EY Case

BYU IS Program Orientation 2019

Christopher McLeod

Christopher Young

Dallin Fairbanks

Bonnie McDougal

Executive Summary

The focus of this report is to assess and strengthen VoydSec's internal security posture and analyze any possible cyber breaches. The findings of this report were gathered by performing a penetration test on the VoydSec network, analyzing the change management process, and investigating login records for any suspicious activity. Issues and risks that were discovered are risk ranked and correlating recommendations are given to mitigate possible impacts.

Penetration Test

The EY Advanced Security Center recently completed an external and internal penetration test of the VoydSec network and customer applications. The following assessments were conducted by EY:

- Internet Assessment
- Intranet Assessment
- Web Application Assessment
- Social Engineering/Phishing Assessment

A total of ten (10) key issues were identified and ranked in order of highest priority/risk to lowest. The current flaws in VoydSec's systems represent significant private and financial risks to VoydSec. To best mitigate these risks, we primarily recommend implementing a multi-factor authentication software. Timeline and cost estimates are also included for VoydSec to implement top recommendations.

Change Management Process

Based on our analysis, we discovered flaws in the change management process regarding

- Segregation of duties,
- Record Keeping, and
- Employee change request folder.

The flaws in the process result in high internal and external risks to the company. In order to mitigate these risks, we recommend restriction of admin access to only the engineering managers, separation of roles in the process, an entry log, and restriction of access to the change request folder.

We anticipate that these changes will occur within the next 6 months. Cost should be minimal, involving the new log entry system. However, this process change will require many labor hours from management.

Suspicious Logins

An analysis of the login attempt data provided yielded five (5) instances of suspicious activities that occurred during the time frame of the suspected breach. Each instance should be investigated further by the EY FTDS team.

Summary

To improve the cyber integrity and internal security at VoydSec, the recommended timeline of solutions should be implemented immediately.

Penetration Test

Attack and penetration assessments were performed on VoydSec's CSOC client portal environment, applications, and related infrastructure to discover the risk of exposure to security threats. These risks were ranked according to the OWASP and NIST SP 800-30 methodologies.

	Risk				
Assessment	**Very High**	**High**	**Moderate**	**Low**	**Very Low**
Web Application	0	1	1	0	0
Internet Testing	0	2	2	0	0
Intranet Testing	0	2	0	0	0
Social Engineering/Phishing	1	1	0	0	0

Issues and Risks

The key issues identified in the VoydSec Security Assessment, ranked from highest to lowest, are as follows:

1. User susceptibility to phishing campaigns (**very high**)
2. User workstation information disclosure (via successful phishing attack) (**high**)
3. Unencrypted protocols in use (**high**)
4. Use of outdated/insecure libraries (**high**)
5. Outdated software versions in use (**high**)
6. Vulnerable Windows Name Resolution Service in Use (**high**)
7. Windows Passwords stored as LAN Manager (LM) hashes (**high**)
8. Unnecessary page present in the production environment (**moderate**)
9. Missing content security policy header (**moderate**)
10. Reflected cross-site scripting exposures (**moderate**)

See Appendix A for the likelihood, impact, and business impact description for each risk.

Change Management Process

The current change management process (CMP) for the CSOC have several issues within the procedures and policies that produce a high level of risk for VoydSec.

Issues

Within VoydSec's CMP, several procedures and policies are cause for concern.

Consistent Engineer Assigned to Projects

Currently within the process, when a request to change the CSOC is submitted, one engineer does the following:

- Accesses and checks out the code
- Edits the code
- Tests the code
- Confirms the code to be correct
- Commits the code to deployment
- Pushes the code back to the system
- Monitors the code to ensure that it is working
- Makes version updates to the application as necessary

While this current procedure is convenient and simple for the company, it creates several severe and significant risks to the company.

Admin Access

All 160 engineers have admin access to the CSOC. Guaranteed access to all levels of the CSOC limits accountability and increases exposure to suspicious activity.

Employee Change Requests Folder

Currently, all change requests from employees to access the CSOC are stored on a network drive that engineers have access to.

Lack of Record Keeping for Engineer Access and Changes

The CMP has no procedure for engineers to document access and changes to the CSOC.

Risks

The issues we addressed in the CMP expose several risks to VoydSec. The risks we found, ranked from highest risk to lowest are

1. Malicious insider attacks from an engineer (**very high**)
2. Non-malicious insider attacks from an engineer (**high**)
3. Malicious attacks from a hacker (**high**)
4. Malicious insider attacks from an employee (**high**)

For a more detailed report of these conclusions, see Appendix B.

Recommendations

We identified recommendations to mitigate the key issues and risks found in VoydSec's Change Management Process and Penetration Assessment Results.

Penetration Test

Top recommendations for restoring security integrity and solving key security issues/risks (listed above) at VoydSec are as follows:

