NAME : Edward Course : IT Risk Management and Disaster Recovery
NIM : 2201741971 Course Code : COMP8040
CLASS : LTY1 Faculty / Department : Binus Graduate Program / Master Track
Essay

1. **[10 point]** Mengapa information security sangat dibutuhkan di era sekarang? Jelaskan detail!

   Answer:

   Information security has evolved from addressing minor and harmless security breaches to managing those with an enormous impact on organization's economic process within the youth of computing. **Security breaches mainly included viruses and worms** that might flash a message or advertisement on the screen without causing any serious damage to the information or systems. However, in rare cases of attacks with the potential to harm information did occur **(Denning, 1991)**.

   As an example, a security breach like the leakage of credit card information can imply a huge damage to card payment companies because of the cancellation and re-issuing of cards, this might also be very expensive as it cost many dollars in penalties to regulatory compliance bodies.

   The case of a gang of Europeans who cloned 32000 credit cards worth £17 million was reported within the Computer Fraud and Security News in 2007 because the biggest (yet) uncovered credit card fraud, this is just a glimpse of losses associated with today's threats.

   It is therefore vital for companies to note that their strength in achieving and sustaining competitiveness within the highly volatile, demanding, and unsure markets lies in their ability to securely protect their information assets and IT infrastructure **(Conray-Murray, 2003)**.

   Organizations would roll in the merely because everybody else is doing it and it's the demand of the day. However, slowly but surely information security is stepping into the forefront of things and has been promoted from a by-product to an integral a part of business operations **(Conner and Coviello, 2004)**.

   The 21st century innovations and developments came alongside a robust dependency thereon infrastructure this leads to open new and attractive doors for the hacking community. Attackers have been evolved as from computer enthusiasts to professional hackers **(Gelbstein, 2006)**.

Bruce Schneider in Anderson (2008) quoted a research that it is merely amateurs who still target machines, career criminals now target people that operate them not only for fun but for financial gains.

Attackers have matured from using hacking skills to point out that they will circumvent the authentication process to access each other's files to use them within the theft of important information and resulted in information security threats like fraud, social engineering, phishing, etc. which may easily compromise authentication and authorization credentials.

Nowadays the motive of an attacker is financial gains and so as to evade the ''long arm of law'', they will do everything to hide their tracks. As an answer and additionally to the authorization and authentication credentials, verification of users became necessary for access. Now the banks has also introduced chip-and-pin non-repudiation has since become a critical issue of the 21st century.

Now the focus of cyber criminals has shifted from stored data to industrial processes and control system to destroy and disrupt related data. New trends show that cyber criminals try to destroy data integrity rather infiltrating the data. **So there is a need not only to take preventive measures but also corrective measures to deal with the data in today's era**.

REFERENCES :

Denning PJ. Computers under attack: intruders, worms, and viruses. United States of America: Addison-Wesley Publishing Company; 1991.

Conray-Murray A. Strategies & issues: justifying security spending.; 2003.

Botha RA, Gaadingwe TG. Reflecting on 20 SEC conferences. Computers and Security 2006.

Gordon LA, Loeb MP, Lucyshyn W, Richardson R. CSI/FBI computer crime and security report.; 2006.

2. **[15 point]** Sila akses www.us-cert.gov dan buatlah daftar (list) dan beri penjelasan detail mengenai 7 virus dan atau worm terbaru yang dapat anda identifikasi!

Answer:

a) BlackMatter Ransomware (AA21-291A)

First Seen : July 2021

Release Date : 18 October 2021

Sector Target : Critical Infrastructure including Food and Agriculture.

Overview : It is leveraging the Lightweight Directory Access Protocol (LDAP) and Server Message Block (SMB) protocol to access the Active Directory (AD) to discover all hosts on the network then remotely encrypts the hosts and shared drives as they are found.

Mitigation :

- Implement Detection Signatures that will identify and block placement of the ransom note on the first share that is encrypted, subsequently blocking additional SMB traffic from the encryptor system for 24 hours.
- Use Strong Passwords should not be reused across multiple accounts or stored on the system where an adversary may have access.
- Keep all operating systems and software up to date to minimize its exposure to cybersecurity threats.
- Limit Access to Resources over the Network such as use a host-based firewall to only allow connections to administrative shares via SMB from a limited set of administrator machines.
- Implement Network Segmentation to help prevent the spread of ransomware by controlling traffic flows "between and access to" various subnetworks and by restricting adversary lateral movement and Traversal Monitoring such as Endpoint detection and response (EDR) tools for detecting lateral connections into common and uncommon network connections for each host.
- Implement time-based access for accounts set at the admin level and higher and disable command-line and scripting activities and permissions.
- Maintain offline backups of data and ensure all backup data is encrypted and immutable.

b) Conti Ransomware (AA21-265A)

First Seen : May 2020

Release Date : 22 September 2021

Sector Target : Healthcare such as Emergency Medical Services.

Overview : Unauthorized access to victim networks through weaponized malicious email links, attachments, or stolen Remote Desktop Protocol (RDP) credentials and observed inside the victim network between four days and three weeks on average before deploying Conti ransomware, primarily using dynamic-link libraries (DLLs) for delivery. If the victim does not respond to the ransom demands two to eight days after the ransomware deployment, Conti actors often call the victim using single-use Voice Over Internet Protocol (VOIP) numbers.

Mitigation :

- Implement and ensure robust network segmentation between networks and functions by define a demilitarized zone that eliminates unregulated communication between networks.
- Enable strong spam filters containing executable files to prevent to prevent phishing emails and attachment from reaching end users by Implement a user training program to discourage users from visiting malicious websites or opening malicious attachments.
- Filter network traffic to prohibit ingress and egress communications with known malicious IP addresses and implement a URL blocklist to prevent users from accessing malicious websites.
- Keep all operating systems and software up to date to minimize its exposure to cybersecurity threats.
- Implement endpoint and detection response tools to allow a high degree of visibility into the security status of endpoints and can help effectively protect against malicious cyber actors.
- Limit Access to Resources over the Network such as restricting RDP.
- Regularly audit administrative user accounts and configure access controls under the principles of least privilege and separation of duties and regularly audit logs to ensure new accounts are legitimate users.

c) TrickBot Malware (AA21-076A)

First Seen : October 2016

Release Date : 17 March 2021

Sector Target : legal and insurance organizations and banking organization.

Overview : spread primarily by spear phishing campaigns using tailored emails that contain malicious attachments or links, which if enabled will execute malware. The phishing emails contain links that redirect to a website hosted on a compromised server that prompts the victim to click on photo proof of their traffic violation. In clicking the photo, the victim unknowingly downloads a malicious JavaScript file that, when opened, automatically communicates with the malicious actor's Command and Control (C2) server to download TrickBot to the victim's system.

Mitigation :

- Consider drafting or updating a policy addressing suspicious emails that specifies users must report all suspicious emails to the security and/or IT departments.
- Mark external emails with a banner denoting the email is from an external source to assist users in detecting spoofed emails.
- Implement filters at the email gateway and block suspicious IP addresses at the firewall and Implement an antivirus program and a formalized patch management process.
- Implement a Domain-Based Message Authentication, Reporting & Conformance validation system and Implement Group Policy Object and firewall rules by Provide social engineering and phishing training to employees.
- Limit unnecessary lateral communications between network hoses, segments, and devices by Segment and segregate networks and functions.
- Consider using application allow listing technology on all assets to ensure that only authorized software executes, and all unauthorized software is blocked from executing on assets.
- Implement an Intrusion Detection System to detect Command and Control activity and other potentially malicious network activity.

d) AppleJeus Malware (AA21-048A)

First Seen : August 2018

Release Date : 17 February 2021

Sector Target : Individuals and companies, including cryptocurrency exchanges and financial service companies.

Overview : used websites that appeared to host legitimate cryptocurrency trading platforms to infect victims with AppleJeus and also using other initial infection vectors such as phishing, social networking, and social engineering techniques to get users to download the malware through the dissemination of cryptocurrency trading applications that have been modified to include malware that facilitates theft of cryptocurrency.

