the vulnerability risk and count by hosts discovered this report period



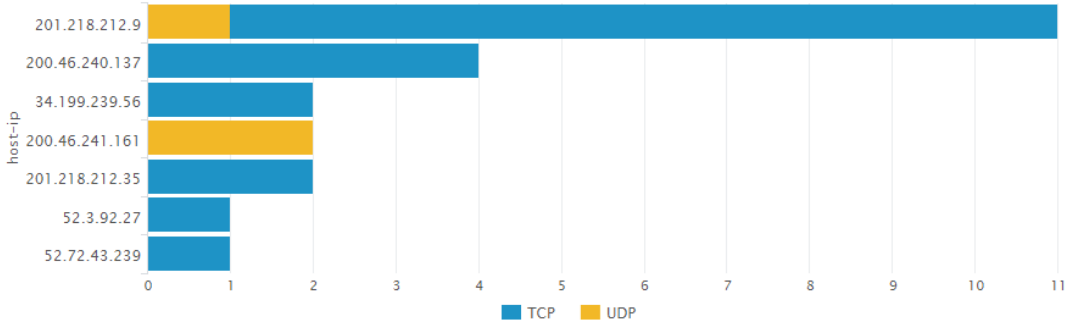
Graph: Host by Port

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



Graph: Host by Protocol

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



Managed Trusted Access Service (MSS-TAS) Intelligence Section

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. This is achieved by GLESEC's cloud-based service, part of the TIP™ platform.

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.

Graph: User two-factor authentication.
This graph shows the total users (active and inactive) for the two factor authentication method on your network.

436

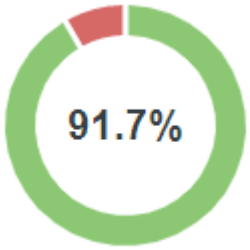
Graph: Total Endpoints.
This graph shows the number of different endpoints used to access your organization system during this period.

245

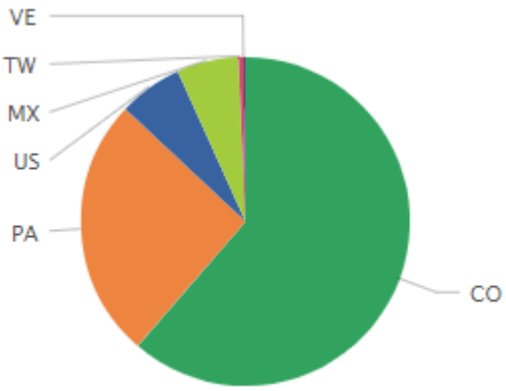
Graph: Endpoints out of date
This graph shows the number of devices that do not have the most recent updates installed.

Graph: Overview
This graph shows Success Rate of All Authentications

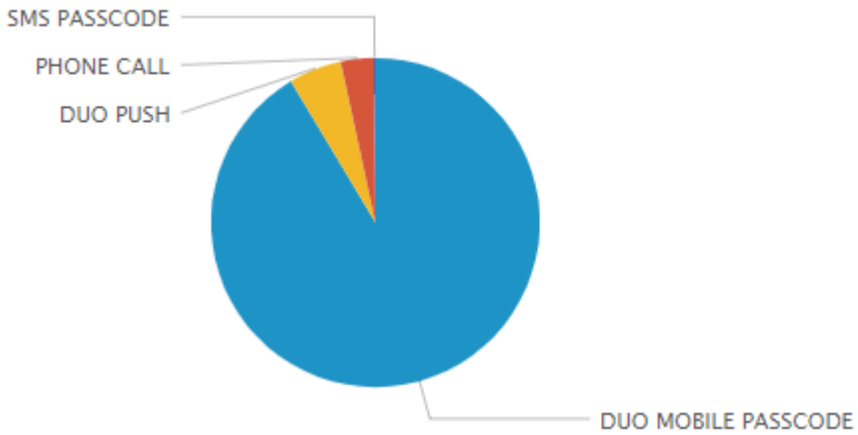
USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355



Graph: Authentication Per Country
This pie chart depicts the proportion of authentications from the different countries of origin



Graph: Successful Authentications by Factor
This pie chart shows the different authentication methods used when access was granted



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	1	0	0

TICKET ACTIVITY

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

Monthly Reports Copa 2018-09-01 00:00:00-2018-09-[..]

Number	Ticket#	Title	Created
1	2018092610000071	TLP AMBER Reporte de Incidencia COPA 1217	2018-09-26 17:09:48
2	2018091710000043	Reporte de Operaciones e Inteligencia, Agosto 2018	2018-09-17 10:24:03

All the services operated normally during the month of September.

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

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

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

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

Info@glesec.com
www.glesec.com