Cyber - Scan, Analyse, Remediation

Cloud Activ8 Cyber Manager combines machine learning and intelligent tagging to identify anomalous activity, suspicious changes and threats caused by misconfigurations. Cyber Manager also comes value-packed with everything you need to sell and deliver out-of-the-box cybersecurity. You'll appreciate the, dynamic, built-in marketing material to help you position and sell your new security services with default Service Plans, Product Catalogues, and end-user slide shows. We've even included a Managed Security Service Agreement that auto populates with the details of the security services you will be delivering.

The Cloud Activ8 Platform is the foundation for delivering the industry's first 24/7 SOC-as-a-Service without requiring hardware. Architected enterprise cloud solution provides insight and visibility across your fleet of customers, and integrates with your preferred security stack. The platform offers popular integrations for ticketing, provisioning and deployment in the Cloud activ8 platform

Cyber Manager incorporates built-in breach detection technology that finds footholds that your anti-virus can't. Detect keyloggers, trojans, spyware, unauthorized registry changes, or other malicious activity. The standard Breach Detection System is automatically deployed for all your Cyber Manager sites. It performs a weekly scan and will let you know if it finds any lingering malware footholds that typically go unnoticed by anti-virus software, as they lie in wait on a client network and postpone their attack until a specified time in the future. Your weekly report includes summary information about the nature of the discovered issue.

Cyber Manager makes it easy for you to do the following:

- Expose Unauthorized logins or attempts to restricted computers
- Identify a new user profile suddenly added to the business owner's computer
- Find an application just installed on a locked down system
- Get alerted to unauthorized wireless connections to the network
- Notice if a new user was just granted administrative rights
- Detect an unusual midnight log-in for the first time by a day-time worker
- Find sensitive Personal Identifiable Information (PII) stored on machines where it doesn't belong
- Detect breaches that make it by the firewall and anti-virus
- Expose hacker footholds along with instructions on how to remove
- Advanced breach detection technology finds footholds that your anti-virus /spam can't.
- Detect keyloggers, trojans, spyware, unauthorized registry changes, or other malicious activity.
- Expose Unauthorized logins or attempts to restricted computers
- Find an application just installed on a locked down system
- Get alerted to unauthorized wireless connections to the network
- Notice if a new user was just granted administrative rights
- Detect an unusual midnight log-in for the first time by a day-time worker
- Find sensitive Personal Identifiable Information (PII) stored on machines where it doesn't belong
- Detect breaches that make it by the firewall and anti-virus
- Scans user, asset, and configuration data that monitoring systems don't.
- Discovers threats that anti-virus/anti-spyware/firewalls don't.
- Always "on patrol" scanning the network at pre-set scheduled times.
- Scheduled updates detailing Anomalies, Changes, and Threats prioritized by Severity.
- Alerts include interactive actions to "remediate" "investigate" or "ignore" the alert.

Daily Alerts and Weekly Notices Keep You Ahead of Any Internal Threat
Cyber Manager keeps you posted of any potential internal security issues going on inside your client's network. Set the time for the daily scan and Cyber Manager reports back with an email alert sent to any address you specify, including your own ticketing system. The daily alerts aggregate the issues that were detected during the past 24 hours and can be sorted either by priority/severity (high, medium and low) of the threat, or by the type of issue (threat, anomaly, change).

Monitoring Microsoft 365

24/7 Managed Security Operation Center (SOC) detects and responds to adversaries targeting your Microsoft 365 and Azure applications while helping you comply with regulatory mandates like PCI, HIPAA, SOC 2 and CMMC.

One of the largest blindspots in the industry is the lack of visibility into Microsoft 365 user threat data and to constantly have eyes monitoring it. Cloud ACtiv8 SOC platform purposely built for the MSP industry, provides a cloud experience backed by seasoned security analysts hunting malicious and suspicious activity.

Benefits of the SOC for Microsoft 365

REDUCE DWELL TIME - Quickly determine if your business is already compromised or under attack. With proactive security monitoring and threat hunting, CloudActiv8 significantly improves detection and response time down to minutes to minimize disruption when an incident does occur.

REDUCE COST - The CloudActiv8 SOC delivers security monitoring with the power of the cloud and billed as a monthly subscription eliminating expensive capital expenditures eventually consumed by the business owner.

SKILLS GAP – Companies around the globe report having difficulty recruiting cyber security talent. Furthermore, staffing around-the-clock all year around is not practical. Partnering with a Managed SOC provider has proven to be more cost effective and eliminates the skill resource gap.