Cloud1Solutions

Managed Security Services
Post Pandmic

Overview

Threat Actors are busy at work exploiting the ever increasing vectors of entry.

Remote and mobile workers have become a prime target of sophisticated cybercriminals. Organizations need to extend corporate security controls to these vulnerable end-users, and rapidly detect and respond to attacks on remote and local devices.

Check List

- ✓ Assets
- ✓ Access
- ✓ Data
- ✓ Communication

☎ 408 320 6966

info@cloud1solutions.com

www.cloud1solutions.com

Mike Wiechmann

C1S Security Operations Center

While many companies have sufficient parament defense deployments such as VPN, antivirus, firewalls, the missing component is interior monitoring. Without this visibility threat actors can live in your network for months exfiltrating data before encrypting and shutting down servers for ransom payment demands.

It all starts with the multi-level cloud architecture fueled with integrated threat intelligence, a built-in app store with purpose-built threat detection apps enabling MSPs to deliver 24/7 threat monitoring providing visibility across 5 attack pillars:

1) Endpoint
Windows & macOS event log monitoring, breach detection, malicious files and processes, threat hunting, intrusion detection, 3rd party NGAV integrations and more.

2) Network
Firewall and edge device log monitoring integrated with threat reputation, whois and DNS information.

3) Cloud
Microsoft 365 security event log monitoring, Azure AD monitoring, Microsoft 365 malicious logins, Secure Score.

4) Local Access Control List
Monitor policy and permission changes used by threat actors to elevate administrator permissions.

5) Human Behavior
By monitoring behavior we get advance 24/7 notification of breaches, malicious tools, permission changas and cyberterrorist state connections.