

**Security Assessment   
US-Western-10**

**Confidential**

November 19, 2022

**This page is intentionally left blank**

**Table of Contents**

**1. Executive Summary PAGE**

1.1 Strategic Recommendations PAGE

**2. Engagement Overview** **PAGE**

2.1 Scope and Limitations PAGE

2.2 Network Topology PAGE

2.3 Methodology PAGE

**3. Technical Findings PAGE**

3.1 Vulnerability Summary + Statistics PAGE

3.2 **Critical Severity Findings PAGE**

3.3.1 Technical Finding #1 PAGE

3.3.2 Technical Finding #2 PAGE

**3.3 High Severity Findings PAGE**

3.4.1 High Severity Finding #1 PAGE

3.4.2 High Severity Finding #2 PAGE

**3.4 Medium Severity Findings PAGE**

3.5.1 Medium Severity Finding #1 PAGE

3.5.2 Medium Severity Finding #2 PAGE

**3.5 Low Severity Findings PAGE**

3.6.1 Low Severity Finding #1 PAGE

3.6.2 Low Severity Finding #2 PAGE

**3.6 Informational Severity Findings PAGE**

3.7.1 Informational Severity Finding #1 PAGE

3.7.2 Informational Severity FInding #2 PAGE

**4. Appendix PAGE**

4.1 Appendix A: PAGE

4.2 Appendix B: PAGE

4.3 Appendix C: PAGE

4.4 Appendix D:

**THIS DOCUMENT IS CONFIDENTIAL**

**Disclosure Statement**

The scope of the following security audit performed by US-Western-10 is limited to the allotted 9-hour time period as defined by the client, The Cozy Croissant (TCC). Thus, findings presented in the report may not fully encompass all potential vulnerabilities on the network. The following reports include only findings encountered during the assessment. US-Western-10 highly recommends that a further evaluation of The Cozy Croissant (TCC) network is performed to ensure the confidentiality, integrity, and accessibility of all its resources. US-Western-10 recommends that external audits be conducted annually to verify that security and regulatory controls are adhered to once fully implemented by the organization.

**1. Executive Summary**

2-4 PARAGRAPHS MAXIMUM

[On November 19, 2022 [GIVEN TEAM NAME] conducted a security assessment of The Cozy Croissant (TCC)]   
  
[The executive summary serves as a high-level view of both risk and business impact in plain English. The purpose is to be concise and clear. It should be something that non-technical readers can review and gain insight into the security concerns highlighted in the report.

While IT staffers may need all the technical details, executives don’t need to understand the technology. They need to understand business risk, something a good executive summary will effectively communicate. It is imperative that business leaders grasp what’s at stake to make informed decisions for their companies, and the executive summary is essential to delivering that understanding.

Visual communication can also be helpful in getting complex points across clearly. Look for graphs, charts, and similar visuals in communicating the summary data provided here.]

1.1 Strategic Recommendations

[Includes advised next steps or categorized into immediate and long-term strategic actions]

Security is not just a destination, but a journey. In the absence of a defined security strategy, one-time security fixes can only do so much to protect your organization. Strategic recommendations from security experts will prove to be invaluable for your business, hence, look for a service provider that will give strategic recommendations to improve the working and security of your business.

**2. Engagement Overview**

2.1 Scope and Limitations

[Describes the parameters and scope of the engagement]

Timeframe

The testing of the TCC network was conducted within the following time frame:

Start Date/Time:

End Date/Time:

Assets Included

The included assets within the assessment include, but are not limited to:

[TCC’s systems and network; ie Corporate Network Systems (Windows domain controllers and user workstations), POS terminals, printers, public web servers…etc)

2.2 Network Topology

[Include diagram of network topology]

This website has 18 free templates that are customizable:

<https://online.visual-paradigm.com/diagrams/templates/network-diagram/>

2.3 Methodology

[Include Cyber Kill Chain methodology description]

<https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/>

[Our Pentesting methodology]

**3. Technical Findings**

3.1 Vulnerability Summary + Statistics

[Overall summary of findings and graphical statistics, e.g. pie charts, graphs, etc]

Chartle.com is a free chart maker

[Include Killchain Diagram]

[Findings + charts by severity]  
[Findings + charts by vulnerability type]

[Reminder: indicate not only the technical aspects but the business impact as well. The most valuable reports are those that speak to all audience members in the language they understand – especially those in leadership positions.]

