MāKINSIGHTS
Accomplish together

Ransomware Resiliency Service Brief

PICUS

Contents

- Background
- Services overview
  - CTEM/BAS services focusing on Ransomware & Threat resilience
  - Penetration Testing / Red & Purple teaming
  - Business Continuity Program (BCP) development
  - Business Impact Analysis & Crown Jewel decomposition
  - IR/DR operational governance
  - IR/DR plan testing & oversight
  - Data identification, backup, recovery & offsite storage
- Q&A

Background

MAKINSIGHTS was founded in **2013 in Detroit, MI** and expanded to **Lima, Peru in 2018.** Our competitive edge is combining a global "Big-4" mindset with local talent and expertise through our worldwide footprint of partners and industry veterans possessing unique **INSIGHTS**

MAKINSIGHTS has successfully established programs and delivered innovative projects across **IT Risk Management, Privacy, Information Security, Cybersecurity,** and **IT Governance** in the US, Europe, Asia-Pacific, and South American countries

MAKINSIGHTS actively supports global organizations and those with other levels of scale in the following verticals:

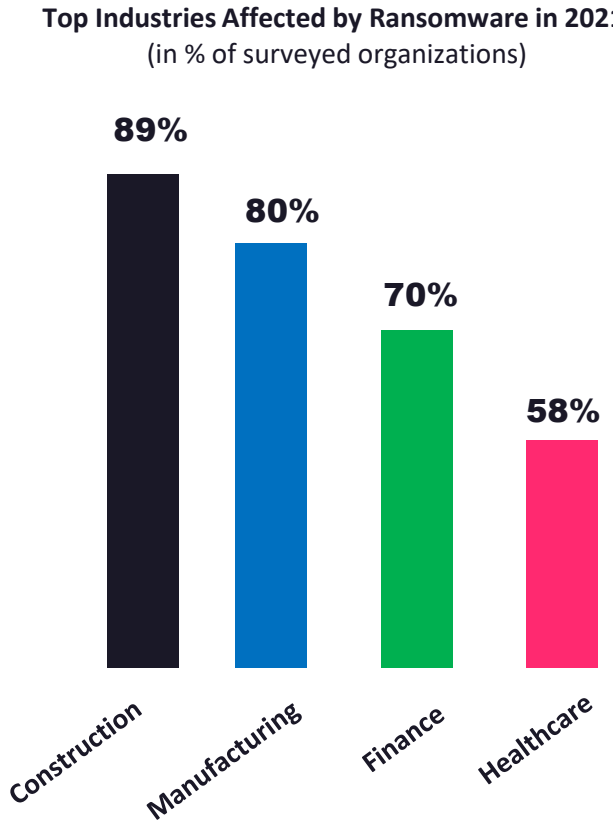
- Manufacturing
- Financial Services
- Healthcare
- Internet/Technology
- Telecommunications & Utilities

Ransomware Resiliency services overview

Applications, data, people, and competitive processes continue to be the lifeblood of modern companies and are amongst the most critical assets of your organization to protect.

With many variations of Ransomware and related Threats running rampant, these assets are repeatedly subject to attacks by amateurs, hacktivists, professional cybercriminal groups or rogue employees. Not knowing your organization's susceptibility to Ransomware or how these bad actors operate can lead to financial penalties, material losses, regulatory headaches or even lack of going concern.

MAKINSIGHTS has developed a set of complementary Ransomware Resiliency services to provide our clients with clarity as to their susceptibility and ensure that our clients are knowingly prepared to prevent, detect and respond to these threats.

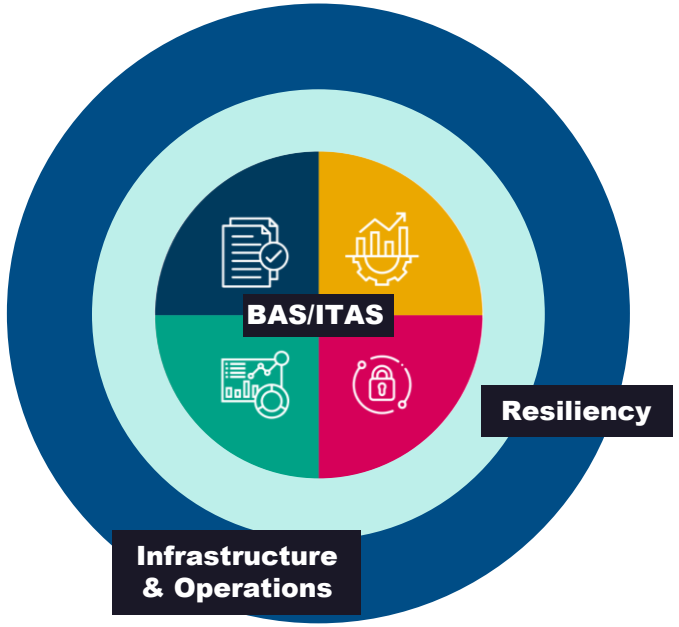


Ransomware Resiliency services summary

Understand your organization's true susceptibility to Ransomware and Threat Actors while being prepared to prevent, detect, and respond to adverse attacks in a timely manner