- Subscribe to Duo Security Dual Authentication software for all employees (solves penetration risks 1, 2, 3, 6, 7)
- Implement annual training on current fraudulent (phishing) attack methodology (penetration risks 1, 2)
- Require annual password reset from current employees (penetration risks 1, 2, 6, 7)
- Disable LLMNR/NBNS protocol for each employee computer and via system group policy (penetration risks 6, 7)
- Implement NoLMHash Policy for each employee computer and via system group policy (penetration risk 7)
- Better manage production environment by removing unnecessary/completed pages into appropriate files; separate development and production environments (penetration risk 8)
- Ensure proper authorization for entering production and development environments by implementing access controls (penetration risk 8)
- Update company software to these latest versions: Apache 2.4.41, Apache Tomcat 9.0.24, PHP/7.3, jQuery v3.4.1 (penetration risks 4, 5)
- Assign the following responsibilities to VoydSec's IT Team:
    1. Regularly check for and apply software updates/patches/fixes to entire VoydSec system (penetration risk 3, 4, 5, 9)
    2. Update and maintain communication protocols; apply File Transfer Protocol Secure (FTPS) for data transfer and storage (penetration risk 3)
    3. Consistently monitor outdated and unencrypted protocols to protect against data leaks and breaches (penetration risk 3)
    4. Acquire and install SSL Certificates to strengthen web server security and protect private information (penetration risk 3)
- Implement OWASP XSS Prevention steps (penetration risk 10)
- Enable/create Content Security Policy (CSP) for affected hosts and as a safeguard against XSS (penetration risks 9, 10)
- Manage and update CSP for new website releases and monitor reported violations in browser console log (penetration risk 9)

Change Management Process

In accordance with the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework, we recommend several guidelines to help minimize risk within the CMP at VoydSec. A process diagram will be outlined later in Appendix C.

Segregation of Duties

To help eliminate the vulnerability of the system, we recommend separating out the different duties within the change management process. Only the eight managers of the engineering team will have access to check-in and check-out code for editing and updating. These managers do not have access or authority for code editing and developing.

The change management process will follow these six steps:

1. Check out code for editing/updating
2. Update and/or edit the code
3. Test and approve the code
4. Commit the code for deployment
5. Push code back into the system
6. Monitor code to ensure function

A different engineer will be assigned to each step.

Record Keeping

Once receiving his or her assignment, an engineer is responsible for leaving a detailed log of what he or she accomplishes on the assignment. The log will start with the managers who downloads the document. With the download, he or she will include a detailed entry of what is expected with the batch. The batch will then be passed on to the engineers assigned to the project. These engineers may include notes to help other engineers understand what happened in the process. This log will be uploaded to a secured network drive only accessible to the managers of the engineering department.

Employee Change Request Folder

The employee change request folder should only be shared with the customer support managers in order to prevent editing in the event of fraud or attacks.

Analysis of Login Attempts

Following is a list of suspicious login activities drawn from the login data provided. We recommend that they be investigated by the FTDS team:

- There was a large amount of login activity from Manaus, Brazil; Beijing, China; St. Petersburg, Russia; and Pyongyang, North Korea, none of which are considered primary business locations of Voydsec (Chart D-1).
    - The login activity from China, Russia, and Korea appears coordinated (Chart D-7) and consists of attempts with failure percentages exceeding 90% (Chart D-1 and D-8)
    - The login data from Manaus, Brazil more closely mirrors regular company activity in success/failure percentages, login attempt quantity, and the hours of login attempts in local time (Charts D-2 and D-3).
- In Los Angeles, there were a large number of failed login attempts from a single IP address (79.94.36.131) during business hours that may indicate an insider threat (Charts D-4 and D-9)
- In Charlotte, North Carolina there is suspicious after-hours activity around 9:00 p.m. local time from a single IP address (106.154.21.164) with an 80% failure rate (Chart D-5).
- Login activity in Sao Paulo begins around 10:00 a.m. local time and ends around 10:00 p.m. local time. (Chart D-6)

Implementation Guide

Penetration Test Recommendations Implementation Guide		
Immediate Actions	**Resources Required**	**Estimated Cost**
Subscribe to Duo Security Dual Authentication	Duo Beyond services are $9 per user per month	$24,000 (year's subscription for approximately 200 users)
Update all software and libraries within the system	Updates are available for free from vendor websites	No expected cost
Require all employees to change password	None	No expected cost
Within 1 month	**Resources Required**	**Estimated Cost**
Assign recommended responsibilities (see page #) to VoydSec IT Team	Labor hours required for training IT Team Purchase a 2 year EV SSL top protection license for $500	$500
Separate development and production environments and organize appropriate files within (see new CMP)	Labor hours required to separate environments (4-5)	No expected cost
Implement proper access controls for development and production environments	Labor hours required to set up access controls (4-5)	No expected cost
Within 6 months	**Resources Required**	**Estimated Cost**
Hold annual fraudulent activity training for all employees	Estimated $5000 for training set-up, food, and guest expert Labor hour cost (1 hour)	$5000
Implement OWASP XSS Prevention Steps	Training for development engineers Labor hour cost for updating current system	$1000
Disable LLMNR/NBNS Default Protocols via system group policy	Labor hour (1)	No expected cost
Enable/create a client-side Content Security Policy (CSP) to protect sensitive web information	Labor hours required (unknown amount)	No expected cost
Implement NoLMHash policy via system group policy	Labor hour (1)	No expected cost

CMP Recommendations Implementation Guide

Immediate Actions	Resources Required	Estimated Cost
Remove admin access from all engineers	Labor hours required	No expected cost
Give engineers access to only edit and update code	Labor hours required	No expected cost
Give engineering managers access to only pull and push code from and into the system	Labor hours required	No expected cost
Plan training for new CMP process (to be given within the week)	Labor hours required	No expected cost
Begin designing log entry process	Time with consultant to build system	$3000
Restrict access to change request folder to only customer support managers	Labor hours required	No expected cost
Within 1 month	**Resources Required**	**Estimated Cost**
Begin implementing new CMP for all projects	Labor hours required	No expected cost
Execute training to the engineering department for how to utilize the new record-keeping system	Labor hours required	No expected cost
Begin utilizing log entry system for all engineers and managers	Labor hours required	No expected cost
Within 6 months	**Resources Required**	**Estimated Cost**
Distribute surveys to the engineers to evaluate how the changes are being implemented and received	Labor hours required	No expected cost

Appendix A: Penetration Test Risks

User susceptibility to phishing campaigns

Twelve percent of VoydSec employees exposed sensitive information in the mock phishing and social engineering assessment. The unawareness of phishing methods, despite email filtering services, is a very high risk to VoydSec. Via phishing, a malicious attacker can obtain user credentials, financial information, and personal information.