Mitigation :

- Verify source of cryptocurrency-related applications.
- Use multiple wallets for key storage, striking the appropriate risk balance between hot and cold storage and Use custodial accounts with multi-factor authentication mechanisms for both user and device verification.
- Patronize cryptocurrency service businesses that offer indemnity protections for lost or stolen cryptocurrency and Consider having a dedicated device for cryptocurrency management.
- Install antivirus software to run daily deep scans of the host and Ensure your anti-virus software is setup to download the latest signatures daily.
- Ensure all software and hardware is up to date, and all patches have been installed and Ensure network-based firewall is installed and/or up to date also Ensure the firewall’s firmware is up to date.
- Install a Host Based Intrusion Detection (HIDS) based software and keep it up to date.
- Introduce two-factor authentication solution as an extra layer of verification and Use hardware wallets, which keep the private keys in a separate, secured storage area.
- Initiate and always update organization’s Incident Response Plan (IRP) by Assume malware have moved laterally within the organization network.

e) LokiBot Malware (AA20-266A)

First Seen : February 2016

Release Date : 22 September 2020

Sector Target : Individuals and companies including federal organizations.

Overview : Steal sensitive information such as usernames, passwords, cryptocurrency wallets, and other credentials through the use of a keylogger to monitor browser and desktop activity and can create a backdoor into infected systems to allow an attacker to install additional payloads or via email, malicious websites, text, and other private messages.

Mitigation :

- Implement a user training program to discourage users from visiting malicious websites or opening malicious attachments.
- Filter network traffic to prohibit ingress and egress communications with known malicious IP addresses and implement a URL blocklist to prevent users from accessing malicious websites.
- Enable strong spam filters containing executable files to prevent to prevent phishing emails and attachment from reaching end users.
- Ensure all software and hardware is up to date, and all patches have been installed and Ensure network-based firewall is installed and/or up to date also Ensure the firewall’s firmware is up to date.
- Implement endpoint and detection response tools to allow a high degree of visibility into the security status of endpoints and can help effectively protect against malicious cyber actors.
- Implement time-based access for accounts set at the admin level and higher and disable command-line and scripting activities and permissions.
- Implement Network Segmentation to help prevent the spread of ransomware by controlling traffic flows "between and access to" various subnetworks and by restricting adversary lateral movement and Traversal Monitoring such as Endpoint detection and response (EDR) tools for detecting lateral connections into common and uncommon network connections for each host.

f) Emotet Malware (AA20-280A)

First Seen : April 2015

Release Date : 6 October 2020

Sector Target : State and local governments including banking organization.

Overview : Spread via phishing email attachments and links that, once clicked, launch the payload then attempts to proliferate within a network by brute forcing user credentials and writing to shared drives and difficult to combat because of its “worm-like” features that enable network-wide infections that uses modular Dynamic Link Libraries to continuously evolve and update its capabilities.

Mitigation :

- Block email attachments commonly associated with malware and Block email attachments that cannot be scanned by antivirus software.
- Implement Group Policy Object and firewall rules and Implement an antivirus program and a formalized patch management process.
- Implement filters at the email gateway and block suspicious IP addresses at the firewall.
- Implement a Domain-Based Message Authentication, Reporting & Conformance validation system by Segment and segregate networks and functions.
- Exercise caution when opening email attachments, even if the attachment is expected and the sender appears to be known.
- Enable a firewall on agency workstations, configured to deny unsolicited connection requests and Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious email attachments; ensure the scanned attachment is its "true file type".
- Scan all software downloaded from the internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate access control lists.

g) Dridex Malware (AA19-339A)

First Seen : October 2015

Release Date : 5 December 2019

Sector Target : Financial services sector including financial institutions and customers, the techniques, tactics, and procedures.

Overview : Once downloaded and active, can infiltrate browsers, detect access to online banking applications and websites, and inject malware or keylogging software, via API hooking, to steal customer login information. After stealing the login data, the attackers have the potential to wire transfers, open fraudulent accounts, and potentially adapt victim accounts for other scams involving business e-mail compromise or money mule activity.

Mitigation :

- Inform and educate employees on the appearance of phishing messages, especially those used by the hackers for distribution of malware in the past.
- Update intrusion detection and prevention systems frequently to ensure the latest variants of malware and downloaders are included.
- Conduct regular backup of data, ensuring backups are protected from potential ransomware attack.
- Maintain up-to-date antivirus signatures and engines and Keep operating system patches up-to-date.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrator's group unless required.
- Scan for and remove suspicious email attachments; ensure the scanned attachment is its "true file type"

REFERENCES :

https://us-cert.cisa.gov/ncas/alerts

https://malpedia.caad.fkie.fraunhofer.de/

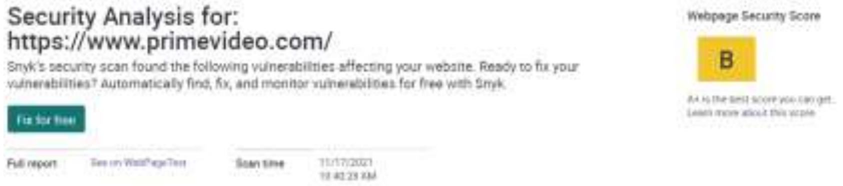
3. **[25 point]** Sila anda pilih salah satu online tool untuk men-scan kerentanan / celah keamanan sebuah website perusahaan! Pilih juga satu website yang akan anda scan dan lakukanlah proses scan tersebut! Buatlah laporan saintifik berkenaan hasil scan kerentanan keamanan dan jenis respon yang harus perusahaan lakukan dari hasil scan web yang telah anda lakukan tersebut! (ingat, perintah soal ini hanya digunakan untuk kebutuhan pembelajaran dan bersifat akademis, tidak untuk disebar luaskan).

Answer:

Online Website Vulnerability Scanner Tools Choice : https://snyk.io/website-scanner/

Website to be Scanned : https://www.primevideo.com/

Scientific Report:



Security Analysis for:
https://www.primevideo.com/

Snyk's security scan found the following vulnerabilities affecting your website. Ready to fix your vulnerabilities? Automatically find, fix, and monitor vulnerabilities for free with Snyk.

Full report See on WebPageTest
Scan time 11/17/2021 10:40:23 AM

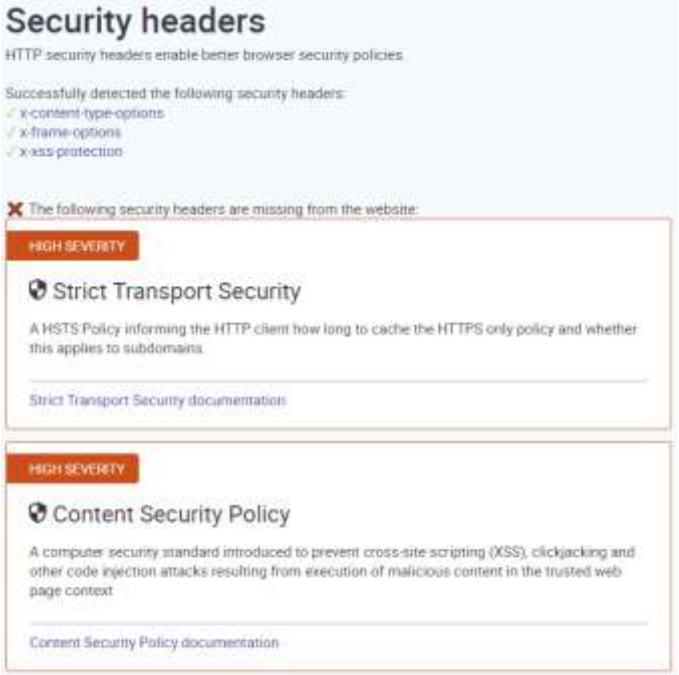
Webpage Security Score

B

A+ is the best score you can get.
Learn more about this score

Security scores are based on two core metrics:

1) Vulnerable versions of JavaScript libraries which were detected on the page and pose a potential security threat.
2) Security headers, in which checking which HTTP security headers have been set for the website, and those which are missing but recommended to turn on.



