AI BASED CYBER DEFENSE PLATFORM
Security & Productivity. Connected

The COVID-19 pandemic has forced Organizations to quickly enable their employees to work remotely for an extensive period of time. Having people work remotely changes many things. This sudden spike in Work From Home scenario has exposed enterprises to serious security risks that security teams across the world are grappling with. Cybersecurity has been the most vulnerable area for all Organizations in the current situation as it encompasses everything that pertains to protecting our sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, governmental and industry information systems from theft and damage attempted.

Hence cyber defense mechanism is most essential for all organizations for Protection of enterprise mission critical application environment

The most common risks for companies when it comes to remote workers are the following:

- Inadequate threat monitoring to address the heightened scale of incidents

- Continuum of attack surface expanded to WFH – Remote Workers

- New users and partially compliant end points leading to risk exposure

- Complex & dynamically changing IT and IT GRC controls
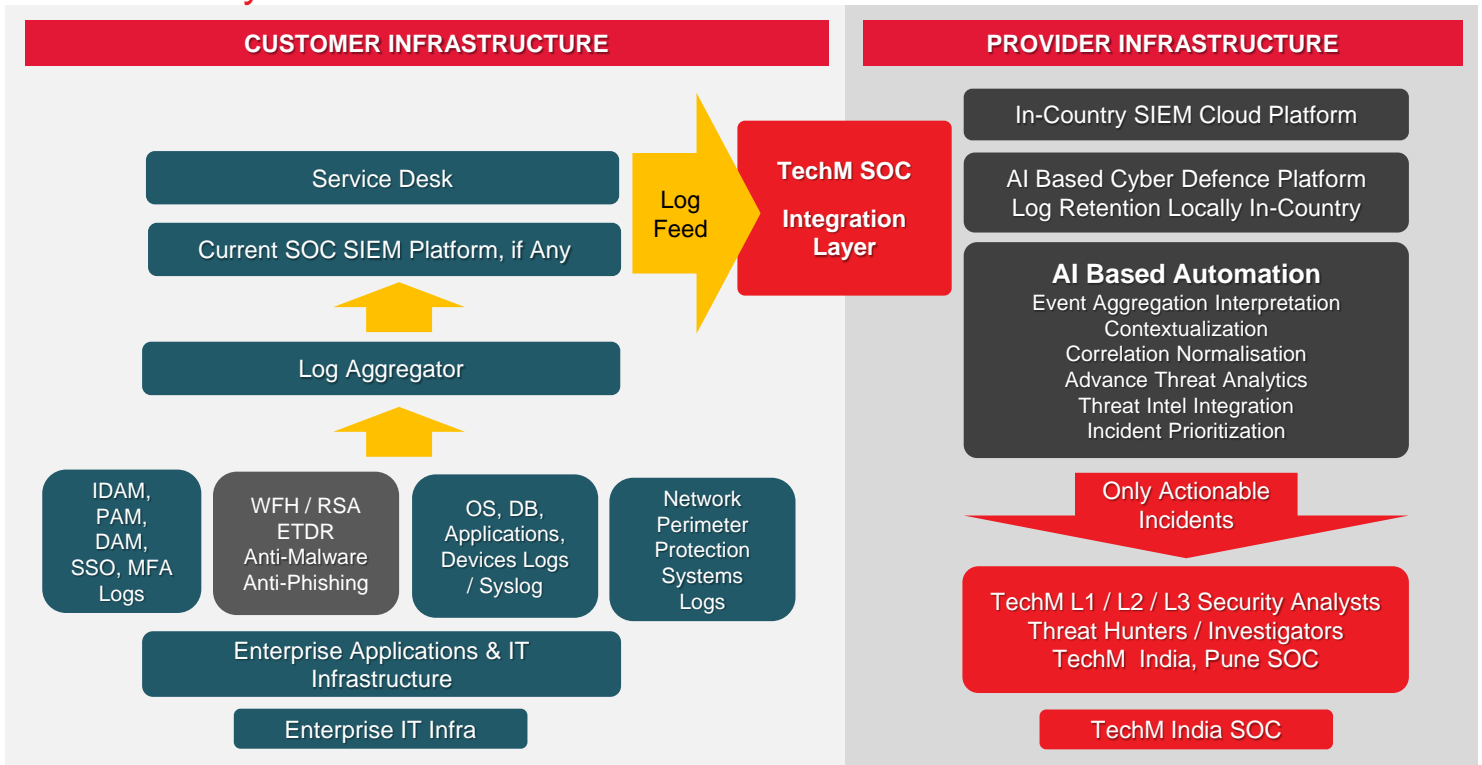
How do we address this?

Tech Mahindra's AI BASED CYBER DEFENSE PLATFORM SOLUTION is a fast & remotely deployable, cost-effective and have cloaking capability against attacks and help Organizations to stay ahead of the curve.

This solution can help in

- AI Based Automated threat detection and response resulting in minimum human intervention

- Addressing shortage of SOC Analysts during COVID crisis by leveraging Artificial Intelligence

- Cloud Based AI-SOC Integration for Remote Security Incident Monitoring & Response

- Integrated and Continuous End-Point Threat Detection & Response

Connected World.
Connected Experiences.

AI Based Cyber Defence

CUSTOMER INFRASTRUCTURE

- Service Desk
- Current SOC SIEM Platform, if Any
- Log Aggregator
- IDAM, PAM, DAM, SSO, MFA Logs
- WFH / RSA ETDR Anti-Malware Anti-Phishing
- OS, DB, Applications, Devices Logs / Syslog
- Network Perimeter Protection Systems Logs
- Enterprise Applications & IT Infrastructure
- Enterprise IT Infra

Log Feed

TechM SOC Integration Layer

PROVIDER INFRASTRUCTURE

- In-Country SIEM Cloud Platform
- AI Based Cyber Defence Platform Log Retention Locally In-Country
- **AI Based Automation**
  Event Aggregation Interpretation
  Contextualization
  Correlation Normalisation
  Advance Threat Analytics
  Threat Intel Integration
  Incident Prioritization

Only Actionable Incidents

- TechM L1 / L2 / L3 Security Analysts Threat Hunters / Investigators TechM India, Pune SOC
- TechM India SOC

Business Benefits

- Cloud-based & Light-weight solution
- OPEX based Model and No upfront CAPEX or investment commitment.
- Push deployable within 4-7 days
- Scalable and flexible to handle surge in user volume
- Leverages existing setup
- Proven AI Cyber Defence Platform
- Cost-effective @ $xx/EPS/month or $xx/GB/Month or $xx/User/Month
- Compliant with US-CERT released advisories
- Plug and Play, Easy to Deploy 200+ Use Cases (Developed by Tech Mahindra)

https://www/us-cert.gov/ncas/alerts

Why should you engage with us?

With 18+ years of experience in Cyber Security Services, 1200+ dedicated security professionals and 170+ large Enterprise clients, Tech Mahindra is in a strong position to help organizations in Security Consulting, Data Security/ GDPR services, Identity & Access Management, Cloud Security, IoT /OT Security, Advance threat management, Application Security.

Tech Mahindra has pioneered in some of the innovation in Cyber Security domain like Deep Dark Web Services, Threat Hunting, Zero Day Attack Mitigation and AI- Micro Segmentation

Tech Mahindra has been awarded as the most Innovative Cyber security Company in the Cyber Security Excellence awards, 2019

Tech Mahindra is recognised as leaders by leading analysts like Forrester and Avasant.

Connected World.
Connected Experiences.