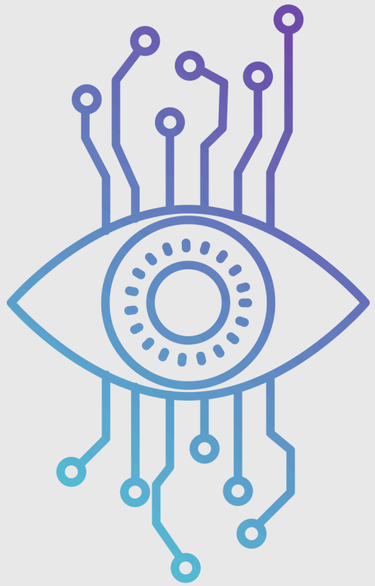
SECURITY MEASURES FOR THE E-COMMERCE APPLICATION



S9L5

COVI MICHELE

INDEX

01 INTRODUCTION

02 ANALYSIS OF WEB APPLICATION SECURITY

03 ECONOMIC IMPACT OF A DDOS ATTACK

04 RESPONSE TO A MALWARE INFECTION

05 BONUS

06 CONCLUSION

INTRODUCTION 01

This report was developed to provide a detailed and comprehensive analysis of vulnerabilities and threats affecting the examined e-commerce web application. Through the analysis of various attack scenarios - including SQL Injection, XSS, and DDoS attacks - and examination of real-world data from malware analysis platforms like Any.Run, this document aims to identify critical risk areas and propose preventive/corrective measures to strengthen application security.

The report specifically examines threat mitigation and response strategies, assessing potential attack impacts on business continuity and economics. Additionally, it discusses structural and strategic modifications to network infrastructure to improve overall resilience and security.

Finally, the report's bonus section provides a detailed analysis of specific documented attack reports detected via Any.Run, offering actionable insights for preventing and effectively responding to such threats in the future.

WEB APPLICATION SECURITY ANALYSIS

As our first task, we were asked: What preventive measures could be implemented to defend the web application from SQLi or XSS attacks by a malicious user?

Preventive Measures Against SQLi and XSS

1. Input Validation

We implement strict input validation for user-supplied data, placing "Input Validation" checks in the data flow between users and the DMZ server. This process verifies and sanitizes all entered data to prevent malicious code injection.

2. Database Access Controls

We deploy advanced access controls between the DMZ and internal network, represented by the "Database Access Control" icon. These include:

- Prepared statements and parameterized queries to neutralize SQLi attacks
- Least-privilege database access to limit potential damage

3. Content Security Policies (CSP)

We implement Content Security Policy (CSP) to restrict unauthorized external script execution, placing a CSP symbol in the data flow from application to users. These policies:

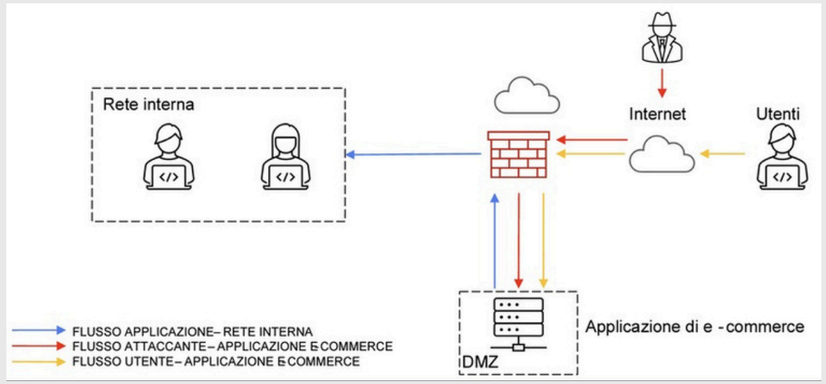
- Prevent XSS attacks
- Ensure only trusted content is executable/displayable

4.Web Application Firewall (WAF)

Strategically positioned at the Internet ingress point, our WAF serves as the first defense layer against external attacks. Key features:

- Configured to detect, inspect, and block suspicious/malicious requests
- Prevents unauthorized access to the DMZ and web application
- Optimized placement maximizes SQLi/XSS attack detection and blocking