Security headers

HTTP security headers enable better browser security policies

Successfully detected the following security headers:
✓ x-content-type-options
✓ x-frame-options
✓ x-xss-protection

✗ The following security headers are missing from the website:

HIGH SEVERITY

Strict Transport Security

A HSTS Policy informing the HTTP client how long to cache the HTTPS only policy and whether this applies to subdomains

Strict Transport Security documentation

HIGH SEVERITY

Content Security Policy

A computer security standard introduced to prevent cross-site scripting (XSS), clickjacking and other code injection attacks resulting from execution of malicious content in the trusted web page context

Content Security Policy documentation

Security headers are based on five core metrics:

a) x-content-type-options

The X-Content-Type-Options response HTTP header is a marker used by the server to block content sniffing that was happening and could transform non-executable MIME types into executable MIME types.

b) x-frame-options

The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page to avoid click-jacking attacks, by ensuring that their content is not embedded into other sites.

c) x-xss-protection

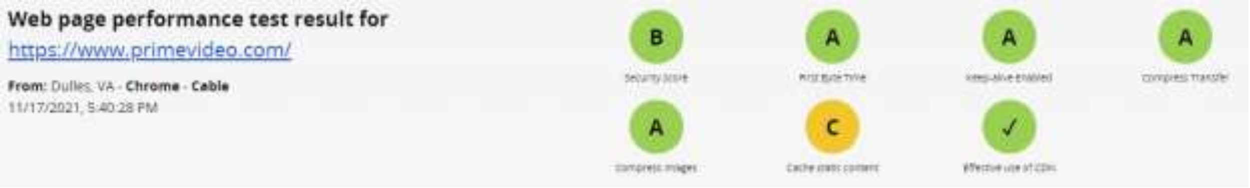
The HTTP X-XSS-Protection response header is a feature to stops pages from loading when they detect reflected cross-site scripting (XSS) attacks.

d) Strict Transport Security

The HTTP Strict-Transport-Security response header is a feature to tell browsers that it should only be accessed using HTTPS, instead of using HTTP.

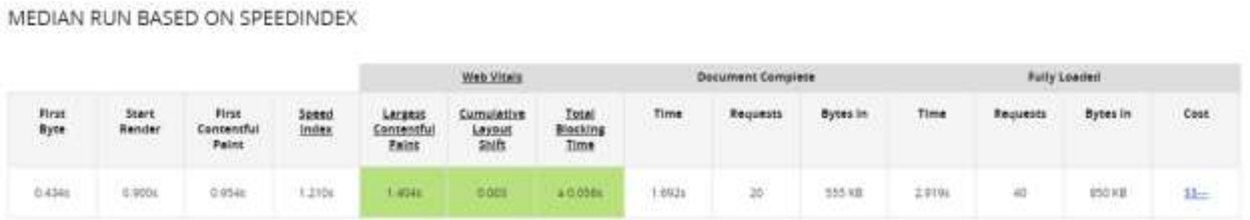
e) Content Security Policy

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross-Site Scripting (XSS) and data injection attacks.



Web page performance test result for
https://www.primevideo.com/

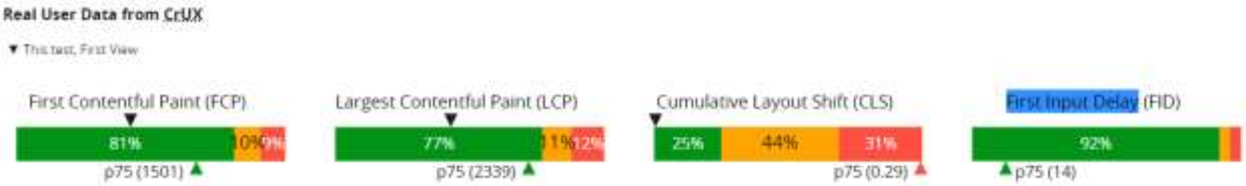
From: Dulles, VA - **Chrome** - **Cable**
11/17/2021, 5:40:28 PM



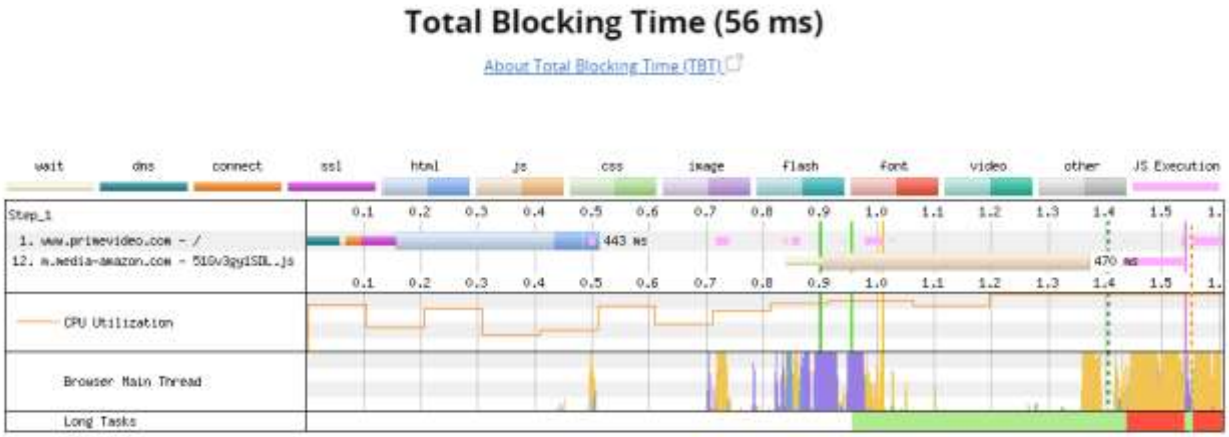
MEDIAN RUN BASED ON SPEEDINDEX

				Web Vitals			Document Complete			Fully Loaded			
First Byte	Start Render	First Contentful Paint	Speed Index	Largest Contentful Paint	Cumulative Layout Shift	Total Blocking Time	Time	Requests	Bytes In	Time	Requests	Bytes In	Cost
0.434s	0.900s	0.954s	1.210s	1.404s	0.003	≥ 0.036s	1.692s	20	555 KB	2.919s	40	850 KB	$$---

Speed Index measures how quickly content is visually displayed during page load by captures a video of the page loading in the browser and computes the visual progression between frames.

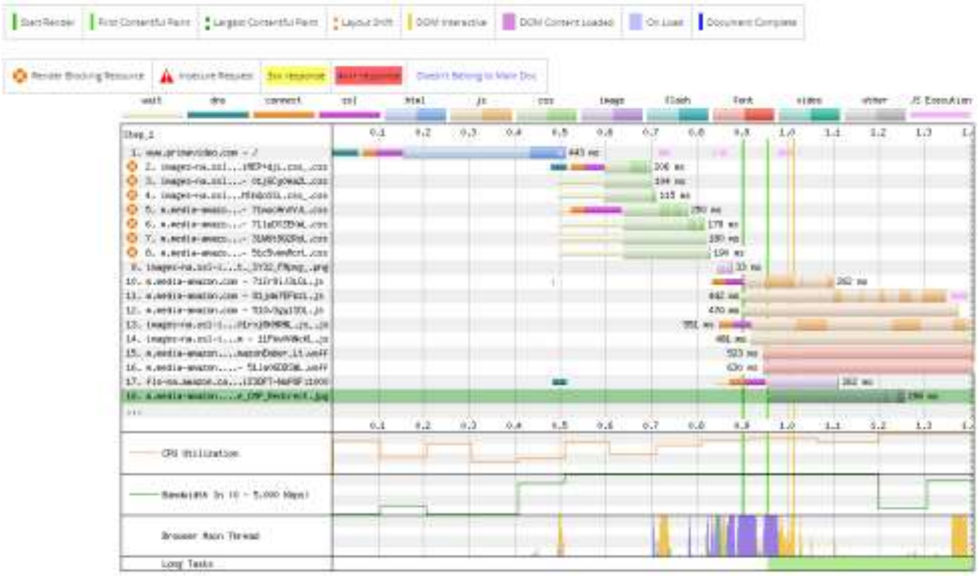


a) **First Contentful Paint (FCP)** is when the browser renders the first bit of content from the Document Object Model such as text, image and providing the first feedback to the user that the page is actually loading.



