
cuatroi

Cyber Digital

cuatroi

Cyber Digital

Context

At this time it is very natural that business information is consulted through different devices by employees and third parties, in addition, it is increasingly common to see the use of hybrid and cloud environments for the needs of services and operation of enterprises, this situation leads us to the **new perimeter of information protection is not defined by the physical locations of the organization but by the resources and corporate services.**

However, organizations are still **not aware and continue to base their security only on the data center** through the firewall, IPS and VPN and with this scheme they are only protecting a part of their information, but they **lack the complete visibility and management of the information accessed outside this control environment**

Objective

CUATROi's CYBER DIGITAL service offers its clients the **Design, Deployment and support of a security model** that effectively adapts to the complexity of the modern environment, specifically in the use of **Hybrid environments**, where an **end-to-end protection strategy is established focused on the protection and response to events and incidents** that may be generated in the following elements: **Identities, devices, applications, information, infrastructure and networks**

Approach

Cyber Digital's security model focuses on:

- **All access requests are authenticated and authorized** according to security policy restrictions and any anomalies are inspected before access to information assets is granted
- Controls configured on **the principle of least privilege**
- **Multi-factor authentication** methods
- **Micro-segmentation**
- **Encryption, monitoring and control of activities, data traffic** on the network, applications, devices and infrastructure
- **Identification and response before advanced cybersecurity threats and alert management**

Cyber Digital
Solución

A Security Support Team that manage the incident and response, focus on the following security scope in Microsoft Azure:

Identity and Access Management

Deployment of access and identity management services through Azure Active Directory (Azure AD), focused on configuration of:

- Assignment of accounts and administrator roles
- Tracking the use of management accounts with Privileged Identity Management
- Azure AD Multi-Factor Authentication implementation
- Password and user account policy configuration
- Locking down legacy authentication protocols
- Enablement of Azure Active Directory Identity Protection for tracking session starts and compromised credentials
- Centralized device management
- Migration and integration of SaaS applications
- Automation of user account provisioning
- Monitoring and auditing of users

Cyber threat protection

Deployment of solutions for protection and mitigation of cyber threats in the Multi-Cloud Environments, focused on configuration of the following solutions:

- Centralized endpoint configuration Microsoft Defender ATP, Azure ATP and Office 365 ATP to manage advanced threats to servers, mobile devices, Office 365 and cloud applications
- Control and management of application traffic through Azure Application Gateway
- Implementation of the SIEM Azure Sentinel
- Enabling native anti-spam service and removing internal rules
- Enabling security alerts, Anti-phishing configuration

Cloud Security

Deployment of solutions that allow monitoring and control of activities and data in Hybrid Infrastructure and Apps:

- Intune Policy Enablement
- Microsoft Cloud App Security Implementation
- Azure Security Center monitoring of the different security components in Hybrid Environments
- Blueprint Security and Compliance: PCI DSS 3.2.1, ISO27001, Azure CIS
- End-to-end encryption, data transmission and storage
- Installation and configuration of the health check agents on the On-premise infrastructure
- Universal validation of assets to perform the integration of office365, Azure and On-premise security components
- Analysis of vulnerabilities, advisory in the definition of action plans and monitoring of the defined treatment

