Crayon

Cloud Security Assessment

SERVICE DESCRIPTION

Crayon Cloud Security Assessment

Crayon Cloud Security Assessment helps all customers using Microsoft 365 and Microsoft Azure understanding your business risks and exposure to cyberthreats.

Through a data-driven evaluation and analysis, Crayon provides prioritized remediations and recommendations for a safer innovation in Microsoft clouds.

-

Crayon Cloud Security Assessment enables you to:

- Get a documented understanding of your current security maturity and posture
- Innovate safely with full confidence in your cloud security posture
- Progress with confidence in your Zero Trust journey following achievable and prioritized steps
- Gain business stakeholders to support your efforts
- Achieve compliance across all relevant security standards

Crayon

Product Break-down

Data Collection

- extensive **scans** and data collection from your **Microsoft 365** and Microsoft **Azure** estate
- in-depth **guided interview** with your IT organization, collecting **organizational**, **process** and **awareness** key information

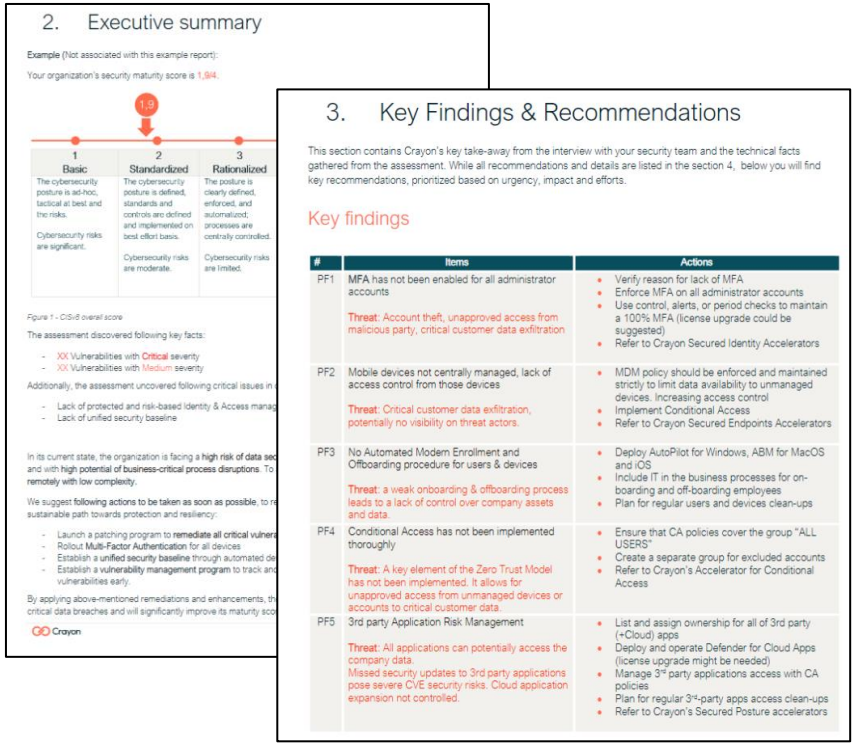
! all gathered data remains within your Microsoft Azure tenant.

Data Driven Analysis

- The gathered data is consolidated and analyzed by Crayon **security experts** following the **CIS Controls v8** to prioritize your Zero Trust journey and have the greatest impact on risk reduction based on current threats
- A **roadmap** is built from the processed data. It addresses the most critical and actionable remediations, while paving the way to your **Zero Trust** journey

Crayon Cloud Security Assessment Report

- An **executive summary** on the company's security maturity and the necessary initiatives towards a stronger security posture
- Crayon's **prioritized actions and recommendations**, articulated around an actionable short and mid-term **roadmap**
- Identified **critical technical weaknesses** (Microsoft365 & Microsoft Azure, Endpoints)



2. Executive summary

Example (Not associated with this example report):

Your organization's security maturity score is 1,9/4.

1,9

1 Basic	2 Standardized	3 Rationalized
The cybersecurity posture is ad-hoc, tactical at best and the risks. Cybersecurity risks are significant.	The cybersecurity posture is defined, standards and controls are defined and implemented on best effort basis. Cybersecurity risks are moderate.	The posture is clearly defined, enforced, and automatized; processes are centrally controlled. Cybersecurity risks are limited.

Figure 1 - CIS v8 overall score

The assessment discovered following key facts:

- XX Vulnerabilities with Critical severity
- XX Vulnerabilities with Medium severity

Additionally, the assessment uncovered following critical issues in

- Lack of protected and risk-based Identity & Access manag
- Lack of unified security baseline

In its current state, the organization is facing a high risk of data sec and with high potential of business-critical process disruptions. To remotely with low complexity.

We suggest following actions to be taken as soon as possible, to re sustainable path towards protection and resiliency:

- Launch a patching program to remediate all critical vulnera
- Rollout Multi-Factor Authentication for all devices
- Establish a unified security baseline through automated de
- Establish a vulnerability management program to track and vulnerabilities early.

By applying above-mentioned remediations and enhancements, th critical data breaches and will significantly improve its maturity sco

Crayon

3. Key Findings & Recommendations

This section contains Crayon's key take-away from the interview with your security team and the technical facts gathered from the assessment. While all recommendations and details are listed in the section 4, below you will find key recommendations, prioritized based on urgency, impact and efforts.