Benefits

- Fostering assurance of your program and further increasing credibility with stakeholders and regulators
- Briefing the BOD with confidence on your organization's susceptibility to the newest threats and attacks
- Demonstrating a measurable commitment to cybersecurity that can be tracked over time
- Developing and implementing strategic plans that measurably address significant control weaknesses
- Prioritizing limited Information Security resources to secure the most critical systems
- Ensuring restore and recovery capabilities link to the most critical services that your business needs
- Tuning your response capabilities to minimize downtime, data loss, and negative financial repercussions



Offerings

- Ransomware attack simulations (R-ITAS)
- Threat-ITAS (ITAS-2); Threat-ITAS with Integrations (ITAS-3)
- Penetration Testing / Red & Purple teaming
- Business Continuity Program (BCP) development
- Business Impact Analysis & Crown Jewel decomposition
- IR/DR operational governance
- IR/DR plan testing & oversight
- Data identification, backup, recovery & offsite storage

Ransomware attack simulations (R-ITAS)

MāKINSIGHTS
Accomplish together

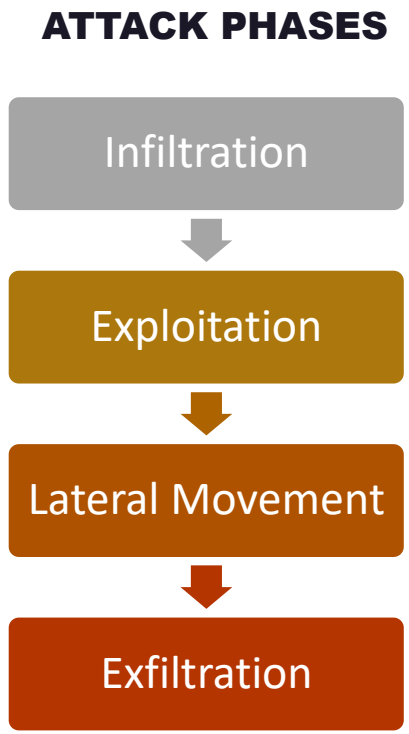
Implement proactive cybersecurity practices that involve simulating Ransomware attacks to assess organizational readiness and response capabilities

Benefits

- Understand your true susceptibility to Ransomware and prioritize protection, detection, and response capabilities accordingly
- Promote fact-based engagement with important internal and external stakeholders such as the BOD, governance bodies, and regulators
- Allow security teams to experience the entire lifecycle of an attack from initial compromise to containment and recovery
- Promote cross-functional collaboration among IT, security, legal, communications, executive management and key suppliers
- Prepare for real-world Ransomware attacks by testing the veracity of existing Incident Response plans and procedures
- Gain practical experience in dealing with Ransomware attacks, which can enhance skills in threat detection, incident analysis, response, and improve decision-making under pressure
- Validate the in-situ effectiveness of security controls across Firewalls, IPS/IDS, NGAVs, EDRs, and Secure Email Gateways against real and up to day Ransomware

Key activities

- Executing simulated attacks to identify weaknesses and susceptibility to Ransomware
- Developing and implementing a control strategy that protects the organization's key digital assets
- Identifying and prioritizing vulnerabilities and supporting remediation
- Formulating and executing Incident Response plans to handle Ransomware attacks
- Educating employees and stakeholders about the organization's capabilities and opportunities to improve



Threat-ITAS (ITAS-2)

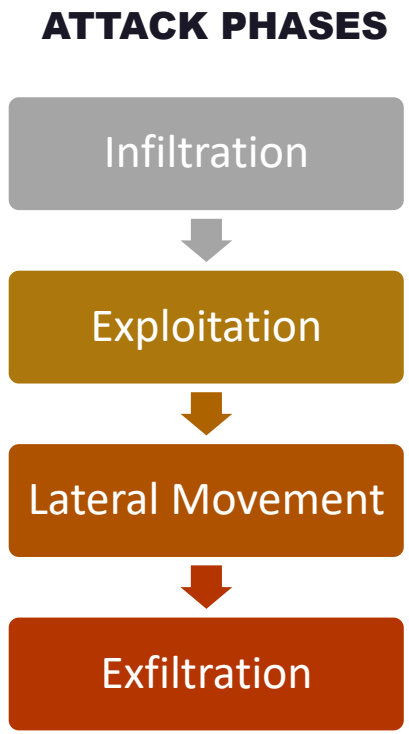
Implement proactive cybersecurity practices that involve simulating Ransomware and other related attacks to assess organizational control veracity and response capabilities

