

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

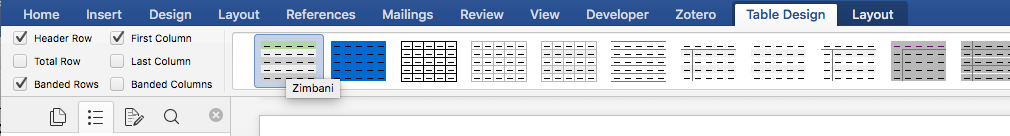


Figure 2 - Table Style location

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