Key findings

#	Items	Actions
PF1	MFA has not been enabled for all administrator accounts Threat: Account theft, unapproved access from malicious party, critical customer data exfiltration	• Verify reason for lack of MFA • Enforce MFA on all administrator accounts • Use control, alerts, or period checks to maintain a 100% MFA (license upgrade could be suggested) • Refer to Crayon Secured Identity Accelerators
PF2	Mobile devices not centrally managed, lack of access control from those devices Threat: Critical customer data exfiltration, potentially no visibility on threat actors.	• MDM policy should be enforced and maintained strictly to limit data availability to unmanaged devices. Increasing access control • Implement Conditional Access • Refer to Crayon Secured Endpoints Accelerators
PF3	No Automated Modern Enrollment and Offboarding procedure for users & devices Threat: a weak onboarding & offboarding process leads to a lack of control over company assets and data.	• Deploy AutoPilot for Windows, ABM for MacOS and iOS • Include IT in the business processes for on-boarding and off-boarding employees • Plan for regular users and devices clean-ups
PF4	Conditional Access has not been implemented thoroughly Threat: A key element of the Zero Trust Model has not been implemented. It allows for unapproved access from unmanaged devices or accounts to critical customer data.	• Ensure that CA policies cover the group "ALL USERS" • Create a separate group for excluded accounts • Refer to Crayon's Accelerator for Conditional Access
PF5	3rd party Application Risk Management Threat: All applications can potentially access the company data. Missed security updates to 3rd party applications pose severe CVE security risks. Cloud application expansion not controlled.	• List and assign ownership for all of 3rd party (+Cloud) apps • Deploy and operate Defender for Cloud Apps (license upgrade might be needed) • Manage 3rd party applications access with CA policies • Plan for regular 3rd-party apps access clean-ups • Refer to Crayon's Secured Posture accelerators

Crayon

SERVICE CONTENT

Example of collected data

All gathered data is stored in customer's tenant.

OS:
- version, supported or not supported by security updates, End of Life

Devices:
- Microsoft Intune list, inactive devices, active devices
- Missing security updates on endpoints
- Manually flagged endpoints
- Bitlocker disabled on how many devices
- Firewalls status

Applications:
- Installed applications on endpoints, version, risk level

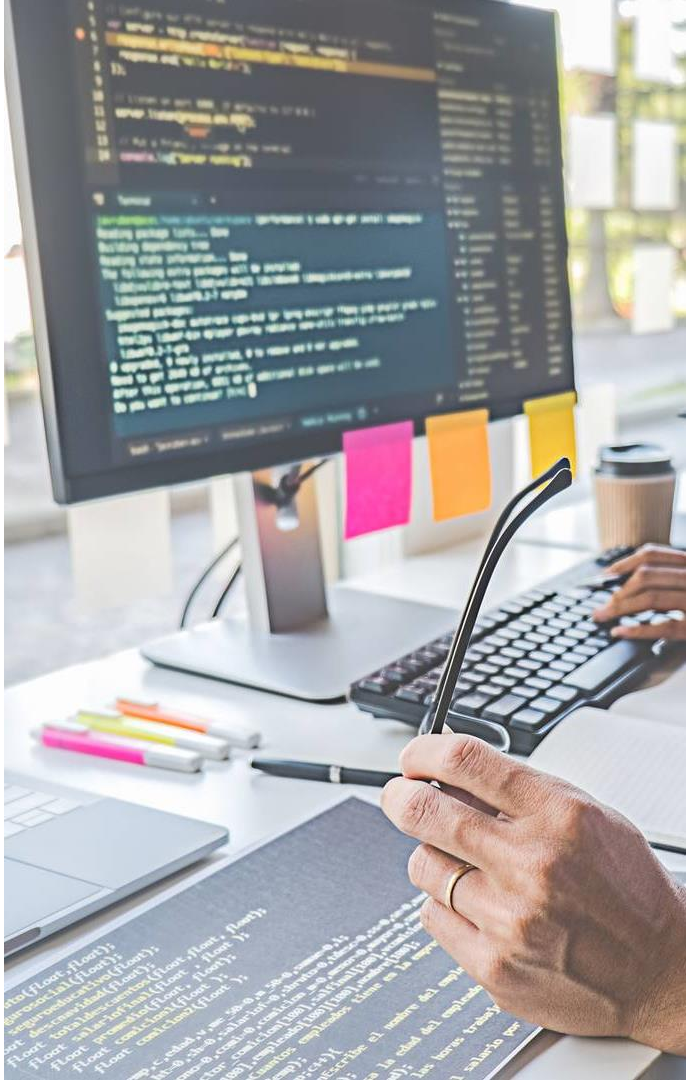
User accounts:
- Admin account, amounts and types (both Microsoft AAD and AD), MFA level
- enabled and disabled accounts, inactive accounts (30 and 90 days)
- Microsoft AAD external users, users without MFA, total enabled users

Endpoint security level (spec. services):
- PowerShell exe level, RDP level, SMB level
- Antivirus overview

Email protection:
- SPF, DKIM and DMARC records

Microsoft365:
- Potential PII data based on customer and consultant PII word list, Microsoft365 Secure Score
- Microsoft SharePoint external document sharing based on PII listing

Microsoft Azure resources:
- Azure Storage account security level (TLS, unencrypted sharing, SMB level)
- Azure SQL transparent encryption level
- Azure Secure Score
- Azure NSG rules
- Azure Secure Score



DELIVERY PLAN AND SCHEDULE

Break-down and delivery plan

Offer and decision

- Scope and offer adjustment
- Approval
- Contract signature

Delivery kick-off, data gathering

- Kick-off workshop
- Solution deployment in customer tenant
- Technical scan
- OpSec maturity assessment

Assessment conclusions

- Delivery of the assessment report
- Presentation of keys findings and recommendations
- Closing and next steps towards stronger security

Week xx-yy 2022 | Week xx-yy 2022 | Week xx 2022

Crayon