	Risk
Overall Risk	**Very High**
Likelihood	**Very High**
Technical Impact	**High**
Business Impact	**Very High**

Business Impact:

- Private financial data exposed
- Significant revenue loss (if attacker obtains financial credentials)
- Major damage to brand reputation
- Customer and employee privacy intrusion

User workstation information disclosure (via successful phishing attack)

Successful phishing attacks also passively share information about the users' workstation including the operating system, browser, and plugins. An attacker can use this information to send specific malware to the user workstation which can result in data corruption or ransom, and privacy intrusion.

	Risk
Overall Risk	**High**
Likelihood	**High**
Technical Impact	**High**
Business Impact	**Moderate**

Business Impact:

- Private financial data exposed
- Small to large impact on annual revenue
- Major damage to brand reputation
- Privacy intrusion

Unencrypted Protocols in Use

File transfer protocols were accessed from the internet. Using FTP provides no security to the files that are being transferred which means that anyone that may be looking can easily steal or corrupt that data. If not secured properly this could lead to a data breach that could compromise the sensitive data of the clients.

	Risk
Overall Risk	**High**
Likelihood	**High**
Technical Impact	**Moderate**
Business Impact	**Moderate**

Business Impact:

- Significant effect on annual revenue
- Private data compromised
- Damage to brand
- Violations due to non-compliance

Use of Outdated/Insecure Libraries

Out of date and insecure libraries leave the door open for attackers to find known vulnerabilities that can easily be exploited. Through these vulnerabilities, they can get insights into how the software and system are constructed which they can then use as leverage in an attack to either steal valuable information or disrupt the system.

	Risk
Overall Risk	**High**
Likelihood	**Moderate**
Technical Impact	**High**
Business Impact	**High**

Business Impact:

- Moderate decrease in annual profit
- Loss of goodwill among customers
- Possible violations due to non-compliance
- Damage to system

Outdated Software Versions in Use

Multiple cases of outdated or unpatched software were discovered in the system. Hackers can use automated tools to discover these known vulnerabilities and then easily exploit their individual weaknesses. They can breach the system to steal private information or plant viruses/malware in the affected places.

	Risk
Overall Risk	**High**
Likelihood	**High**
Technical Impact	**Moderate**
Business Impact	**Moderate**

Business Impact:

- Loss of sensitive information
- Decrease in goodwill among customers
- Potential damage to software structures
- Minor effects on annual profit

Vulnerable Windows Name Resolution Service in Use

Hosts in the VoydSec Windows Domain were vulnerable to the Link Layer Multicast Name Resolution (LLMNR) spoofing attacks. When a host seeks to resolve a name it is looking for, Windows will fall back to legacy name resolution protocols (NBNS/LLMNR). These protocols will seek to resolve the request by broadcasting to the network.

While on the local subnet, an attacker can spoof a response to the requests and redirect the requesting host to the attacker's system. This allows an attacker to respond to the request traffic as if it knows or is the requested name site, effectively poisoning the system so that the host will communicate with the attacker. The attacker can then receive the hashed version of network/login credentials and from the host computer, and convert them into cleartext.

	Risk
Overall Risk	**High**
Likelihood	**Moderate**
Technical Impact	**High**
Business Impact	**Moderate**

Business Impact:

- Confidential data exposed
- Non-compliance exposure
- Brand damage

Windows Passwords stored as LAN Manager (LM) hashes

Password hashes obtained from VoydSec’s domain controller revealed multiple accounts to have both Lan Manager (LM) and NTLM hashes stored. Attackers can easily break LM hash passwords and gain access to system and user credentials.

	Risk
Overall Risk	**High**
Likelihood	**Moderate**
Technical Impact	**High**
Business Impact	**Moderate**

Business Impact:

- Financial information can be accessed
- Personal information disclosed

Unnecessary Page Present in the Production Environment

Pages and files that no longer function as a part of the working production environment can be easily exploited to disclose how the programming of the website and the overall system works. In the wrong hands, this information can then be leveraged to either steal data or obstruct the functionality of the overall system.

	Risk
Overall Risk	**Moderate**
Likelihood	**High**
Technical Impact	**Moderate**
Business Impact	**Moderate**

Business Impact:

- Minor effects on annual profit
- Potential for loss of major accounts
- Potential damage to the system
- Exposure due to non-compliance

Missing Content Security Policy (CSP)

CSP’s control what content the web page can load by only allowing certain domains, subdomains, and other resources. When the CSP is missing like in this case the site is vulnerable to cross-site scripting, formjacking attacks, and malware that injects unwanted ads onto the website. The consequences of these breaches can vary from annoying ads to sensitive information leaks.

	Risk
Overall Risk	**Moderate**
Likelihood	**Moderate**
Technical Impact	**Moderate**
Business Impact	**Moderate**

Business Impact:

- Violations for non-compliance
- Possible damage to website structure
- Loss of goodwill among customers
- Unwanted content on websites

Reflected Cross-Site Scripting Exposures

This type of attack occurs typically when the attacker will inject malicious code into the JavaScript of the victim's browser. This happened on the VoydSec search gateway when we performed our test. Reflected XSS typically must be interacted with to be dangerous but when it is interacted with, sensitive data may be lost.