Benefits

- Understand your true susceptibility to Ransomware **and other Threats** while prioritizing protection, detection, and response capabilities accordingly
- Promote fact-based engagement with important internal and external stakeholders such as the BOD, governance bodies, and regulators
- Allow security teams to experience the entire lifecycle of an attack from initial compromise to containment and recovery
- Promote cross-functional collaboration among IT, security, legal, communications, and management teams and key suppliers
- Prepare for real-world Ransomware & other attacks by testing the veracity of existing Incident Response plans and procedures
- Gain practical experience in dealing with Ransomware & other attacks, which can enhance skills in threat detection, incident analysis, response, and improve decision-making under pressure
- Understand the susceptibility of new acquisitions or multiple locations to **emerging industry Threats**
- Validate the in-situ effectiveness of security controls across Firewalls, IPS/IDS, NGAVs, EDRs, and Secure Email Gateways against real and up to day Threats

Key activities

- Addressing multiple environments or locations; supporting M&A activities
- Executing simulated attacks to identify weaknesses and susceptibility to Ransomware **& other Threats**
- Developing and implementing a control strategy that protects the organization's key digital assets
- Identifying and prioritizing vulnerabilities and supporting remediation
- Formulating and executing Incident Response plans to handle Ransomware attacks
- Educating employees and stakeholders about the organization's capabilities and opportunities to improve



Threat-ITAS with Endpoint & SIEM Integration (ITAS-3)

Implement proactive cybersecurity practices that involve simulating attacks to assess organizational control veracity and response capabilities with tight EDR and SIEM integration

Benefits

- Understand your true susceptibility to Ransomware **and other Threats** while prioritizing protection, detection, and response capabilities accordingly
- Promote fact-based engagement with important internal and external stakeholders such as the BOD, governance bodies, and regulators
- Allow security teams to experience the entire lifecycle of an attack
- Promote cross-functional collaboration among IT, security, legal, communications, management teams and key suppliers
- Gain practical experience in dealing with attacks and decision-making under pressure
- Validate susceptibility of new acquisitions or multiple locations to **emerging industry Threats**
- Reduce remediation complexity by integrating with your specific endpoint provider
- Validate SIEM effectiveness and quickly adjust logging and alerting capabilities to address zero-day **Threats**
- Add DLP and WAF validation to the existing scope of security control validation including Firewalls, IPS/IDS, NGAVs, EDRs, and Secure Email Gateways

Key activities

- Addressing multiple environments or locations; supporting M&A activities
- Executing simulated attacks to identify weaknesses and susceptibility to Ransomware **& other Threats**
- Developing and implementing a control strategy that protects the organization's key digital assets
- Identifying and prioritizing vulnerabilities and supporting remediation
- Formulating and executing Incident Response plans to handle Ransomware attacks
- Analyzing endpoint tool capabilities and adjusting tool configurations to better respond to Threats
- Adjusting and tuning SIEM rules to better log and alert SOC staff; rule tuning
- Educating employees and stakeholders about the organization's capabilities and opportunities to improve

MÄKINSIGHTS
Accomplish together

Attack Path Validation – Additional Module

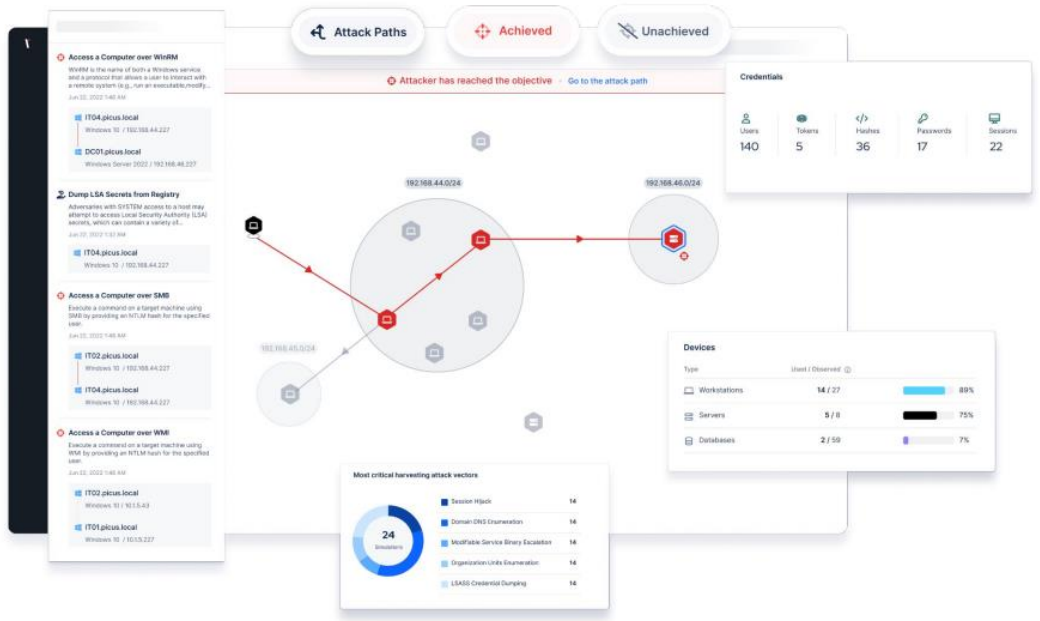
Stop adversaries in their tracks by identifying and eliminating the most direct routes to critical assets