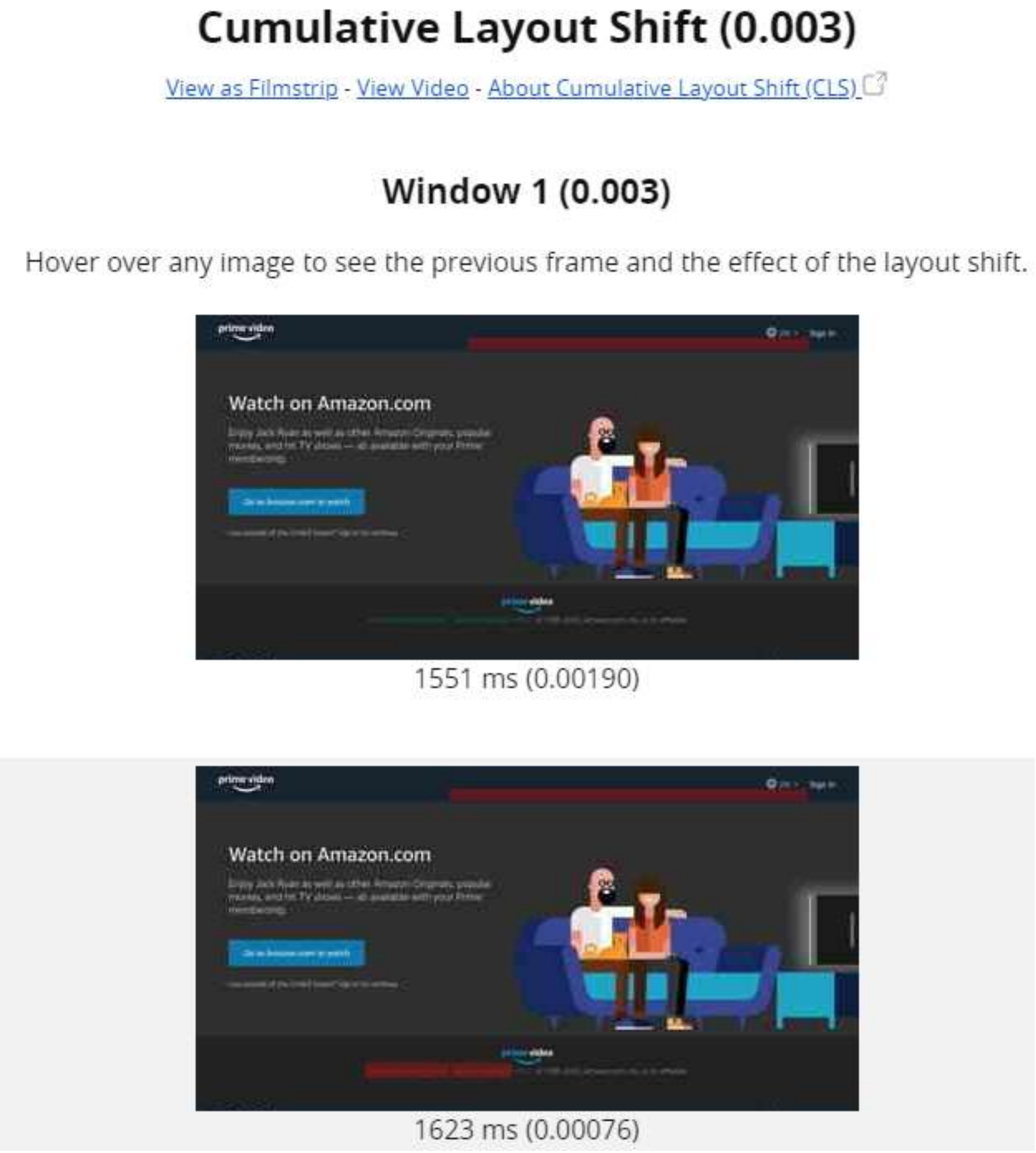
The Total Blocking Time (TBT) metric measures the total amount of time between First Contentful Paint (FCP) and Time to Interactive (TTI) where the main thread was blocked for long enough to prevent input responsiveness.

b) **Largest Contentful Paint (LCP)** provides details about the largest image or text paint before user input on a web page.



NAME : Edward Course : IT Risk Management and Disaster Recovery
NIM : 2201741971 Course Code : COMP8040
CLASS : LTY1 Faculty / Department : Binus Graduate Program / Master Track

Cumulative Layout Shift (CLS) is a performance metric to measure the perceived visual stability of a page load.



Cumulative Layout Shift (0.003)

View as Filmstrip - View Video - About Cumulative Layout Shift (CLS)

Window 1 (0.003)

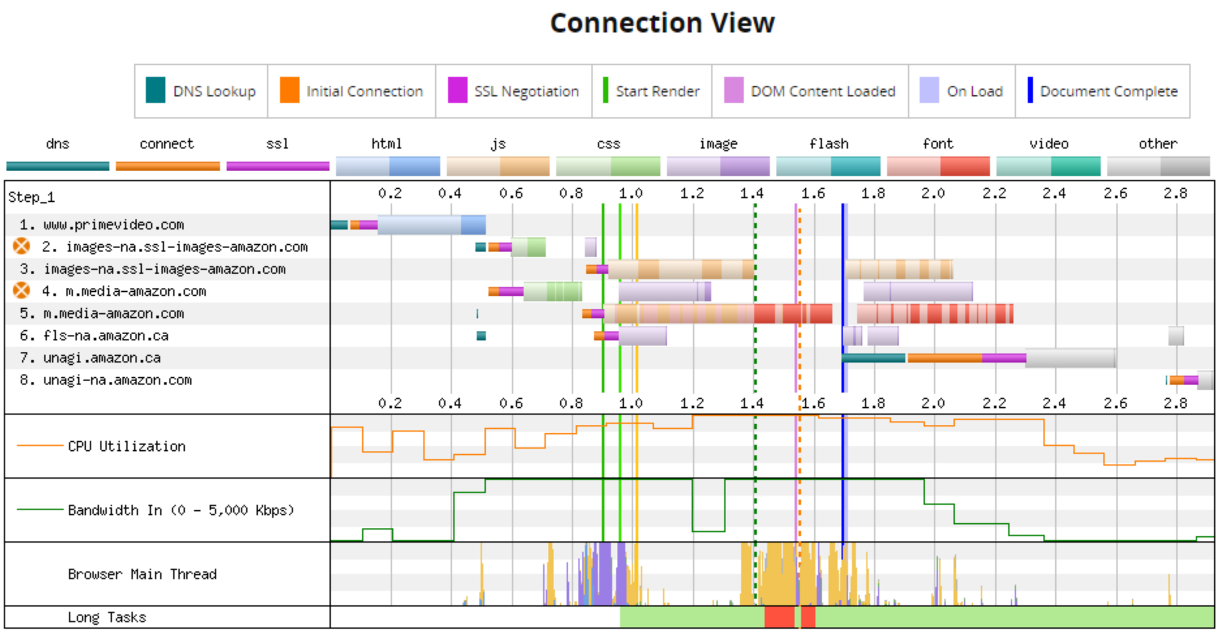
Hover over any image to see the previous frame and the effect of the layout shift.

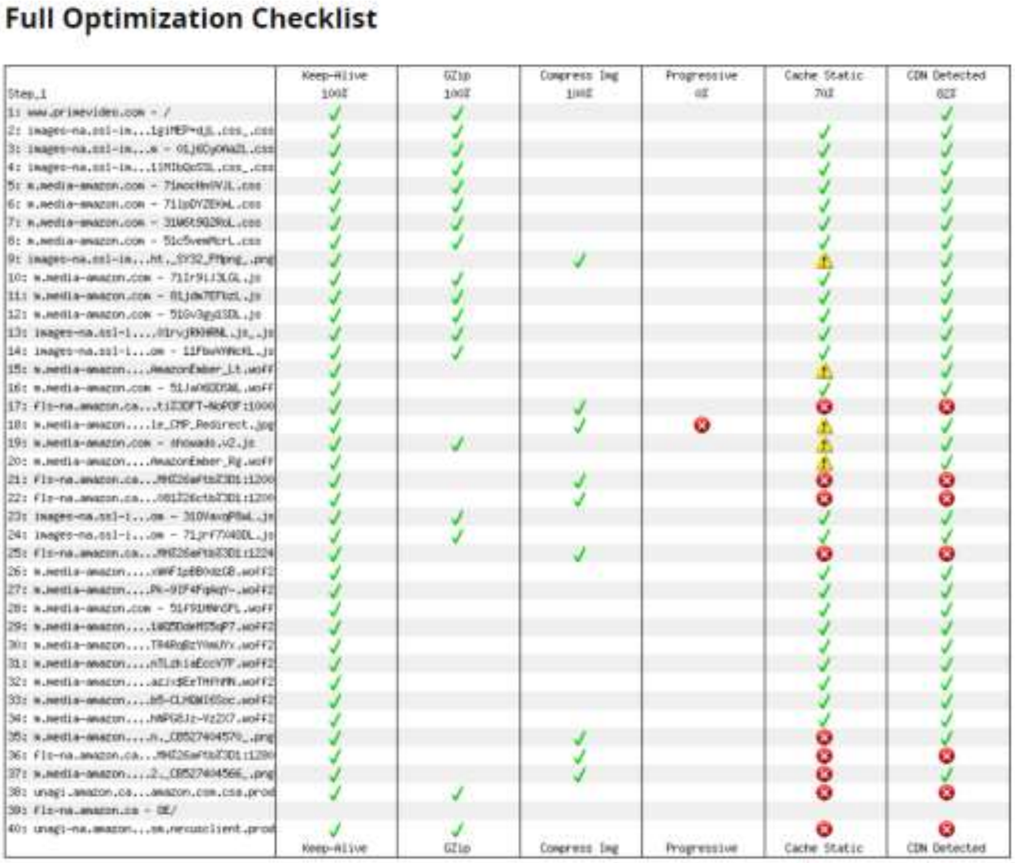
1551 ms (0.00190)