	Risk
Overall Risk	**Moderate**
Likelihood	**High**
Technical Impact	**Moderate**
Business Impact	**Low**

Business Impact:

- Loss of private sensitive information
- Major accounts compromised
- Minor financial damage
- Potential for loss of goodwill

Appendix B: CMP Risks

This section offers more detail on the risks involved in the CMP.

Malicious Insider Attacks from an Engineer

VoydSec gives admin access to all 160 engineers and does not practice segregation of duties for the CMP. Because of this, the overall risk of an engineer making a malicious attack on the customer portal application, operating system, and database is **very high**. We concluded this risk based on the likelihood, technical impact, and business impact involved in this risk.

	Risk
Overall Risk	**Very High**
Likelihood	**Very High**
Technical Impact	**High**
Business Impact	**High**

Business Impact:

- Major damage to finances (financial data exposed to the attacker)
- Major damage to reputation
- Customer privacy violated
- Non-compliance to COSO

Non-Malicious System Error from an Engineer

Due to the vulnerability of the system through admin access, the overall risk of a non-malicious attack from an engineer is **high**.

	Risk
Overall Risk	**High**
Likelihood	**High**
Technical Impact	**High**
Business Impact	**High**

Business Impact:

- Possible major damage to finances (depending on what the engineer does)
- Major damage to reputation
- Customer privacy violated
- Non-compliance to COSO

Malicious Attacks from a Hacker

If a hacker could access an engineer's account, he or she could inflict major damage to the company through the customer portal. The risk of a malicious attack from a hacker is **high**.

	Risk
Overall Risk	**High**
Likelihood	**High**
Technical Impact	**High**
Business Impact	**High**

Business Impact:

- Major damage to finances (financial data exposed to the attacker)
- Major damage to reputation
- Customer privacy violated
- Non-compliance to COSO

Malicious Insider Attacks from an Employee

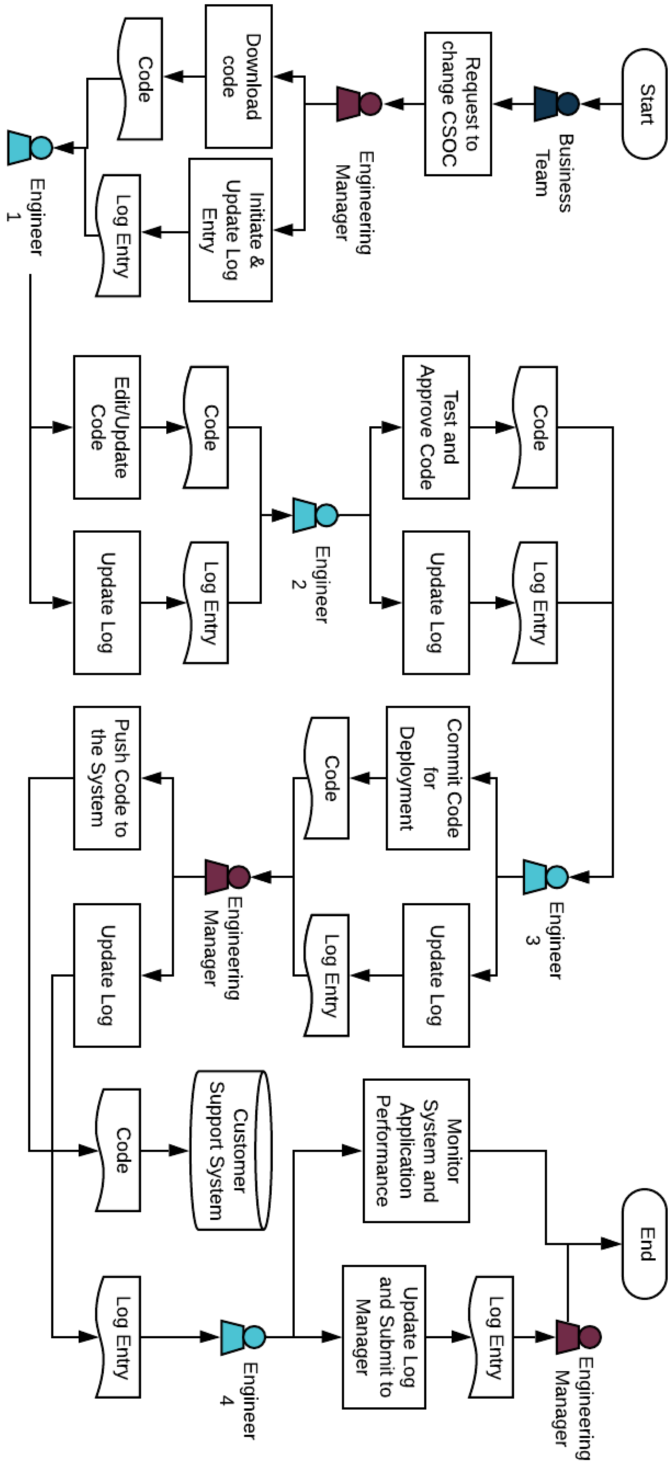
While non-engineer employees within VoydSec may not have the same technical skills or access as the engineers, the risk of an attack from an employee is still **high**.

