CYRISMA DATA SHEET

Cyber risk reduction through data-centric security analysis. A simplified approach with complementary risk management functions under a single application framework. Cloud based SaaS (Software as a Service) provides easy implementation and universal secure accessibility.

RISK MANAGEMENT FUNCTIONS

- Sensitive Data Discovery
- Vulnerability Scanning & Patching
- External Web App Scanning
- Configuration Hardening
- Active Directory Review
- Dark Web Monitoring
- Mitigation and Remediation Action

OVERALL RISK MANAGEMENT

- Compare progress of current & past scans
- Visible risk trend analysis and Scorecards
- Host risk matrix assessment
- Cyber Risk Assessment report and presentation
- Track progress against compliance standards (HIPAA, PCI DSS, NIST CSF, CIS Controls V8)
- Compare cybersecurity performance against other organizations in the same industry

VULNERABILITY MANAGEMENT

- Agent/Agentless based host
- Windows/Linux/MacOS/Network Devices
- Email alerts and notifications
- Detailed CVE results
- Root cause analysis
- Vulnerability lookup and research
- Progressive scan compare
- Remediation action plan assistance
- Patch Management - 3rd Party Apps

SENSITIVE DATA DISCOVERY

- Endpoint support (Agent and Agent-less options)
- Windows/Linux/MacOS
- Network Attached Storage/File Shares
- Local Office 365 Sync Scanning
- Cloud Office 365 Scanning (Exchange, OneDrive, SharePoint, and Team shares)
- Google Workspace (Google Drive, Docs, Sheets, Gmail)

Native File Format Summary

- *Open-source Office Suites*
- *Open document standards*
- *File databases*
- *Compressed archives*
- *ASCII text files of unknown types*

Sensitive Data Categories

- *All PCI DSS payment types*
- *Financial data, routing, swift, IBAN*
- *National IDS, SSN and many other countries*
- *Personal Info; names, address, phone, DOB*
- *Driver's license and passports*
- *Custom data patterns of unlimited variety*

OS CONFIGURATION HARDENING

- Windows/Linux/MacOS
- Email alerts and notifications
- Direct tie to CIS/DISA configuration protocols
- Baseline standards lookup and research
- Compare progress over time
- Remediation action plan assistance

ACTIVE DIRECTORY MONITORING

- Monitor type - Azure AD & On-prem AD
- Domain Information - DCs , Domain Mode
- User Information - Active vs Disabled
- Last log on
- Password last changed
- Group Information - Group Types , User Group Membership

MICROSOFT SECURE SCORE

- Track your progress to secure your Microsoft cloud environment
- View recommendations to enhance your security posture

RISK ASSESSMENT REPORTING

- Generate easy-to-understand overall and category-specific risk assessment and scan reports

DARK WEB MONITORING

Continuous Monitoring for Domain/IP Info in

- Breach Data (Compromised Accounts)
- Forums (Ransomware/Marketplaces etc.)

RISK MITIGATION PLANS

- Automatically generate action plans from results
- Monitor plan progress
- Assign plans to departments with accountability
- Remediation actions Include:
  - Secure delete of sensitive data
  - Encrypt sensitive data
  - Move sensitive data
  - Mask specific data within a file
  - Remove specific access rights

+1 585-326-5829

www.cyrisma.com

sales@cyrisma.com