Benefits

- Strengthen your internal network security by assuming compromise and discovering possible attack paths internal intruders might take
- Focus on actual world scenarios to discover paths that pose real security risks
- Automate offensive security testing and ensure investments deliver better outcomes and value

Key activities

- Scoping simulations tailored to your use cases and team expertise
- Creation and execution of planned simulations
- Analysis and remediation planning & validation support
- Development of executive and c-level reporting



Detection Rule Validation – Additional Module

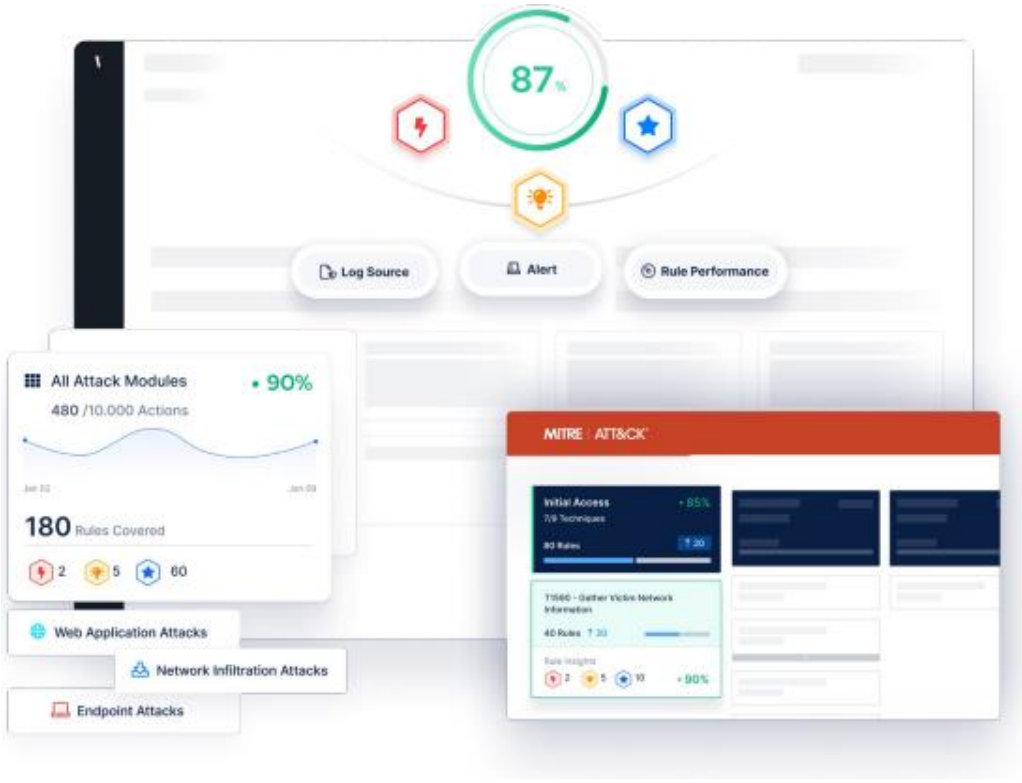
Significantly reduce the time necessary to tune your SIEM and improve the incident management capability of your SOC

Benefits

- Significantly improve SOC threat detection and response capabilities
- Enhance threat coverage, accuracy and performance of your SIEM rules
- Enable prioritization of alerts and alarms based on active, real-world threats
- Visualize and expand your team's understanding of threat coverage by mapping to the MITRE ATTC&K framework

Key activities

- Planning SIEM Health checks tailored to your use cases and team expertise
- Management of SIEM review process
- Detailed rule and configuration analysis with recommendations
- Oversight and validation of rule tuning outcomes
- Development of executive and c-level reporting