	Risk
Overall Risk	**High**
Likelihood	**High**
Technical Impact	**High**
Business Impact	**High**

Business Impact:

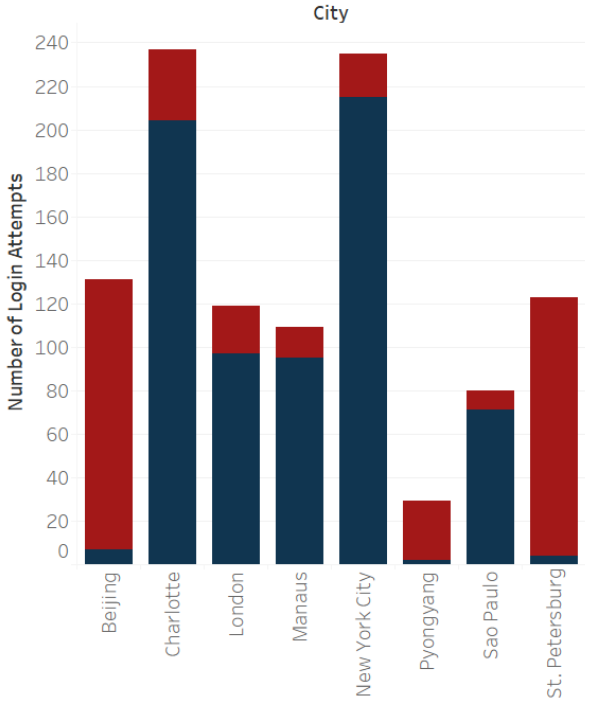
- Major damage to finances (financial data exposed to the attacker)
- Major damage to reputation
- Customer privacy violated
- Non-compliance to COSO