1623 ms (0.00076)

NAME : Edward Course : IT Risk Management and Disaster Recovery
NIM : 2201741971 Course Code : COMP8040
CLASS : LTY1 Faculty / Department : Binus Graduate Program / Master Track

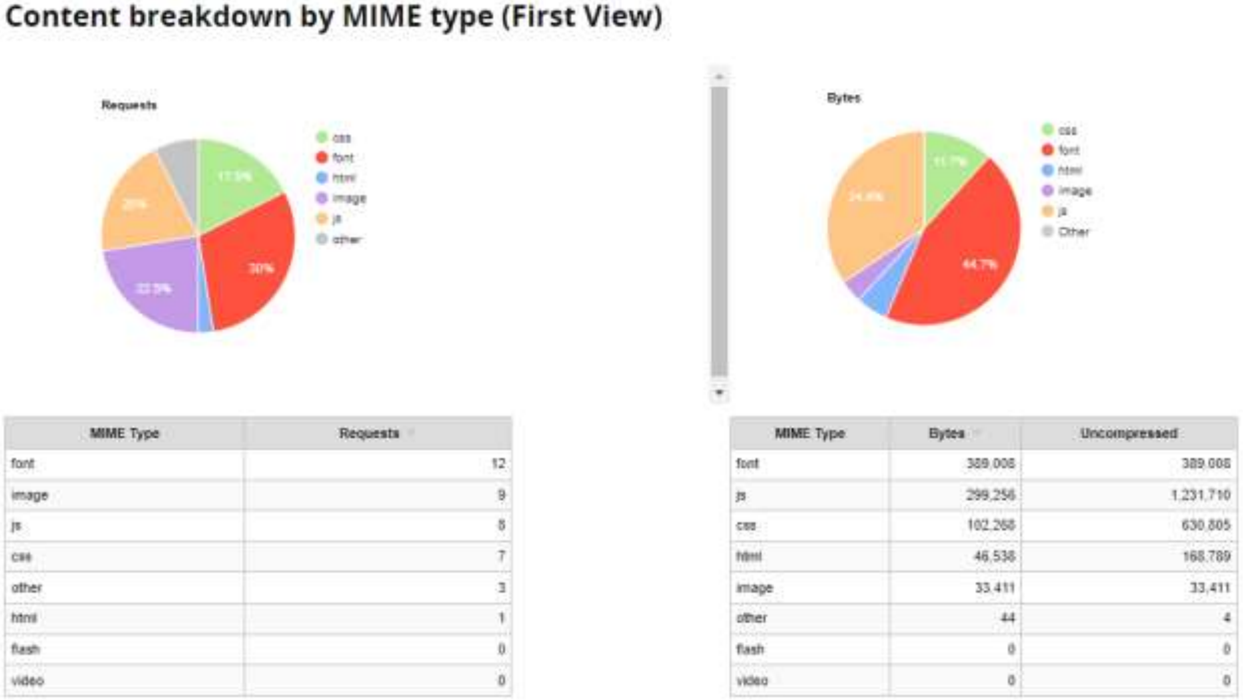
First input delay (FID) measures the time from when a user first interacts with site such as click a link, tap on a button to the time when the browser is actually able to respond to that interaction.





Full Optimization Checklist

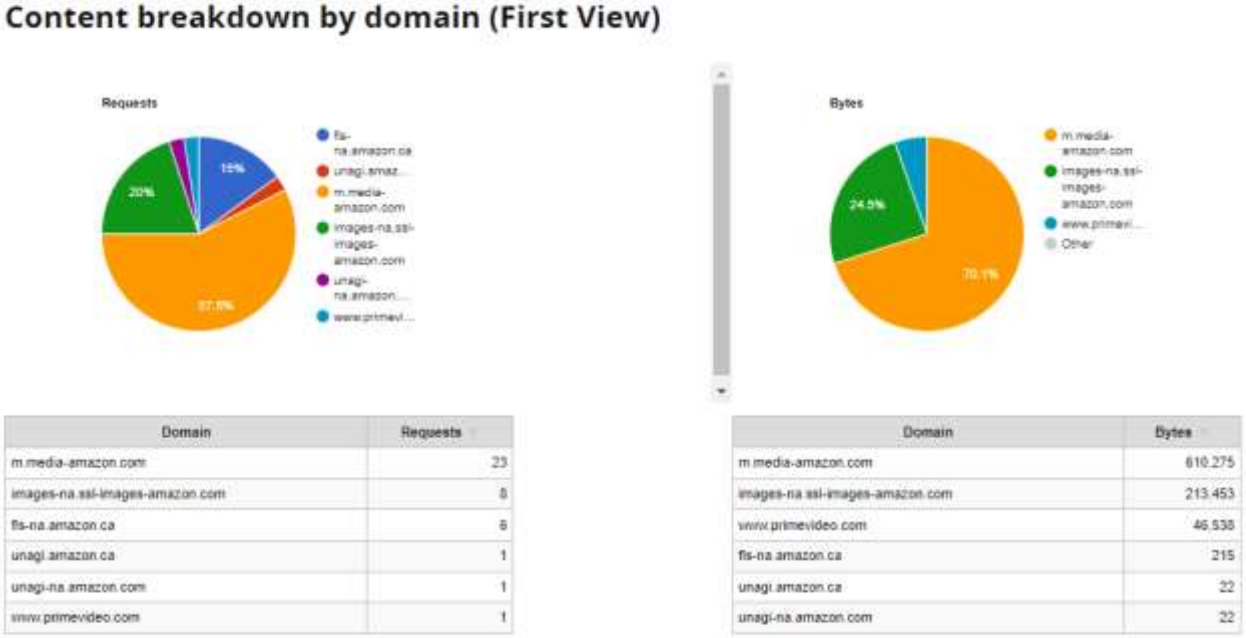
Step_1	Keep-Alive 100%	GZip 100%	Compress Img 100%	Progressive 0%	Cache Static 70%	CDN Detected 82%
1: www.primevideo.com - /	✓	✓				✓
2: images-na.ssl-im...1giMEP+dJL.css_.css	✓	✓			✓	✓
3: images-na.ssl-im...m - 01j6CyOWa2L.css	✓	✓			✓	✓
4: images-na.ssl-im...11MIbQoS5L.css_.css	✓	✓			✓	✓
5: m.media-amazon.com - 71mocHnVJL.css	✓	✓			✓	✓
6: m.media-amazon.com - 71lpDYZEKbL.css	✓	✓			✓	✓
7: m.media-amazon.com - 31W6t9Q2RoL.css	✓	✓			✓	✓
8: m.media-amazon.com - 51c5vemMcrL.css	✓	✓			✓	✓
9: images-na.ssl-im...ht._SY32_FMpng_.png	✓		✓		⚠	✓
10: m.media-amazon.com - 71Ir9LiJ3LGL.js	✓	✓			✓	✓
11: m.media-amazon.com - 81jdw7EFkzL.js	✓	✓			✓	✓
12: m.media-amazon.com - 51Gv3gyd3DL.js	✓	✓			✓	✓
13: images-na.ssl-i....81rvjRKHRNL.js_.js	✓	✓			✓	✓
14: images-na.ssl-i...om - 11FbwVYWcKL.js	✓	✓			✓	✓
15: m.media-amazon....AmazonEmber_Lt.woff	✓				⚠	✓
16: m.media-amazon.com - 51JaX6DD5NL.woff	✓				✓	✓
17: fls-na.amazon.ca...t1Z3DFT-NoPOF:1000	✓		✓		☒	☒
18: m.media-amazon....le_CMP_Redirect.jpg	✓		✓	☒	⚠	✓
19: m.media-amazon.com - showads.v2.js	✓	✓			⚠	✓
20: m.media-amazon....AmazonEmber_Rg.woff	✓				⚠	✓
21: fls-na.amazon.ca...MHI26aFtbZ3D1:1200	✓		✓		☒	☒
22: fls-na.amazon.ca...081I26ctbZ3D1:1200	✓		✓		☒	☒
23: images-na.ssl-i...om - 310VavqP8wL.js	✓	✓			✓	✓
24: images-na.ssl-i...om - 71jrF7X40DL.js	✓	✓			✓	✓
25: fls-na.amazon.ca...MHI26aFtbZ3D1:1224	✓		✓		☒	☒
26: m.media-amazon....xWAF1pBBOdzG8.woff2	✓				✓	✓
27: m.media-amazon....Pk-9IF4FqAqY-.woff2	✓				✓	✓
28: m.media-amazon.com - 51F91MNnGFL.woff	✓				✓	✓
29: m.media-amazon....1WZBDdeMS5qP7.woff2	✓				✓	✓
30: m.media-amazon....T4ARqBzYWmUYx.woff2	✓				✓	✓
31: m.media-amazon....nTLzkiaEccV7F.woff2	✓				✓	✓
32: m.media-amazon....aCi:$EzTHFhMN.woff2	✓				✓	✓
33: m.media-amazon....b5-CLMDWI6Soc.woff2	✓				✓	✓
34: m.media-amazon....hWPG8Jz-Vz2X7.woff2	✓				✓	✓
35: m.media-amazon....n._CB527404570_.png	✓		✓		☒	✓
36: fls-na.amazon.ca...MHI26aFtbZ3D1:1200	✓		✓		☒	☒
37: m.media-amazon....2._CB527404566_.png	✓		✓		☒	✓
38: unagi.amazon.ca...amazon.com.csa.prod	✓	✓			☒	☒
39: fls-na.amazon.ca - OE/						
40: unagi-na.amazon....sm.nexusclient.prod	✓	✓			☒	☒
	Keep-Alive	GZip	Compress Img	Progressive	Cache Static	CDN Detected