MÄKINSIGHTS
Accomplish together

Cloud Security Validation – Additional Modules

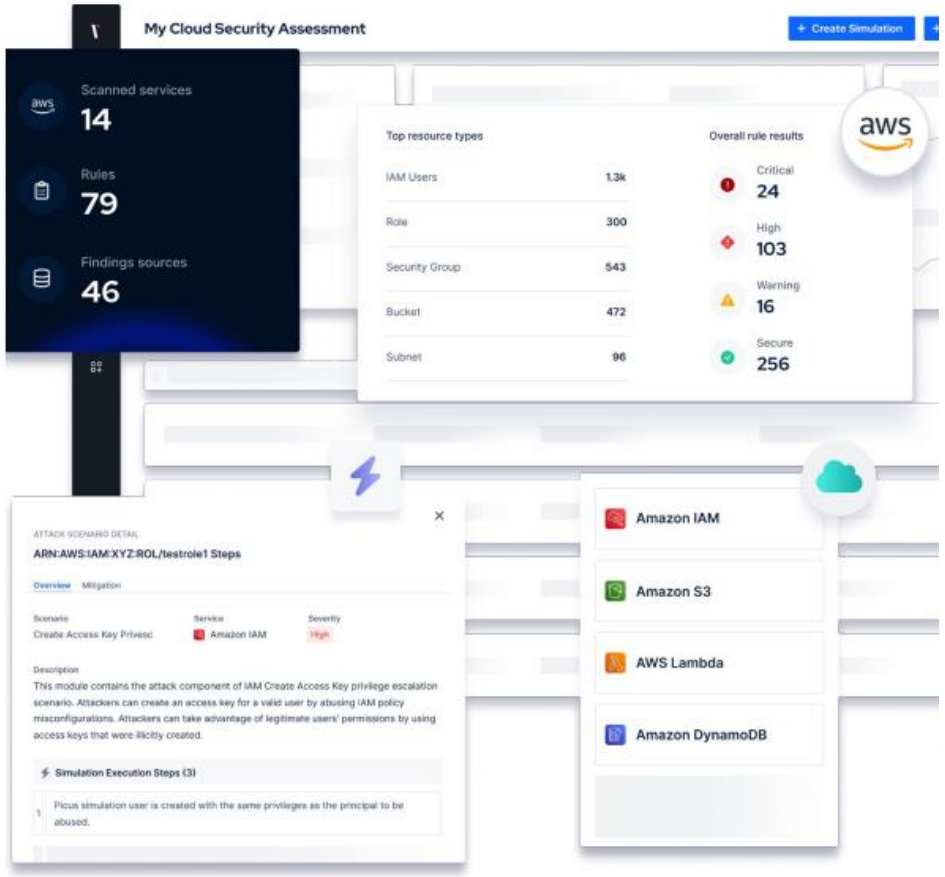
Optimize your cloud security posture through automated assessments and attack simulations focused on your specific cloud configurations

Benefits

- Quickly identify cloud service misconfigurations that attackers could exploit
- Understand weaknesses on your cloud access policies by simulating attacks in a controlled environment
- Mitigate found gaps with actionable insights

Key activities

- Planning audits and simulations tailored to your use cases and team expertise
- Creation and execution of planned simulations
- Analysis and remediation planning & validation support
- Development of executive and c-level reporting



MāKINSIGHTS
Accomplish together

Attack Surface Validation – Additional Module

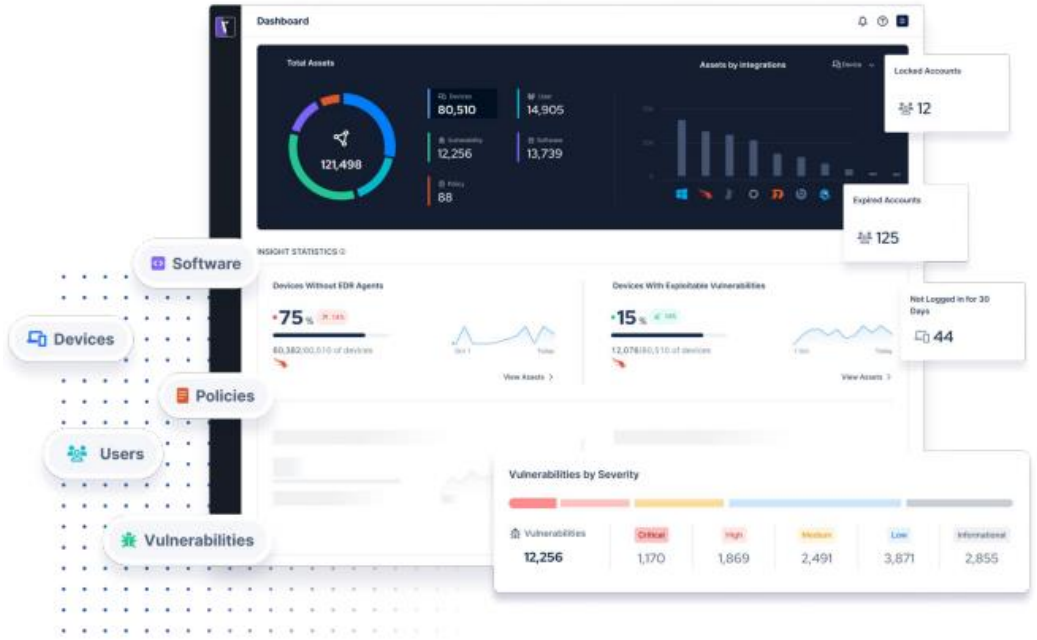
Streamline the discovery, classification, and risk assessment of your organization's internal and external cyber assets

Benefits

- View information about your external assets via a single pane of glass
- Detect non-compliant and misconfigured devices with insufficient security coverage
- Gain broad and deep visibility by integrating a wide range of data sources