BEFORE



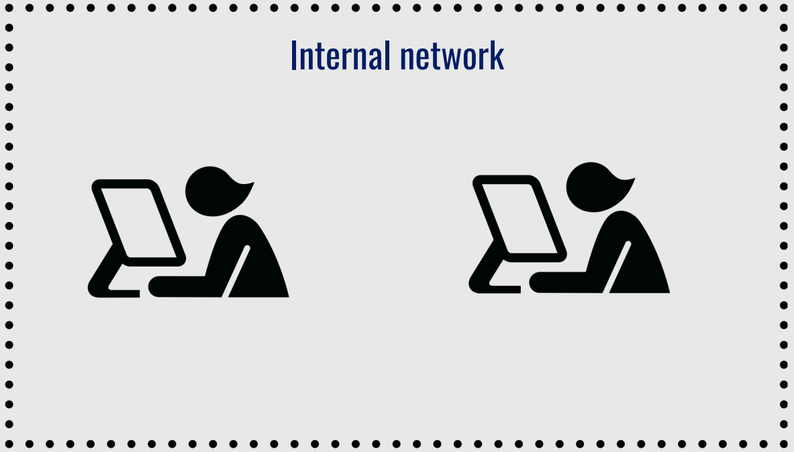
Database access control

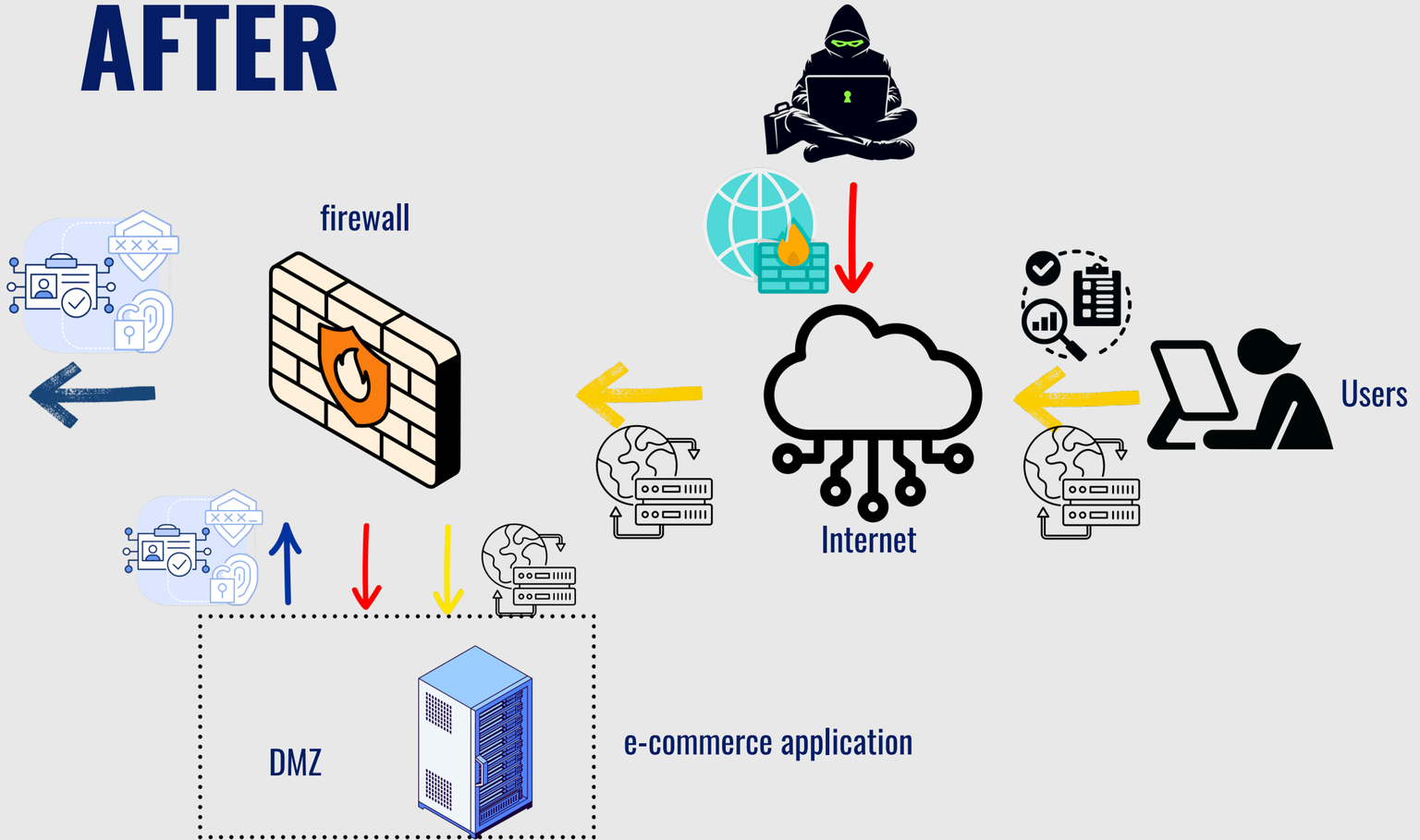
Validation Input

Content Security Policy

Web Application Firewall

AFTER





ECONOMIC IMPACT OF A DDOS ATTACK PT1

Second task: Business impacts – The web application suffers a DDoS attack, rendering the service unavailable for 10 minutes. Calculate the business impact due to service downtime, considering users spend an average of €1,500 per minute.
Exercise outline and requirements: External DDoS attack targeting the e-commerce platform. Include potential preventive measures for this scenario.

A Distributed Denial of Service (DDoS) attack is designed to make a web service inaccessible by overwhelming the server with traffic volume exceeding its capacity. This results in service disruption, preventing legitimate users from accessing the application (e.g., an e-commerce site). The economic impact can be severe, especially for businesses reliant on online availability for sales/services

Economic Loss Calculation:
Assuming €1,500 lost per minute of downtime:
Total Loss = Cost per Minute × Downtime Duration
Total Loss = €1,500/min × 10 min = €15,000

This calculation assumes:

- Complete site unavailability for all users during the attack
- Each minute of direct downtime translates to lost sales based on average revenue per minute during normal operation.

ECONOMIC IMPACT OF A DDoS ATTACK PT2

Preventive Measures Against DDoS Attacks

To defend against DDoS attacks and minimize their impact, organizations can implement the following technical and operational strategies:

1. Bandwidth Capacity Increase and Redundancy

