MAKINSIGHTS
Accomplish together

RANSOMWARE RESILIENCY SERVICES

Powered by
PICUS

OVERVIEW

Information and competitive processes continue to be the lifeblood of modern companies and are amongst the most critical assets to protect. With the many variants of Ransomware and related Threats running rampant, it's essential to have a layered defense based on:

- knowledge of your critical information assets,
- clarity as to your true susceptibility to distinct and evolving attack variants, and
- a resiliency strategy that prepares your org and team to respond and take definitive action.

MAKINSIGHTS has developed a set of Ransomware Resiliency services to provide our clients with the critical **INSIGHTS** necessary to be prepared to prevent, detect and respond to these Threats.

BENEFITS

- ✓ Immediately verify susceptibility to Threats and take action with explicit prevention and detection actions
- ✓ Quickly prioritize control resources to best defend against emerging Threats
- ✓ Increase credibility with stakeholders and regulators
- ✓ Brief the Executive team and BOD with confidence
- ✓ Demonstrate a measurable commitment to cybersecurity that can be tracked over time
- ✓ Implement strategic resiliency programs that address Business and IT responsibilities cohesively
- ✓ Focus resiliency resources on the most critical of your business processes and Crown Jewels
- ✓ Tune response capabilities to minimize downtime, data loss, and negative financial repercussions

6 DAYS
AVG DOWNTIME FOR OVER 60% OF BUSINESSES

92%
OF BUSINESSES FAIL TO RECOVER ALL FILES

OFFERINGS

Ransomware Attack Simulations (R-ITAS)

Implement proactive cybersecurity practices that involve simulating Ransomware attacks to assess organizational control veracity and response capabilities

Business Impact Analysis & Crown Jewel decomposition

Understand which key business processes and technology assets (Crown Jewels) are most vital to meet your business objectives

Immediate Threat Analysis Service (ITAS)

Leverage simulated Threats to assess organizational control veracity and response capabilities with tight EDR and SIEM integration

IR/DR operational governance

Develop the guidance that different teams require to properly plan, execute, govern and report on key aspects of the IR & Resiliency programs

Penetration Testing / Red & Purple teaming

Leverage our highly skilled personnel to perform focused, non-destructive attacks working in collaboration or against your existing InfoSec teams

IR/DR plan testing & oversight

Simulate security incidents to proof the Incident Management and Resiliency processes while building muscle memory and preparing for REAL incident handling

Business Continuity Program development

Develop a robust business continuity strategy to navigate significantly disruptive events and enable continued realization of corporate objectives

Data identification, backup, recovery & offsite storage

Translate plans into specific operational and technological activities that support resiliency by identifying, protecting, responding, and recovering critical assets

EXPERIENCES

WELLS FARGO · tandym · GE Healthcare · LIPPERT · SUNAT · CAVALI · BANCO PICHINCHA · EAST WEST BANK

pillsbury · Diners Club INTERNATIONAL · JPMorganChase · LION STUDIOS BY APPLOVIN · CREDINKA · VISA · APPLOVIN · KAISER PERMANENTE

SCHEDULE A MEETING

MAKINSIGHTS.com

ideas@makinsights.com

Detroit, MI USA
Lima, Peru