Key activities

- Planning of simulations tailored to your use cases and team expertise
- Tool configuration support
- Creation and execution of planned simulations
- Creation and execution of pre-planned tracking actions
- Development of analysis and remediation reports
- Development of executive and c-level reporting



Penetration Testing

Leverage our highly skilled personnel to perform focused, non-destructive attacks on assets such as infrastructure, networks, mobile applications and web applications

Benefits

- Avoid the costs and reputational damage from a security breach
- Identify vulnerabilities before a hacker or rogue trusted insider can realize exploits
- Identify and analyze potential security weaknesses that could allow an attacker to gain access to specific critical assets
- Promote faster and more effective response in the event of an actual breach
- Provide evidence of compliance with regulatory/certification standards and address key requirement to obtain cyber insurance

Key activities

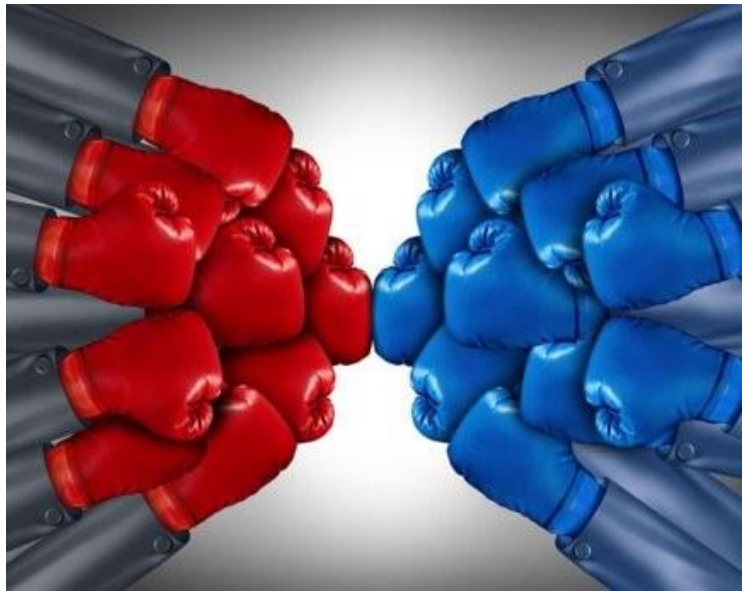
- Conducting automated scanning and manual testing to identify weaknesses such as open ports and services, misconfigurations, missing patches, and other logical vulnerabilities
- Exploiting the weaknesses using various manual testing techniques and tools
- Classifying the risk of the identified vulnerabilities and the potential impact of the exploits
- Helping determine the remediation strategies to support prioritization and decision-making
- Retesting of vulnerabilities to validate the efficacy of remediation
- Providing on-going remediation guidance to ensure systems remain secure

Red & Purple Teaming

Proactively protect the organization against cyberattacks by strengthening detection and response team capabilities through combative or collaborative engagements

Benefits

- Improved collaboration; by working together, red and blue teams can share information and learn from each other, leading to a better understanding of security risks and better decision-making
- Faster response; by simulating real-world attacks and testing incident response procedures, purple teaming can help organizations respond more quickly and effectively in the event of a breach
- Enhanced Training; purple teaming provides opportunities for red and blue team members to receive hands-on training and develop their skills in a real-world setting
- Ensure an understanding of existing Blue team capabilities and identify needs of the responders



Key activities

- Collaborating between red and blue teams to determine the scope of the engagement and ensure everyone is on the same page
- Simulating attacks, red team members simulate real-world attacks while blue team members work to detect and respond
- Providing detailed records of all evaluations carried out and all corrective detections and mitigations required to address the problems encountered during the investigations
- Sharing information and best practices between red and blue teams to continuously improve security posture and incident response capabilities

Business Continuity Program development

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

Benefits

- Understand the needs of business partners and customers; translate these into specific capabilities needed by your program
- Build a strategy that addresses the needs of key business partners and partners/clients
- Develop clear, measurable objectives for the business continuity function
- Analyze and understand how to allocate your people, process and technology resources
- Leverage valuable information about trends and improve your decision making
- Develop tools needed for the efficient operation of your program
- Be prepared for a wide range of disruptive events; limit continuity surprises
- Leverage our expertise and tools to bootstrap your program in a short amount of time

Key activities

- Defining the BCM program scope, processes, activities, and roles
- Planning of Business Impact Analysis (BIAs)
- Evaluating budget and investment options to support varying service levels
- Developing the program business (investment) case and program mission & charter
- Defining roles and responsibilities supporting the program
- Reporting, recommendation development and investment roadmap maintenance