Appendix C: New CMP Diagram



Appendix D: Login Attempt Visualizations

D-1

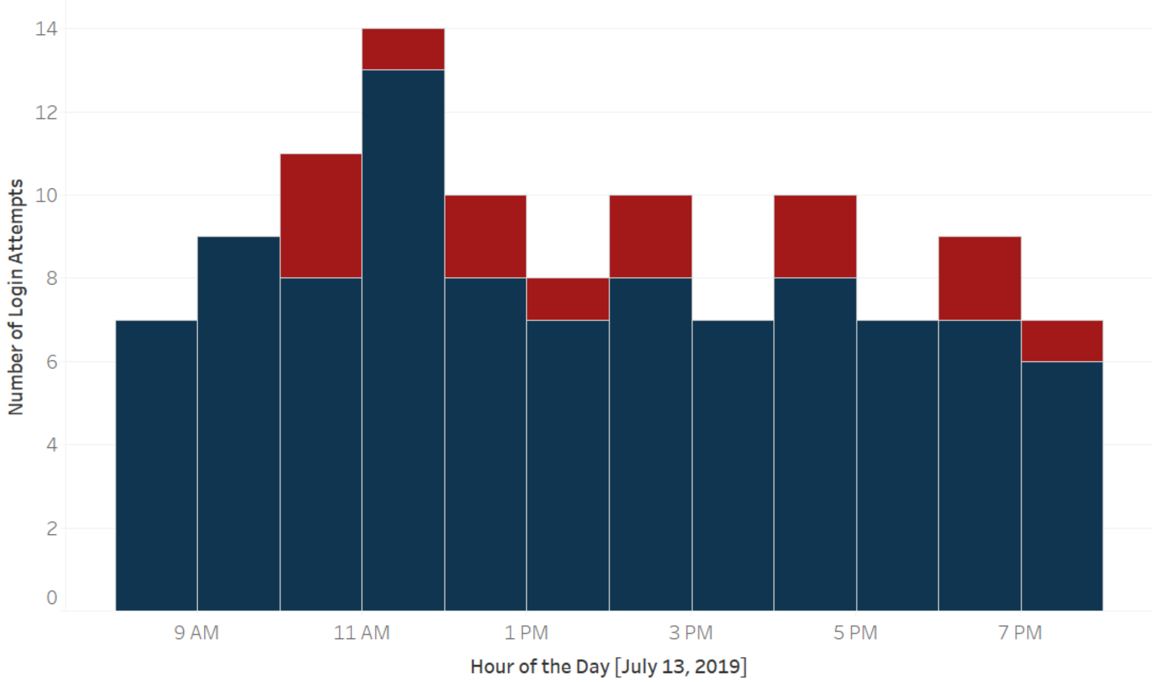

Login Attempts by City

Success / Failure

🟥 Failure

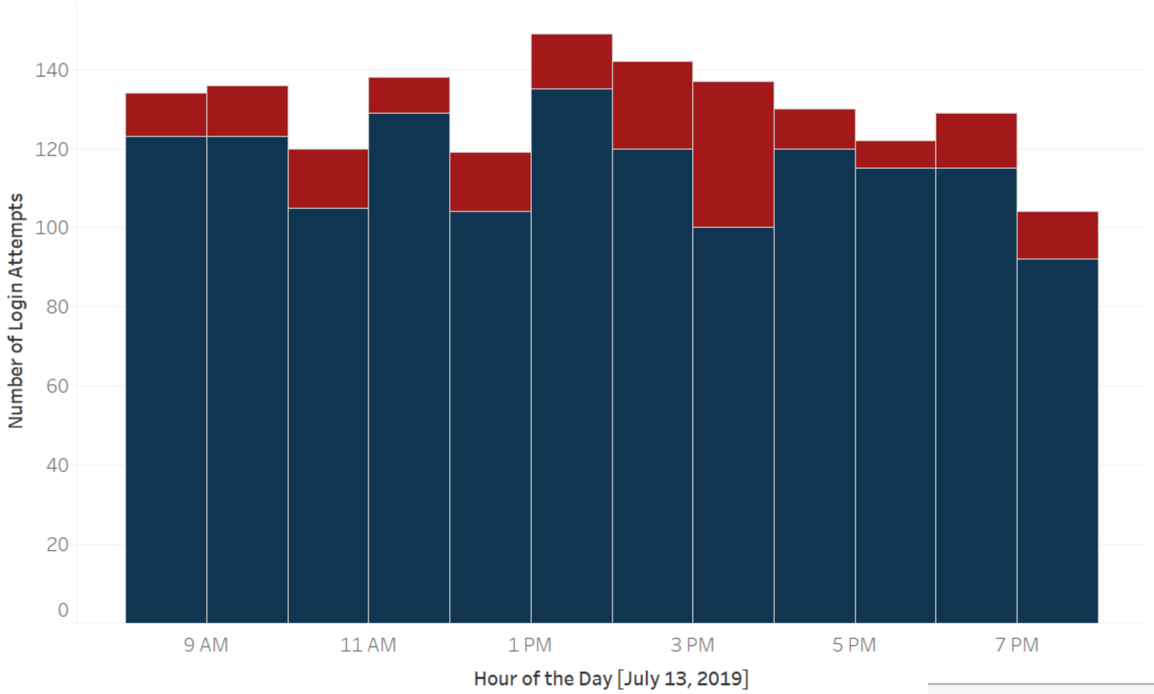
■ Success

D-2


Manaus Local Time

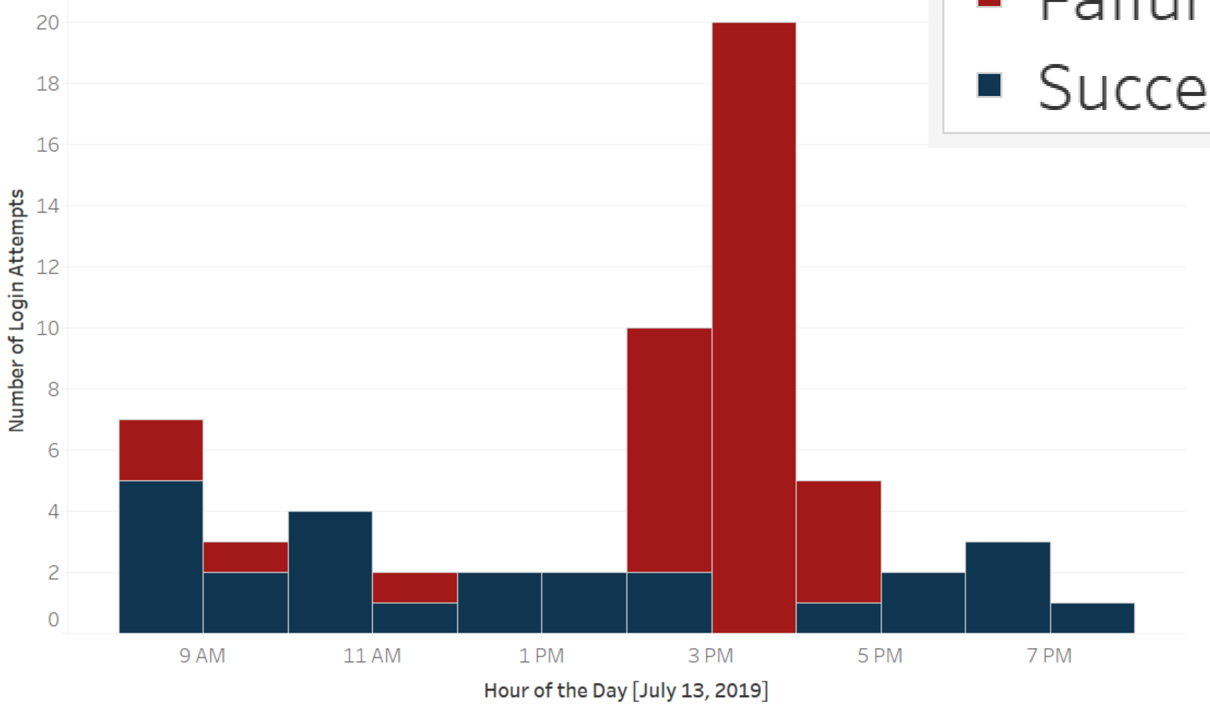
D-3

Los Angeles Local Time



D-4

Los Angeles Suspicious IP Address Activity Over Time



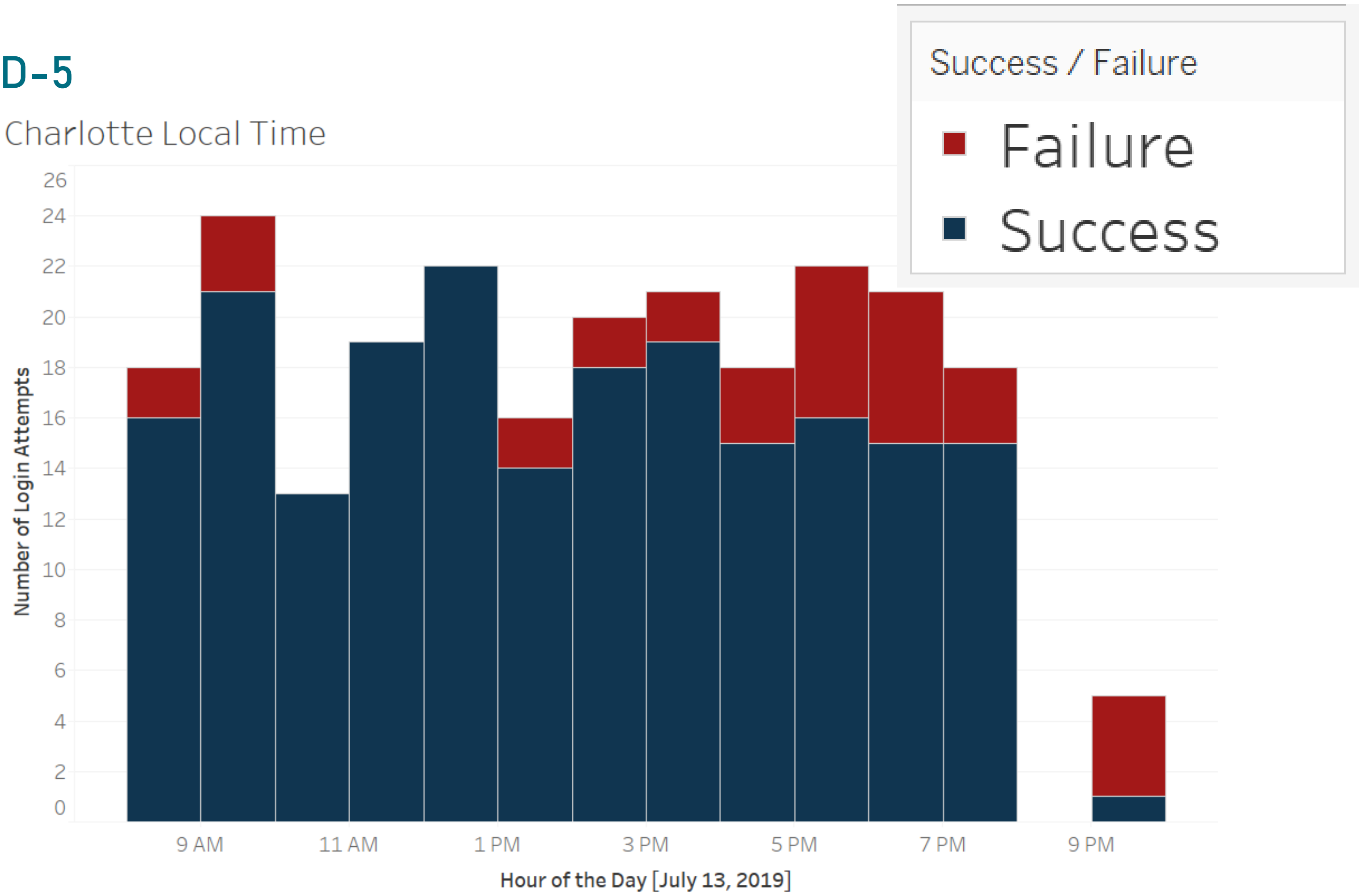
Success / Failure

🟥 Failure

■ Success

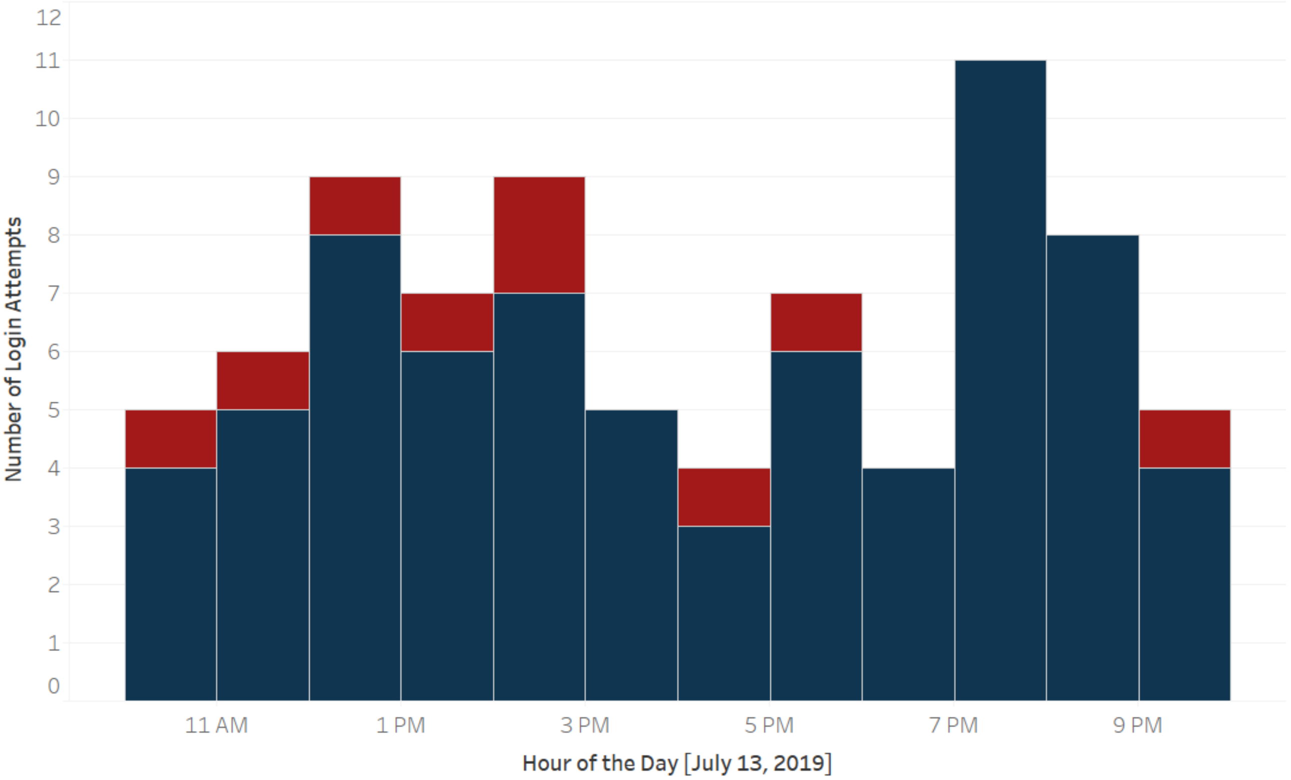
D-5

Charlotte Local Time