Content breakdown by MIME type (First View)

MIME Type	Requests
font	12
image	9
js	8
css	7
other	3
html	1
flash	0
video	0

MIME Type	Bytes	Uncompressed
font	389,008	389,008
js	299,256	1,231,710
css	102,268	630,805
html	46,538	168,789
image	33,411	33,411
other	44	4
flash	0	0
video	0	0

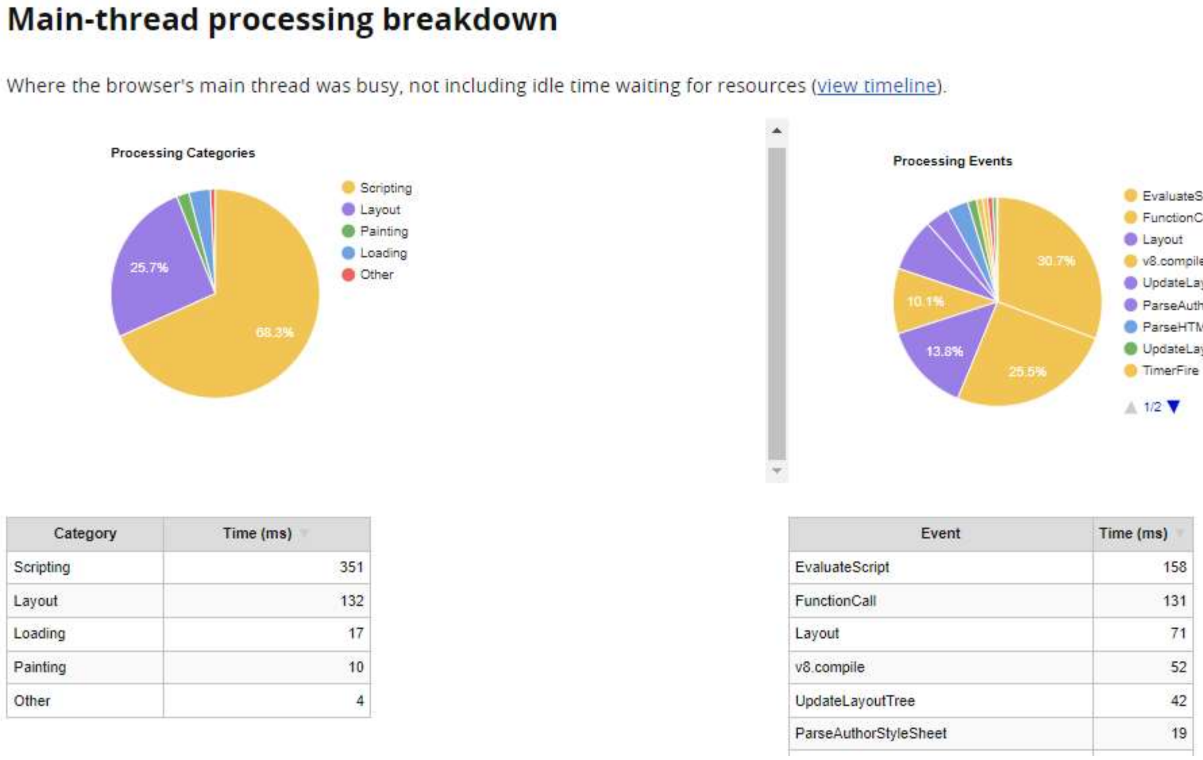


Content breakdown by domain (First View)

Domain	Requests
m.media-amazon.com	23
images-na.ssl-images-amazon.com	8
fls-na.amazon.ca	6
unagi.amazon.ca	1
unagi-na.amazon.com	1
www.primevideo.com	1

Domain	Bytes
m.media-amazon.com	610,275
images-na.ssl-images-amazon.com	213,453
www.primevideo.com	46,538
fls-na.amazon.ca	215
unagi.amazon.ca	22
unagi-na.amazon.com	22

NAME : Edward Course : IT Risk Management and Disaster Recovery
NIM : 2201741971 Course Code : COMP8040
CLASS : LTY1 Faculty / Department : Binus Graduate Program / Master Track

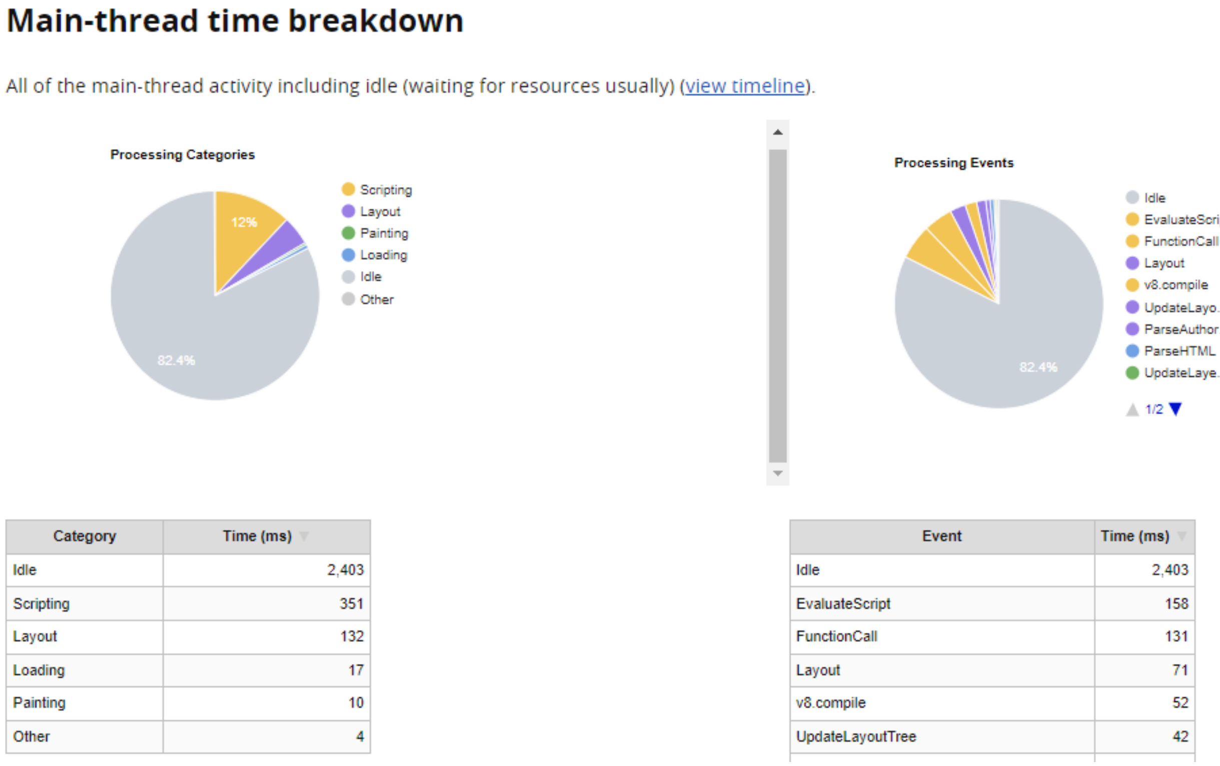


Main-thread processing breakdown

Where the browser's main thread was busy, not including idle time waiting for resources (view timeline).

