cuatroi

Cyber Defense Analysis

cuatroi

Cyber Defense Analysis

Challeges	Ideal Solution	Desired Outcomes
• Tech adoption expands threat landscape: Industry 4.0 (IoT, cloud, blockchain, etc.) • Increasing pressure to comply regulations • Lack of Security pros in the market. • Leadership often not involved building a Security strategy. • Employees not trained	Being able to continuously assess Cyber risk posture and capabilities on three critical areas: Prevention, Detection and Response, and act on the most critical projects first thus balancing investment between risks and potential impacts while complying with industry regulations.	• Ensure that the organization understands the risks and sets the right priorities, putting in place the right governance, the right supporting processes and the right enabling technology. • Use a multi dimensional approach, to tackle the problem, without disrupting the business.
• Cyber crime will cost the global economy $6 trillion (or 6.3%) annually by 2021 • Attacks in june 2020 in South America increased by an average of 15%	Organizations rely in many security solutions from multiple vendors. By now, t here is enough proof that technology alone is not enough. Cyber security is all about prioritization & continuous learning, as well as getting leadership involved for efficient decision making and proper funding, and workforce properly trained.	• Achieve 100% security is neither feasible, not the proper goal instead build a good defensive posture, in which technology is more an enabler than a solution • The key to success is customization and specialization (one size doesn't fit all)

cuatroi

Cyber Defense Analysis

Solution

Cybersecurity assessment and cybersecurity roadmap of the Azure cloud that will allow the client to have a vision of the prioritized recommendations that must be implemented to improve the level of security and reduce the risk of loss or alteration of business information by cyber-attacks. The solution includes the following layers:

Office 365 Cybersecurity Assessment

The assessment will use the **Secure Score** tool in **Azure Security Center**, which will calculate a security score based on the current **security configuration and behavior of Microsoft 365 including application, data and devices** and compare it to Microsoft's security baseline and security best practices - NIST Cybersecurity Framework, ISO27001.

Cloud App Cybersecurity Assessment

To perform the assessment, the **IT Shadow** tool in **Azure Security Center** will be used, through which an exploration of the active cloud applications, resources, services, IP addresses, users and machines used in the cloud environment will be performed. **CUATROi's security specialists will perform an assessment of the risks to which your organization's cloud is exposed.**

Windows Cybersecurity Assessment

To perform the evaluation, the **Windows Secure Score** tool in Microsoft Defender ATP will be used, through which **a Windows security gap analysis will be performed, and the threats and vulnerabilities reported in Microsoft Defender ATP** will be identified. The scope of the security controls analysis will include **Office 365, Enterprise Mobility + Security and Windows 10**

Attack Simulator Analysis

Design and **execute spear phishing attacks** and analyze results of simulated attacks against internal users and document their overall behavior against phishing campaign and evaluate passwords across the company.

To design the spear phishing, the **Attack Simulator** in Microsoft Defender ATP will be used.

Cyber Defense Analysis

Methodology

Asses

Use one or more assessment components to determine active threats and current security posture: Secure Score, Shadow IT, Windows Security, Attack Simulator.

Prioritize

Prioritize security recommendations based on the assessment findings.