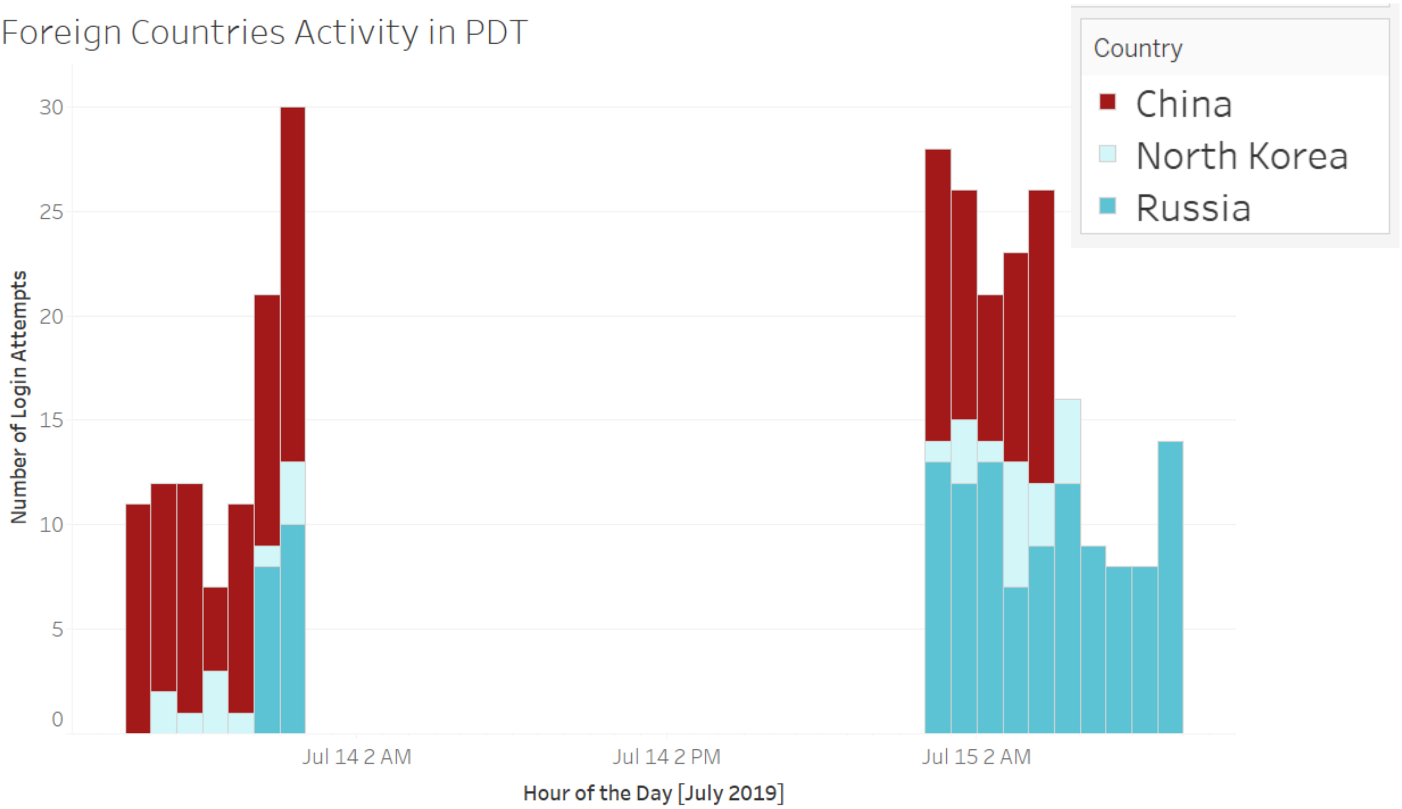


D-6

Sao Paulo Local Time



D-7



Foreign Countries Activity in PDT

D-8

Success v. Failure Percentages by City

Row Labels	Failure	Success
Beijing	94.66%	5.34%
Charlotte	13.92%	86.08%
London	18.49%	81.51%
Los Angeles	11.47%	88.53%
Manaus	12.84%	87.16%
New York City	8.51%	91.49%
Pyongyang	93.10%	6.90%
Sao Paulo	11.25%	88.75%
St. Petersburg	96.75%	3.25%

D-9

Top 11 IP Addresses With Most Failed Login Attempts

IPAddress	Device	Country	City	failCount	successCount
79.94.36.131	WIN4716036	USA	Los Angeles	36	25
170.89.46.80	WIN2786070	China	Beijing	34	3
154.39.66.81	WIN5174268	Russia	St. Petersburg	33	0
155.63.82.36	WIN2658376	Russia	St. Petersburg	32	2
163.34.149.32	WIN6317655	China	Beijing	31	3
170.143.33.75	WIN9307545	China	Beijing	31	1
154.159.72.99	WIN8498262	Russia	St. Petersburg	29	2
169.156.61.69	WIN6854530	China	Beijing	28	0
158.116.125.26	WIN9567273	North Korea	Pyongyang	27	2
152.62.32.64	WIN1171331	Russia	St. Petersburg	25	0
106.154.21.164	WIN8844618	USA	Charlotte	10	18