BIAs & Crown Jewel Analysis

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

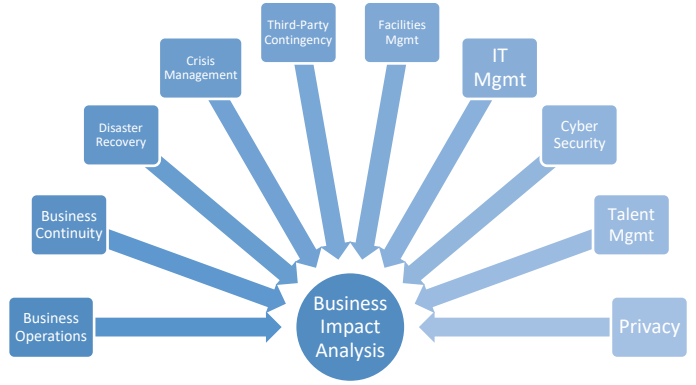
Benefits

- Align your organization's resiliency strategy with the companies' overall mission and goals
- Accurately link resiliency results to the strategic objectives of the business
- Understand the key business processes and their resiliency requirements
- Confirm and discover mission critical IT assets in your organization
- Allocate resources efficiently by identifying and prioritizing your most critical assets
- Leverage our expertise to quickly establish resiliency expectations and develop supporting services

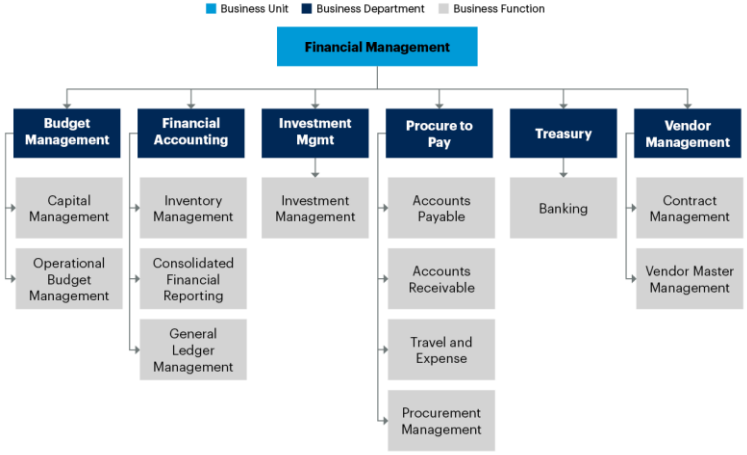
Key activities

- Defining the BIA scope and identification of key business processes
- Engaging stakeholders and decomposing key processes
- Understanding how IT and business activities/controls interact to produce value
- Articulating service/system specifications and dependencies supporting the mission
- Categorizing and prioritizing identified information assets
- Validating and adjusting how IT provides Resiliency services to the business
- Defining key expectations such as RTO and RPO, and how they work in practice
- Building a financial model to support Resiliency decisions

The BIA is the "Center of the Universe" for Resiliency and Business Value



An Example of Business Operations Mapping — Financial Management



IR/DR operational governance (plans, policies, standards)

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

Benefits

- Reuse existing tools to more quickly bootstrap your program
- Articulate expectations at all levels of the program
- Communicate to stakeholders in a language they understand
- Ensure involvement by key functions and roles
- Reduce surprises and alleviate pressure during times of stress
- Minimize additional resource demands on your team

Key activities

- Developing policies and standards
- Determining workflows aligned with roles and responsibilities
- Creating a business continuity communication matrix
- Documenting a process dependencies chart and vendor list
- Establishing a precedence & recovery chronogram
- Articulating recovery plans & playbooks
- Defining management and operational dashboards
- Training employees on the usage of the developed tools

IR/DR operational governance (plans, policies, standards)

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

Benefits

- Reuse existing tools to more quickly bootstrap your program
- Articulate expectations at all levels of the program
- Communicate to stakeholders in a language they understand
- Ensure involvement by key functions and roles
- Reduce surprises and alleviate pressure during times of stress
- Minimize additional resource demands on your team

Key activities

- Developing policies and standards
- Determining workflows aligned with roles and responsibilities
- Creating a business continuity communication matrix
- Documenting a process dependencies chart and vendor list
- Establishing a precedence & recovery chronogram
- Articulating recovery plans & playbooks
- Defining management and operational dashboards
- Training employees on the usage of the developed tools

IR/DR plan testing (table-tops & simulations)

Simulate security incidents and to proof the Incident Management process to build muscle memory and prepare for REAL Incident handling

Benefits

- Increase awareness and understanding of threats
- Evaluate your overall incident preparedness
- Identify deficiencies in your IR plan, including planning, procedural, and technical
- Clarify roles and responsibilities during an incident or disaster
- Validate IR & DR training programs and awareness
- Manage, communicate and socialize lessons learned through training and validate key documentation such as the IR process, DR plan, playbooks and associated guidance

Key activities

- Training work teams regarding their roles and responsibilities
- Testing that all aspects of the IR or DR plan (training, documentation, execution, IT resources, communications, etc.) are considered in advance
- Identifying gaps as well as alternative management & containment mechanisms
- Scoping the exercise, selecting participants, and developing the scenario for the exercise
- Presenting the scenario to the participants and guiding them through the incident response and disaster recovery processes
- Subsequently defining, designing and updating the IR plan and associated DR processes based on lessons learned

FEMA, the Federal Emergency Management Agency, studied responses to natural disasters and cyber attacks. They report that among the businesses that do recover after a disaster, only 29% were still in business two years later.