Category	Time (ms)
Scripting	351
Layout	132
Loading	17
Painting	10
Other	4

Event	Time (ms)
EvaluateScript	158
FunctionCall	131
Layout	71
v8.compile	52
UpdateLayoutTree	42
ParseAuthorStyleSheet	19

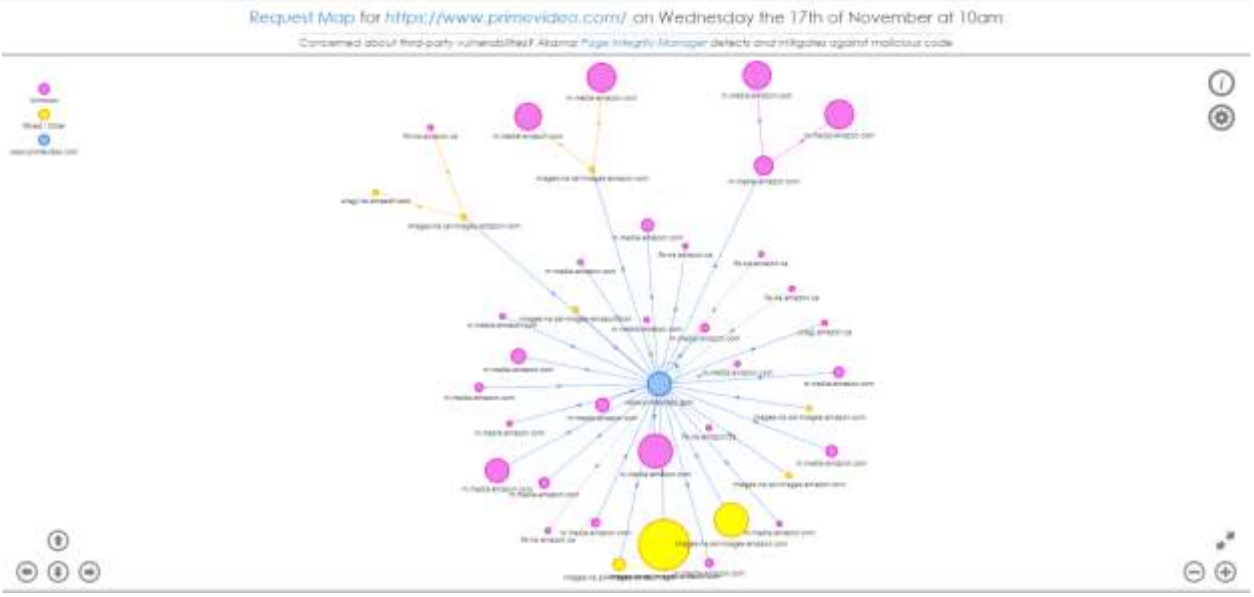


Main-thread time breakdown

All of the main-thread activity including idle (waiting for resources usually) (view timeline).

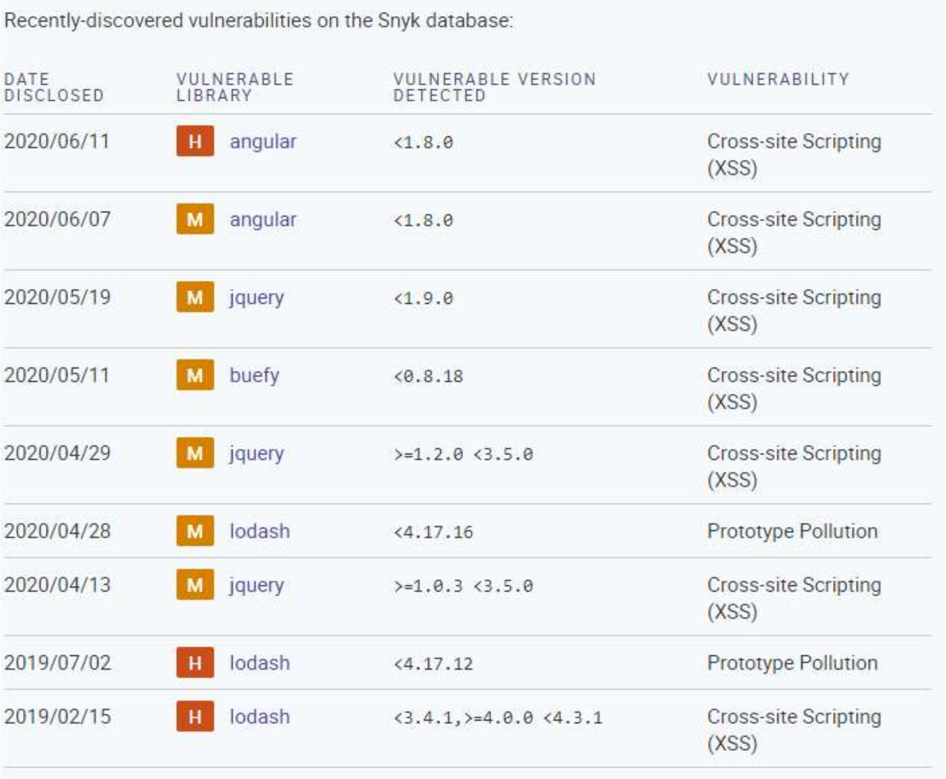
Category	Time (ms)
Idle	2,403
Scripting	351
Layout	132
Loading	17
Painting	10
Other	4

Event	Time (ms)
Idle	2,403
EvaluateScript	158
FunctionCall	131
Layout	71
v8.compile	52
UpdateLayoutTree	42



Request Map for https://www.primevideo.com/ on Wednesday the 17th of November at 10am

Concerned about third-party vulnerabilities? Akamai Page Integrity Manager detects and mitigates against malicious code



Recently-discovered vulnerabilities on the Snyk database:

DATE DISCLOSED	VULNERABLE LIBRARY	VULNERABLE VERSION DETECTED	VULNERABILITY
2020/06/11	H angular	<1.8.0	Cross-site Scripting (XSS)
2020/06/07	M angular	<1.8.0	Cross-site Scripting (XSS)
2020/05/19	M jquery	<1.9.0	Cross-site Scripting (XSS)
2020/05/11	M buefy	<0.8.18	Cross-site Scripting (XSS)
2020/04/29	M jquery	>=1.2.0 <3.5.0	Cross-site Scripting (XSS)
2020/04/28	M lodash	<4.17.16	Prototype Pollution
2020/04/13	M jquery	>=1.0.3 <3.5.0	Cross-site Scripting (XSS)
2019/07/02	H lodash	<4.17.12	Prototype Pollution
2019/02/15	H lodash	<3.4.1,>=4.0.0 <4.3.1	Cross-site Scripting (XSS)

REFERENCES :

https://snyk.io/website-scanner/

https://developer.mozilla.org/en-US/docs/Web

NAME	**: Edward**	**Course**	**: IT Risk Management and Disaster Recovery**
NIM	**: 2201741971**	**Course Code**	**: COMP8040**
CLASS	**: LTY1**	**Faculty / Department**	**: Binus Graduate Program / Master Track**

4. **[10 point]** Di dalam menyusun ***Incident Response (IR) Planning*** perlu dilakukan *testing* pada *Contingency Plan* yang sudah disusun. Berikan usulan strategi testing yang bisa digunakan untuk melakukan testing *IR Planning* yang akan diterapkan pada badan pemerintahan sebagai contoh di Indonesia. Jelaskan dengan singkat usulan Anda dan disertai alasan yang mendukung !

Answer:

Incident Response management is vital in order to make sure business continuity and the overall productivity of an organization. There are various approaches to incident Response management. Information security risks are inevitable, hence it's an economical solution to implement an event management process for an organization to identify issues and take suitable steps to handle the problems systematically.

