



Ransomware Simulation

Have you ever wondered if your organization is protected against Ransomware?

Calian has decades of experience and dozens of experts in Digital Forensics Incident Response (DFIR) that understand the Tactics, Techniques, and Procedures (TTPs) of an attacker.

Equip your organization and protect it from potential ransomware attacks.

We have one objective and that is to help you close the gaps in your security before attacks can exploit and hold your organization ransom.

How is it done?

Our experts deploy a non-intrusive Ransom Simulation Toolkit on key sample assets and our Security Advisor collaborates with the IT Team to observe how your defense reacts.

The average attack costs businesses \$1.8m




An attack happens every 11 seconds




Only 65% of data is recovered




64% of Cyber insurance covers Ransomware

TEST YOUR DEFENSES

SIMULATE A REAL ATTACK WITH CONTROLLABLE COMPONENTS:


-  Command & Control
-  Advanced TTPs
-  Real Time Indicators


-  Encryption
-  Hyper-accurate Detection
-  Threat Intelligence


-  Data Exfiltration
-  Automated Protection Response
-  Remediation Processes


KEY FEATURES

DETERMINE ANY UNDERLYING WEAKNESSES WITHIN YOUR INFRASTRUCTURE AND EXPLORE THE ISSUES THREATENING YOUR SECURITY.

 **CONTROLLABILITY**
Neither the network nor the computer on which it is executed will be affected by the ransomware. All of the artifacts have been developed by iSecurity.

 **NO DOWNTIME**
Encrypt only specific folders on local drives and network shares created specifically for this exercise. Typically, ransomware encrypts only the specified folder.

 **TECHNOLOGY CENTERED**
A member of the client team; system administrator or security personnel will monitor each step of iSecurity's execution via a remote session while the company performs the tests.

 **MONITORED 24/7**
Test all of your anti-malware systems, firewalls, EDRs, IPS, IDS, SIEMs, and other malware protection softwares. Maintain continuous awareness of ransomware attacks with valuable insights so you can quickly respond and prevent them.

HOW IT WORKS

1
Infection through email, device or website



2
User is infected by ransomware



3
All data on PC and networks are locked out



4
Ransomware demand to unlock your data



SUPPORTIVE SERVICES

- Tabletop Exercise
- Cyber Breach & Incident Response Development
- Red Team & Ethical Penetration Testing
- BCP & DRP Assessment
- Threat Modeling & Cloud Security Design