

Date:

Document ID:

Version:

**TITLE**

For **CLIENT**

# 

Table of Contents

[1 Document Control 1](#_Toc516165508)

[2 Executive Summary 1](#_Toc516165509)

[3 Introduction 1](#_Toc516165510)

[3.1 Heading 2 1](#_Toc516165511)

[3.1.1 Heading 3 1](#_Toc516165512)

[Appendix 1](#_Toc516165513)

Table of Figures

[Figure 1 – Document Map 1](#_Toc516165853)

[Figure 2 - Table Style location 1](#_Toc516165854)

Document Control

Author

|  |  |
| --- | --- |
| **Authors** |  |
| **Intellectual Property Ownership** | © 2018 CLIENT Ltd. All rights reserved |
| **Confidentiality** | Confidential |

Stakeholder List

The following list represents the reviewers and approvers for this document.

|  |  |  |
| --- | --- | --- |
| **Name** | **Organisational Role** | **Initiative Role** |
|  |  |  |
|  |  |  |

Reference Documents

The following documents have been considered in developing this document or are referenced in this document.

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Document Name** | **Version/Date** | **Source** |
|  |  |  |  |

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Name** | **Amendments** | **Date** |
|  |  | First release |  |

# Summary

* What are the main points that happened in the last month? What do they need to know about?
* Tell the story, what was onboarded? What has changed? How many vulnerabilities have been found?
* Tell them something about their overall security posture

# Coverage

* What is covered? (infographic if possible – then you can show percentage of coverage)
  + Eg. 32 EC2 in Prod, X in non-Prod
  + CloudTrail across Prod and NonProd
  + GSuite
  + Sophos (number of devices)
  + List of log sources
* What do we know about that isn’t covered?
  + If it’s not covered, what is the plan for getting it onboarded?
* What plans are their to expand the coverage?
  + O365 being onboarded

# Incident Summary (table? – might need to come after summary section)

* What was identified, what actions were taken, what was the outcome?
* This is a summary of details in the next sections

# Email and Collaboration Security

* How many external emails (third-parties) have access to Pillar data?
* Who are the new third-parties?
* Have we detected any anomalies with access to data?
* Need look into GSuite to determine how well security controls are working
* Just report on metrics provided by GSuite

# Endpoint

* How many endpoint devices are covered
* Which devices do we know of that are not covered
* What level of protection are they at?
* Mobile coverage (they have issues with GSuite device management at the moment)

# Vulnerability and Patch Management

* Show vulnerabilities found compared to patches implemented
* Use Threat Intelligence to highlight the Top 5 (or Top 10) patches that need to be addressed asap
* If there are

# IAM & PAM

* Users without MFA
* Number of API keys that have not been rotated**.**
* Failed login attempts for VIP users and administrators
* Unusual, guest & suspicious accounts
* Geographically impossible logins
* Login attempts from TOR/Anonymous nodes/proxies
* Successful login after multiple failed logins…
* Users logging into VPN

# Network Security

* What network attacks were detected and stopped?

# Roadmap (something trackable)

* What are we planning on doing next? Lots of stuff isn’t covered at the moment (vuln scanning, app logs, etc) we need to be proactive in getting this resolved
  + For July
    - Load AV keys on all instances for vuln scanning
    - Modify rsyslog/Loggly configuration to capture application logs
  + When are we planning to have those onboarded?

Appendix

Text

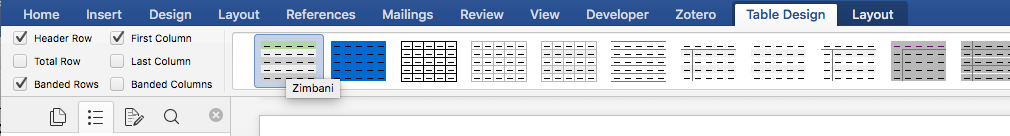


Figure 2 - Table Style location

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# The Python code created Document

This is a test and first paragraph created for this project. To ensure that there is enough content in this paragraph am adding the famous sample text next to it. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

## This is a level 2 heading

This is paragraph 2 and followed by sample test. Sit amet justo donec enim diam vulputate ut pharetra. Commodo quis imperdiet massa tincidunt nunc pulvinar sapien et. Elementum nibh tellus molestie nunc non blandit massa. Neque laoreet suspendisse interdum consectetur libero id faucibus nisl. Enim tortor at auctor urna nunc id cursus. Neque convallis a cras semper auctor neque vitae tempus quam. Congue mauris rhoncus aenean vel. Est lorem ipsum dolor sit amet consectetur adipiscing. Mauris pharetra et ultrices neque ornare aenean. Proin fermentum leo vel orci porta.

|  |  |
| --- | --- |
| City | Country |
| Basildon | United Kingdom |
| Parkville | United States |
| Astoria | United States |
| Echuca | Australia |
| Cahaba Heights | United States |
| Mickleton | United States |
| Peoria | United States |
| Martin | United States |

## This is also a level 2 heading

This is paragraph 3 which should be followed by a line break.. So assuming this appears in a new page. The remaining part of the paragraph is from the famous Lorum Ipsum. Mattis aliquam faucibus purus in massa. Mi bibendum neque egestas congue quisque egestas diam in. Donec adipiscing tristique risus nec feugiat in. Nunc sed id semper risus. Sed viverra tellus in hac. Consequat ac felis donec et odio pellentesque diam volutpat. Non sodales neque sodales ut etiam. Vitae elementum curabitur vitae nunc sed velit. Quisque id diam vel quam elementum pulvinar etiam. Integer vitae justo eget magna fermentum iaculis eu. Risus quis varius quam quisque id diam. Egestas maecenas pharetra convallis posuere morbi leo urna molestie.