Expanding available bandwidth helps absorb increased traffic volumes during DDoS attacks. Geographic redundancy of servers and network infrastructure ensures that even if one part is under attack, other components can maintain normal operations.

2. Load Balancing and Automated Failover

Load balancers distribute incoming traffic evenly across multiple servers, preventing single-server overload. During attacks, automated failover systems redirect traffic from affected devices/data centers to unaffected ones, maintaining service availability.

3. DDoS Mitigation Services

Partnering with specialized DDoS mitigation providers is critical. These services can:

- Detect abnormal traffic spikes in real-time
- Filter and block malicious traffic before it reaches corporate infrastructure

Implementing these measures reduces downtime risks and enhances overall network resilience against cyber threats.

MALWARE INFECTION RESPONSE

Third task: Response – The web application is infected with malware. Your priority is containing the malware from spreading across your network, while deliberately maintaining attacker access to the compromised machine. Modify the diagram in slide 2 with your proposed solution.

Malware Isolation Without Access Removal

Containment: The first step is restricting the malware's ability to communicate with external command-and-control (C&C) servers and propagate internally. Achieve this by:

- Implementing strict firewall rules blocking specific communication ports
- Blacklisting suspicious IP addresses associated with the malware

Traffic Monitoring: Deploy network monitoring systems including:

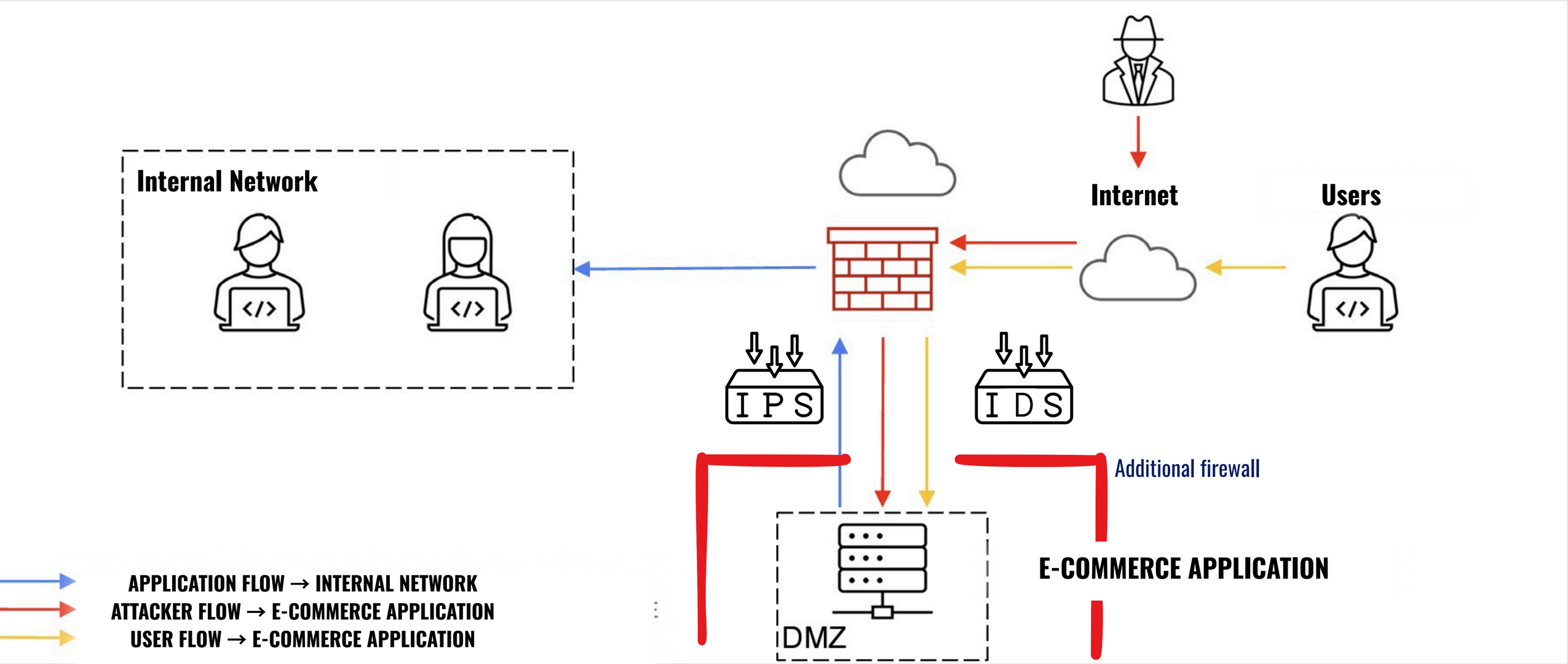
- IDS (Intrusion Detection Systems)
- IPS (Intrusion Prevention Systems)
- SIEM (Security Information and Event Management)
- To detect/log all suspicious activities originating from the infected host, aiding malware behavior analysis and identifying further spread attempts.

Controlled Access: If maintaining access to the infected machine is required (e.g., for business continuity or forensic investigations):

- Enforce multi-factor authentication (MFA)
- Implement strict access controls for authorized personnel
-

Updates & Patching: Ensure all systems – especially uncompromised ones – are fully updated with the latest security patches to prevent malware propagation through known vulnerabilities.

RESPONSE TO A MALWARE INFECTION (MODIFIED IMAGE)



BONUS

Bonus Task:

Analyze the following reports uploaded to Any.Run and prepare a brief summary of findings regarding the reported potential attack. Explain to both users and management:

1. The attack type
2. How to prevent similar attacks in the future

https://app.any.run/tasks/8e6ad6d9-4d54-48e8-ad95-bfb67d47f1d7/

https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e/

DETAILED REPORT OF THE FIRST LINK PT1

Performance_Booster_v3.6.exe

General Description

The file "Performance_Booster_v3.6.exe" has been identified as highly dangerous through detailed analyses conducted on security platforms like Any.Run and VirusTotal. While masquerading as a system optimization tool, analyses reveal it performs malicious activities that compromise computer system security.