Different approaches have various limitations. At an equivalent time, organizational goals and objectives also are different, to various extents. **Organizations therefore require a customized framework**. The following proposed framework may be a flexible one that provides control to an organization to enable customization also as a guided procedure to ensure that different aspects of incident Response management should be taken care of during the process.

The team is additionally a crucial aspect of incident management. It helps in distributing the roles and responsibilities. A structured team with well-defined roles can help in ensuring continuous monitoring for alerts and saving time during incident handling. So, it improves the general productivity time for an organization and increases process efficiency.

An incident that hits an organizational information security infrastructure have a strong impact on the company's customers, suppliers, and other stakeholders. Unavailability of services provided, and downtime may cause the in loss of revenue. This results of each alert from the incident management process investigation which is carried out by the organization to keep it under control.

A dedicated incident management tool is required to track the lifecycle of an incident from receiving an alert to closure. A monitoring system should help in generating alerts from all tools used in the incident management process. It should also help in tracking information such as source and destination IP addresses, event time, system logs, event status and tracking details of the actions taken.

This system also documents the challenges faced, possible counter measures results of root cause analysis, and so on. On successful closure of a ticket for an incident alert by an incident response team it also saves details such as logs, and pieces of evidence used in the process. These details help in preventing similar incidents in the future too.

REFERENCES :

Whitman, M.E., Mattoro, H.J. (2013). Principles of Incident Response and Disaster Recovery.

5. **[10 point]** Ada dua pendekatan dalam *Incident Response (IR) Strategy* yaitu pertama adalah *Protect and Forget*, dan kedua adalah *Apprehend and Prosecute*. Jika ada yang menggunakan **malware** untuk melakukan serangan pada perusahaan kompetitornya, manakah pendekatan yang Anda usulkan untuk menentukan *IR Strategy* ? Jelaskan pendapat Anda dengan singkat !

Answer:

Once the incident is reported it is now the decision of upper management that how it should be handled and investigated, it depends on the nature of the incident. Between the two philosophies of the incident response that is protect and forget, and apprehend and prosecute **(Eoghan Casey,2004)**.

I would recommend Protect and Forget Strategy because in it the focus is mainly on the defense of the data to secure it. For this **first we have to determine if event is a real incident or not as this is the most important and vital step in Incident handling**. It should be identified first that either it is a system configuration error or a user error. If so than **we have to terminate the present intrusion** if it is indeed the incident as this is the important and key part of this strategy **because we have to immediately stop the damage to the system and information further**.

Next is to discover how access was obtained and the way many systems were compromised, how the person gained access to the information and data and where they went when they had access. Restore compromised systems back to the pre-incident configuration, for this backup needs to be redone as all the information may be lost. Secure the tactic of unauthorized access by the intruder on all systems. Document steps taken to affect the incident. Develop lessons learned. Brief upper management on the after math of the incident.

REFERENCES :

Eoghan Casey. Digital Evidence and Computer Crime - 2nd Edition. Academic Press, 2004.

6. **[10 point]** Ada beberapa cara untuk melakukan pendeteksian terkait *data hiding software*, yaitu *Data Hiding Software Application*, *Cached Website Pages*, *dan Cached image indicate*. Lakukan **evaluasi** dengan menggunakan ketiga cara tersebut kemudian tentukan manakah cara yang lebih sesuai untuk melakukan pendeteksian pada *personal computer* atau laptop yang digunakan untuk keperluan pribadi. Jelaskan pendapat Anda disertai alasan!

Answer:

a) Data Hiding Software Application

On the suspect computer data hiding software applications may still exist may indicate the suspect to access the web pages that provide the data hiding software **(Carvin, Andy, 2001)**.

Scanning the data for data hiding software the scanner or the investigator can identify the website, there are number of freeways and commercial tools for viewing.

b) Cached Website Pages

When a user visits an internet site, the browser typically downloads the source and images from that website to the local drive and stores them during a cache file or Temporary Internet Files directory.

The browser stores this information to enable quick access subsequent time the user visits the web site, forming a history of the sites a user has visited. Temporary Internet Files and cache files are often cleared through common methods within the browser **(Carvin, Andy, 2001)**.

For instance, you'll clear the Temporary Internet Files in Internet Explorer by selecting Tools > Internet Options > Delete Files. Both online and offline files must be deleted.

c) Cached Image Indicate

Cache images may indicate the accessed of the suspect and downloading potentially Remaining artifacts indicate that the data used by the system **(Carvin, Andy, 2001)**.

We can view will allow the current and previous images and build an audit trail of pictures, videos, power point presentations, etc. that once resided on the system.

In my opinion Cached Website Pages is more suitable for detecting a personal computer or laptop that is used for personal purposes because instantly we can find the latest data on the cached pages and is easier to access.

REFERENCES :

Carvin, Andy. "When a Picture Is Worth a Thousand Secrets: The Debate Over Online Steganography" The Digital Beat. 2001

NAME	**: Edward**	**Course**	**: IT Risk Management and Disaster Recovery**
NIM	**: 2201741971**	**Course Code**	**: COMP8040**
CLASS	**: LTY1**	**Faculty / Department**	**: Binus Graduate Program / Master Track**

Case

Bapak Ananda memiliki sebuah Start-up yang bergerak di bidang e-commerce. Kantor yang dimiliki Pak Ananda sangat ramah lingkungan dan berada di tepi pantai yang biru. Memang lokasi kantor yang diinginkan Pak Ananda yang dekat dengan alam bukan di daerah perkotaan. Dengan demikian Pak Ananda beserta timnya dapat bekerja dengan baik dengan lingkungan yang nyaman. Namun dengan kondisi lingkungan di tepi pantai ada kemungkinan sewaktu-waktu terjadi bencana alam seperti tsunami atau gempa bumi. Tentunya Pak Ananda perlu menyusun rencana untuk menghadapi kemungkinan bencana yang terjadi. Apalagi ketergantungan pada koneksi internet sangat tinggi dilihat dari karakteristik perusahaan Pak Ananda. Anda sebagai seorang professional di bidang IT Risk Management diminta bantuannya untuk membuat perencanaan *Disaster Recovery* (DR).

Adapun tugas yang perlu dilakukan dalam tahapan perencanaan *Disaster Recovery* ;

a. **[5 point]** Klasifikasikan tipe *Disaster* yang kemungkinan terjadi !

Answer:

The type of disaster that can happened is Geophysical disaster because potentially cause the death toll or injury, property harm, social and financial interruption, or natural debasement.

b. **[5 point]** Usulkan notifikasi yang perlu dilakukan pada bagian yang mendapat dampak dari bencana ini !

Answer:

- Download the Regional Emergency Alert application for basic life-saving alerts.
- Check for current weather and nature conditions.
- Discover where the local area will post data and updates during an emergency.

c. **[5 point]** Usulkan tindakan *recovery* yang perlu dilakukan khususnya pada bisnis proses yang kritikal !

Answer:

1) **Make a Disaster Recovery Team**

The team will be liable for creating, carrying out, and keeping up with the Disaster Recovery Plan (DRP). A DRP ought to recognize the team individuals, characterize every part's liabilities, and give their contact data by distinguish who ought to be reached in case of a disaster or crisis. All workers ought to be educated regarding and comprehend the DRP and obligation if a disaster happens.

2) **Distinguish and Survey Disaster Risks**

Disaster Recovery Team ought to distinguish and survey the risks to company. This progression ought to incorporate things identified with catastrophic events, man-made crises, and innovation related episodes. This will help the team in distinguishing the recovery procedures and assets needed to recuperate from disasters inside a foreordained.

d. **[5 point]** Dalam menyusun *Business Continuity Planning* , apakah perlu dilakukan relokasi pada alternatif lokasi lain terkait dampak dari bencana yang terjadi ? Jelaskan jawaban Anda dengan contoh !

Answer:

1) **Decide Basic Applications, Reports, and Assets.**

Company should assess its business cycles to figure out which are basic to the tasks of the company and should zero in on momentary survivability, **for example**, producing incomes, rather than on a drawn out arrangement of reestablishing the association's full working limit. In any case, the company should perceive that there are a few cycles that ought not be postponed if conceivable.

2) **Indicate reinforcement and off-site stockpiling methods.**

Distinguish what to uphold, by whom, how to play out the reinforcement, area of reinforcement and how every now and again reinforcements ought to happen. **For example**, checks the availability of server.