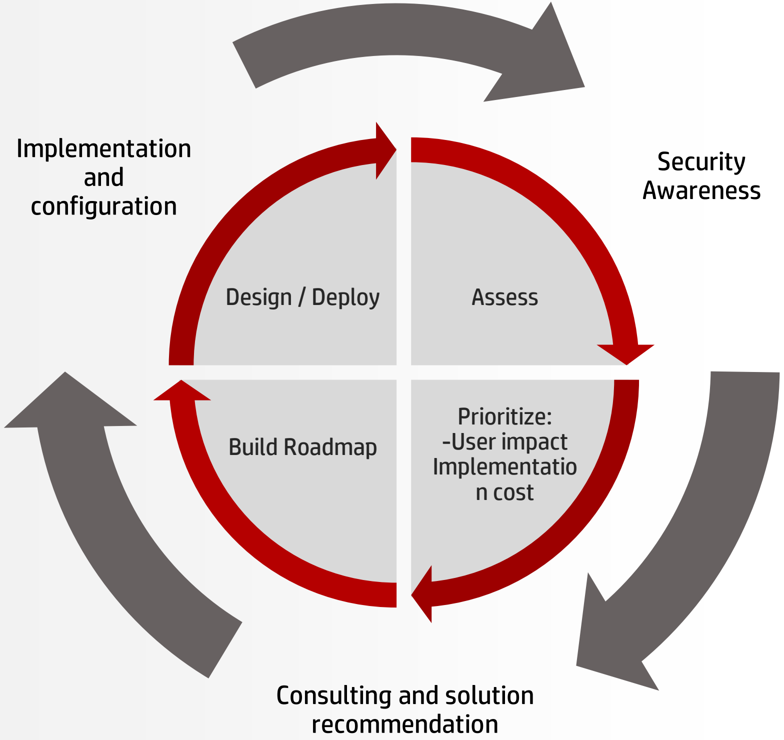
Build Roadmap

Build a roadmap for the implementation of the prioritized security recommendations.

Design / Deploy

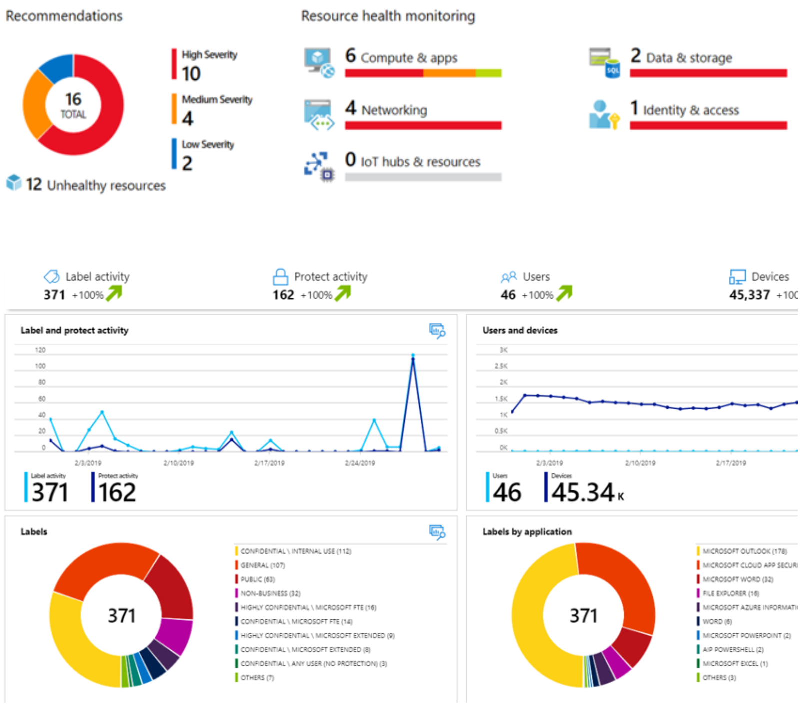
Design and deploy the recommended roadmap items.

Not in scope as part of the assessment engagement. CUATROi has the specialized professionals to support you the configuration and implementatios of this stage.


Implementation and configuration
Security Awareness
Design / Deploy
Assess
Build Roadmap
Prioritize: -User impact Implementatio n cost
Consulting and solution recommendation