Malicious Activities & Indicators of Compromise (IOCs)

1. Malicious Process:
   - Execution of "Performance_Booster_v3.6.exe" scores a risk rating of 100/100, confirming its highly malicious nature.
2. System File/Settings Modification:
   - Attempts to alter critical settings (registry files, PowerShell execution policies) to gain control and persistence on infected systems.

Abuse of System Tools for Unauthorized Changes

1. PowerShell Execution Policy Modifications:
   - Changes to PowerShell policies enable execution of unsigned scripts, increasing vulnerability to malicious script attacks.
2. ATTRIB.EXE Usage:
   - Uses the ATTRIB.EXE command to modify file attributes (e.g., hiding files or setting them to read-only) to evade detection.

DETAILED REPORT OF THE FIRST LINK PT2

Performance_Booster_v3.6.exe

Observed Specific Behaviors

1. Temporary Directory File Creation:
    - Creates files in temp directories (common malware tactic to execute malicious code and evade detection).
2. Registry Queries:
    - Searches system registry for:
        - Microsoft Outlook installation paths
        - Other software details (potential reconnaissance for attacks/spying)
3. Hosts File Manipulation:
    - Attempts to modify the hosts file (could redirect network traffic or block security websites).

Security Recommendations

- Proactive Security:
    - Install/update antivirus software
    - Deploy EDR (Endpoint Detection & Response) solutions for real-time monitoring
- Execution Restrictions:
    - Block unsigned PowerShell scripts
    - Prevent program execution from temp/suspicious locations
- User Training:
    - Educate users on:
        - Malware risks
        - Safe software download/installation practices
- Backup Protocols:
    - Implement robust backup/restore procedures to mitigate infection damage

DETAILED REPORT OF THE SECOND LINK PT1

Analysis of "Microsoft Edge" Download from Suspicious URLs

General Description

The analysis examined activities associated with downloading and installing Microsoft Edge from a URL exhibiting suspicious behavior. Security platforms Any.Run and VirusTotal identified multiple malicious activities linked to these processes, suggesting the use of deceptive or potentially harmful techniques.

Suspicious Activities & Indicators of Compromise (IOCs)

1. Malicious Executions:
    - Processes launched by "Iexplore.exe" and "MicrosoftEdgeSetup.exe" show a 100/100 risk score, indicating high danger potential.
2. Unauthorized File Modifications:
    - Attempts to execute files from temporary locations
    - Use of overwrite commands targeting legitimate content
    - (Potential indicators of malicious software installation)

DETAILED REPORT OF THE SECOND LINK PT2

Analysis of "Microsoft Edge" Download from Suspicious URLs

Observed Specific Behaviors

1. Download/Installation from Untrusted Sources:
   - Process initiates with a browser update prompt via a seemingly legitimate webpage, but the setup file's path/behavior raises authenticity concerns.
2. System Settings/Registry Manipulation:
   - Requests system settings access for installation (common in legitimate installs but suspicious in potentially compromised environments).
3. Suspicious Network Communication:
   - Network traffic analysis reveals multiple requests to domains potentially involved in:
     - Fake update distribution
     - Malware delivery

Security Recommendations

1. Source Verification:
   Download critical software (especially browsers) only from official/verified sources.
2. Execution Control:
   Restrict execution permissions for applications running from:
   - Temporary locations
   - Suspicious paths
3. Network Monitoring:
   Deploy advanced network monitoring solutions to:
   - Detect suspicious traffic
   - Block unauthorized communications
4. User Education:
   Train users on:
   - Risks of unverified download links
   - Best practices for software updates

CONCLUSION 06

This report details the strategies and implemented measures to enhance the e-commerce application's security, emphasizing the critical importance of a proactive approach to safeguarding online transactions and data. The graphical representation updates clearly illustrate adopted security measures, making protective barriers against internal and external threats immediately visible.

The newly deployed security implementations - including:

✓ Enhanced firewalls

✓ Intrusion prevention systems

✓ Stringent security policies

- are specifically designed to intercept and neutralize threats before they can negatively impact operations or user trust. These actions demonstrate our ongoing commitment to security and resilience, ensuring the application can withstand both common and sophisticated attacks.