**3.2 Critical Severity Findings**

[Vulnerability | CVSS Score]

Scope:   
[Affected system(s)]

Description:   
[Description of the vulnerability; can include screenshots]

Impact:   
[Harm/Potential harm from this exploit]

Test(s) Conducted:   
[How did we get to this vulnerability, what actions one takes to approach the vulnerability; can include screenshots]

Evidence & Steps to Reproduction:   
[Steps taken to showcase and exploit vulnerability]

Finding Comments:   
[Additional commentary; can include commentary on ‘likelihood of exploitation’]

Recommendations:   
[Method to fix]

References:   
[Any references, ie links to a compliance, regulation, informational webpage about this specific vulnerability]

**3.3 High Severity Findings**

[Vulnerability | CVSS Score]

Scope:   
[Affected system(s)]

Description:   
[Description of the vulnerability; can include screenshots]

Impact:   
[Harm/Potential harm from this exploit]

Test(s) Conducted:   
[How did we get to this vulnerability, what actions one takes to approach the vulnerability; can include screenshots]

Evidence & Steps to Reproduction:   
[Steps taken to showcase and exploit vulnerability]

Finding Comments:   
[Additional commentary; can include commentary on ‘likelihood of exploitation’]

Recommendations:   
[Method to fix]

References:   
[Any references, ie links to a compliance, regulation, informational webpage about this specific vulnerability]

**3.4 Medium Severity Findings**

[Vulnerability | CVSS Score]

Scope:   
[Affected system(s)]

Description:   
[Description of the vulnerability; can include screenshots]

Impact:   
[Harm/Potential harm from this exploit]

Test(s) Conducted:   
[How did we get to this vulnerability, what actions one takes to approach the vulnerability; can include screenshots]

Evidence & Steps to Reproduction:   
[Steps taken to showcase and exploit vulnerability]

Finding Comments:   
[Additional commentary; can include commentary on ‘likelihood of exploitation’]

Recommendations:   
[Method to fix]

References:   
[Any references, ie links to a compliance, regulation, informational webpage about this specific vulnerability]

**3.5 Low Severity Findings**

[Vulnerability | CVSS Score]

Scope:   
[Affected system(s)]

Description:   
[Description of the vulnerability; can include screenshots]

Impact:   
[Harm/Potential harm from this exploit]

Test(s) Conducted:   
[How did we get to this vulnerability, what actions one takes to approach the vulnerability; can include screenshots]

Evidence & Steps to Reproduction:   
[Steps taken to showcase and exploit vulnerability]

Finding Comments:   
[Additional commentary; can include commentary on ‘likelihood of exploitation’]

Recommendations:   
[Method to fix]

References:   
[Any references, ie links to a compliance, regulation, informational webpage about this specific vulnerability]

**3.6 Informational Severity Findings**

[Information gathered that presents little to no threat to the system it is present on, but should be noted or remediated to lessen the attack surface of the organization.]

[Vulnerability | CVSS Score]

Scope:   
[Affected system(s)]

Description:   
[Description of the vulnerability; can include screenshots]

Impact:   
[Harm/Potential harm from this exploit]

Test(s) Conducted:   
[How did we get to this vulnerability, what actions one takes to approach the vulnerability; can include screenshots]

Evidence & Steps to Reproduction:   
[Steps taken to showcase and exploit vulnerability]

Finding Comments:   
[Additional commentary; can include commentary on ‘likelihood of exploitation’]

Recommendations:   
[Method to fix]

References:   
[Any references, ie links to a compliance, regulation, informational webpage about this specific vulnerability]

**4. Appendix**

4.1 Appendix A

[Perhaps include CVSS Scoring rubric]  
<https://www.first.org/cvss/specification-document>

<https://www.first.org/cvss/calculator/3.1>

4.2 Appendix B

[Additional info on PCI-DSS]

PCI-DSS v4.0 published 2022– see 12 requirements

<https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI_DSS-QRG-v4_0.pdf>

<https://www.auditboard.com/blog/pci-dss-requirements/>

4.3 Appendix C

[Additional info on GDPR Compliance]

<https://gdpr.eu/what-is-gdpr/>

<https://gdpr.eu/checklist/>

<https://gdpr.eu/tag/gdpr/>

4.4 Appendix D

[OSINT findings/references]

**LAST PAGE**