Cyber Defense Analysis

Deliverables Security Azure Cloud



Recommendations

16 TOTAL

High Severity 10

Medium Severity 4

Low Severity 2

12 Unhealthy resources

Resource health monitoring

6 Compute & apps

2 Data & storage

4 Networking

1 Identity & access

0 IoT hubs & resources

Label activity 371 +100%

Protect activity 162 +100%

Users 46 +100%

Devices 45,337 +100

Label and protect activity

Label activity 371

Protect activity 162

Users and devices

Users 46

Devices 45.34K

Labels

371

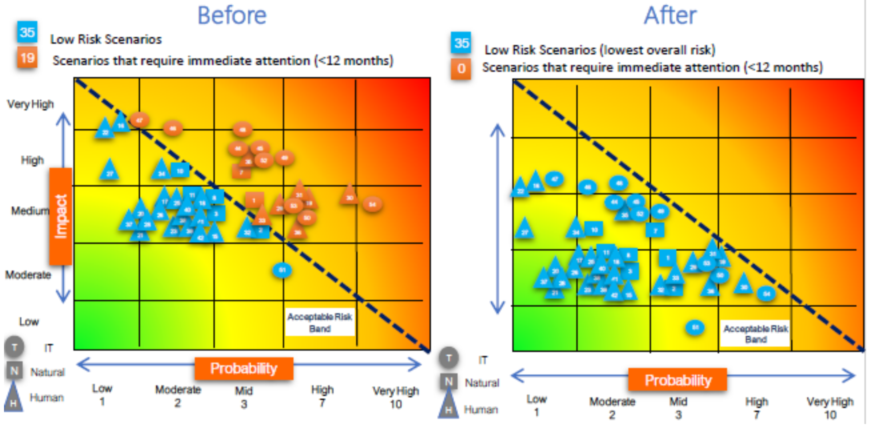
- CONFIDENTIAL \ INTERNAL USE (112)
- GENERAL (107)
- PUBLIC (63)
- NON-BUSINESS (32)
- HIGHLY CONFIDENTIAL \ MICROSOFT FTE (16)
- CONFIDENTIAL \ MICROSOFT FTE (14)
- HIGHLY CONFIDENTIAL \ MICROSOFT EXTENDED (9)
- CONFIDENTIAL \ MICROSOFT EXTENDED (8)
- CONFIDENTIAL \ ANY USER (NO PROTECTION) (3)
- OTHERS (7)

Labels by application

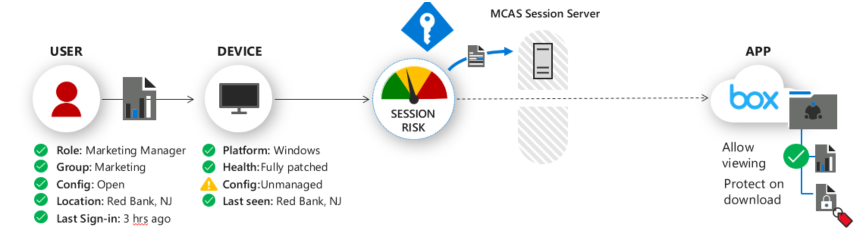
371

- MICROSOFT OUTLOOK (178)
- MICROSOFT CLOUD APP SECURI
- MICROSOFT WORD (32)
- FILE EXPLORER (16)
- MICROSOFT AZURE INFORMATI
- WORD (6)
- MICROSOFT POWERPOINT (2)
- AIP POWERSHELL (2)
- MICROSOFT EXCEL (1)
- OTHERS (3)

GAP ANALYSIS



RISK MAP



- Role: Marketing Manager
- Group: Marketing
- Config: Open
- Location: Red Bank, NJ
- Last Sign-in: 3 hrs ago

- Platform: Windows
- Health:Fully patched
- Config:Unmanaged
- Last seen: Red Bank, NJ

RECOMMENDED SETTINGS

Cyber Defense Analysis

Benefits and Next Steps

Benefits

- Help manage cyber security risk
- Get an overview of the Microsoft security controls required to secure your cloud environment
- Determine the current state of Microsoft security
- Identify the capabilities required to manage Microsoft security in your organization

Effort Required

- A Cyber Defense Analysis project lasts 2 to 3 weeks in length depending on the phases included.
- The customer should provide a staff person to assist approximately 20% of the time during installation, initial configuration, and validation of the work plan for remediation of the identified vulnerabilities.

Country

- LATAM

🇨🇴 Colombia
🇨🇱 Chile
🇵🇪 Perú

- Caribbean

Industry

- Financial
- Automotive
- Education
- Retail
- Manufacture
- Services

Price

From USD
$1.850

Next Steps

- A meeting with CUATROi to provide you with a better understanding of the importance of this service for your company, please contact your CUATROi Account Manager.
- The cost of the evaluation is estimated

cuatroi

cuatroi

CONSULTORIA · OUTSOURCING · SOPORTE

www.cuatroi.com