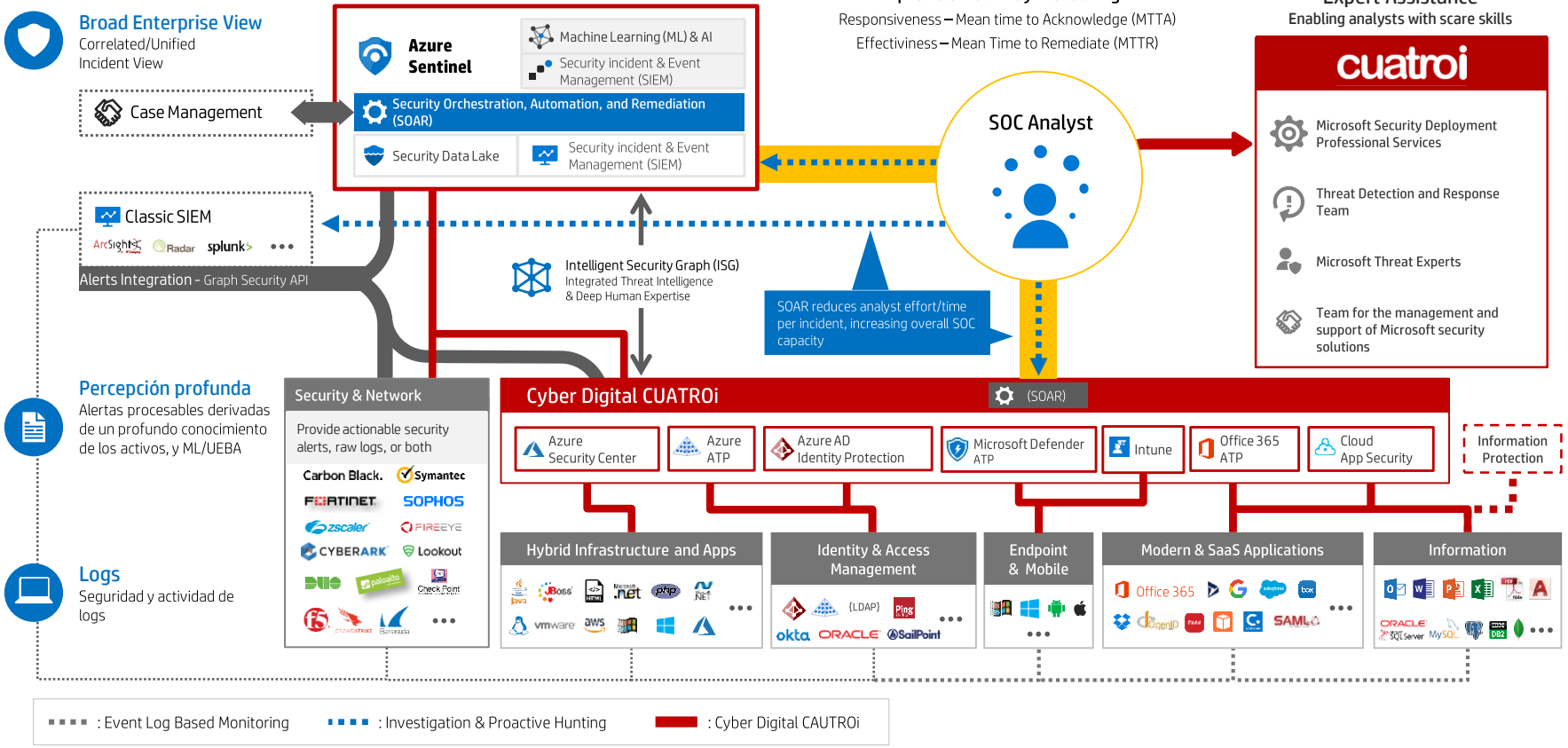
Microsoft Solution

Azure AD Identity Protection

Azure Sentinel SIEM | Office 365 ATP | Microsoft Defender ATP | Azure ATP

Azure Security Center | Cloud App Security | Intune

Cyber Digital
Architecture



Cyber Digital

Methodology

Preparation

- Know the security policies of the entity
- Current technological environment
- Diagnosis and identification of the security mechanisms required for the organization

Installation and configuration

- Definition of the Deployment work plan for each secutiry solution
- Installation and configuration of Microsoft security solutions environments required by the company according to the detailed plan

Testing

- Technical and functional testing of configured solutions in quality environment

Deployment

- Approval to move to the production environment of the configured and tested solutions
- Rollback Plan
- Post-production testing and performance validation

cuatroi

Cyber Digital

Benefits and next steps

Benefits

- Improve the visibility of security threats on information to implement automatic and manual controls
- Improved incident response times and reduced exposure to training risk for users or authorized personnel
- The security model will be implemented according to the client's reality

Effort

- The implementation time of Cyber Digital's service will depend on the security solutions and configurations required by the client according to its reality.

Country

- LATAM
- Colombia
- Chile
- Perú
- Caribbean

Industry

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

Price

It depends on the solutions required by each client and type of service

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

WWW.CUATROI.COM