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

Benefits

- Ensure that even if primary data is lost due to hardware failures, human errors, or cyberattacks, you can recover the lost data from backups
- Reduces the impact of the attack and helps to thwart cybercriminals attempts to extort money
- Quickly restore systems and continue business operations with minimal downtime
- Recover previous versions of data or restore it to a point before the corruption occurred, minimizing disruptions and errors
- Provide the capability to store multiple versions of files, having access to previous versions can help identify when and how changes were made

Key activities

- Categorize data based on sensitivity and importance
- Develop a comprehensive backup plan detailing what data to backup, how often, and using which methods
- Implement regular, automated backups of critical data and systems to a secure location. Keep multiple versions to enable point-in-time recovery.
- Regularly test backups by restoring data in a controlled environment.
- Create a documented strategy for recovering data and systems after disasters.
- Define roles, responsibilities, and procedures to minimize downtime

Questions?

Management Team

MAKINSIGHTS
Accomplish together

Our team of seasoned professionals has led projects around the world for many of the largest and most recognized organizations, providing **MAKINSIGHTS** with deep domain expertise in **IT Strategy, Governance, Risk Management, Compliance, Privacy and Cybersecurity**

MARC KREVINGHAUS
MANAGING PRINCIPAL
President ISC2 - Peru

FELIPE CASTRO
Consulting Director

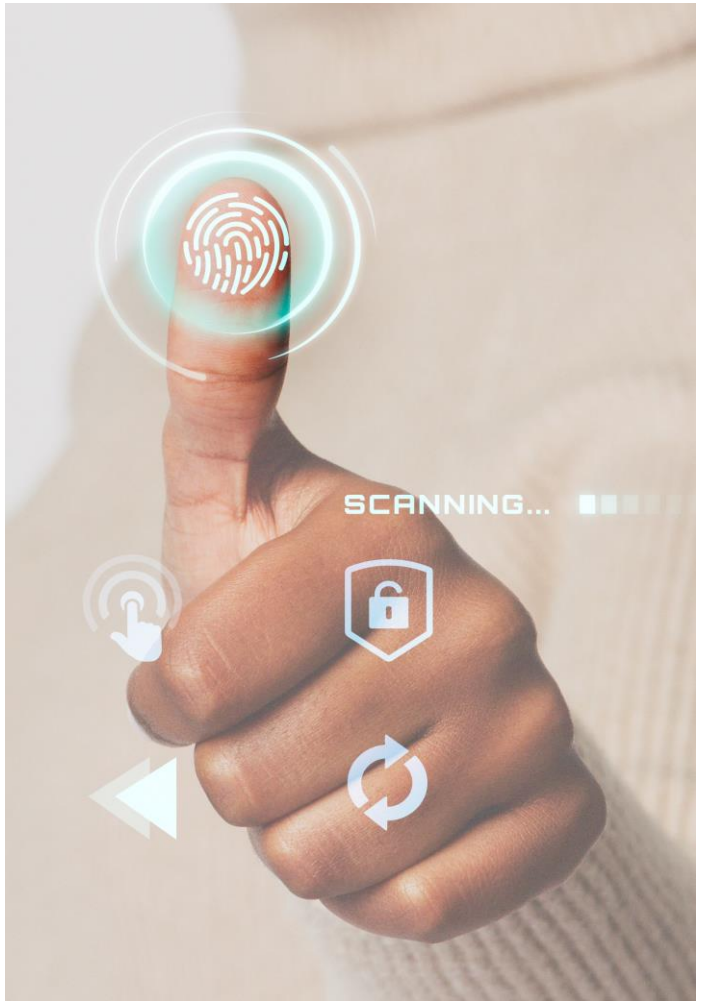
ANDRÉS AYBAR
Consulting Director

ANGEL LAY
Commercial Director

Contact us

MAKINSIGHTS
Accomplish together

ideas@makinsights.com
MAKINSIGHTS.com



MÄKINSIGHTS
Accomplish together

Security controls validation

GAIN CONFIDENCE THAT YOUR PREVENTION AND DETECTION CONTROLS ARE UP TO THE TASK

Benefits

- Transform your security program with a threat centric and proactive approach
- Measure and strengthen your cyber resilience
- Minimize the risk of serious breaches and demonstrate assurance
- Simulate real-world and updated cyber threats to identify prevention and detection gaps
- Obtain actionable mitigation recommendations

Key activities

- Definition of the scope and the simulation plan
- Tool configuration support
- Schedule and management of planned simulations
- Development of analysis and remediation reports
- Development of executive and c-level reporting