ARCTIQ + MIMIC

Architect Security

Proactive Ransomware Defense with Mimic + Arctiq:

A New Standard for Ransomware Resilience

Enterprise Security

OVERVIEW:

Why This Partnership Matters Now

Ransomware isn't just a threat—it's an inevitability. From healthcare to higher ed, ransomware operators continue to refine their playbooks, weaponizing lateral movement, persistence techniques, and extortionware. Mimic's deception-first approach flips that script, transforming your environment into a minefield for attackers.

At Arctiq, we've seen the gap: clients have EDR, backups, and alerting—but lack active dissuasion and decisive containment during the early access phase of an attack. That's where Mimic steps in, and where Arctiq layers in our MDR, SOC, and incident readiness services to deliver a holistic and proactive ransomware defense stack.

THE TECHNOLOGY:

What Mimic Does Differently

Key Differentiators:

- **Autonomous Deception Fabric:** Creates synthetic artifacts (credentials, file shares, memory artifacts, registry keys) that blend into your environment and serve as high-fidelity tripwires.
- **Zero Trust Decoys:** Every alert generated is based on intentional engagement with false assets—no noise, no ambiguity.
- **Adversary Behavior Profiling:** Behavioral fingerprints extracted from engagement give security teams early indicators of attack type and intent.
- **Real-time Response Hooks:** Integrates with EDR, SIEM, and SOAR for automated isolation and response.

Where It Fits Best

This solution is not for everyone—it's for clients who:

- Are already investing in detection/response tooling but need earlier signals or containment triggers.
- Have compliance requirements around ransomware resilience (CMMC, NIST IR-8374, HIPAA Security Rule, etc.).
- Operate in high-target verticals: Healthcare, Government, Higher Ed, Critical Infrastructure.
- Have experienced near-miss ransomware incidents or are seeking stronger lateral movement defense.

How Arctiq Layers In Value

1. Readiness & Design Services

- Ransomware risk assessment (gap analysis mapped to NIST IR-8374).
- Deception strategy design: aligning Mimic deployment with your threat model.
- Integration planning with existing EDR, SIEM, and identity stack.

2. Implementation & Tuning

- Mimic deployment & signal baselining.
- Deception tuning against threat emulation and red team exercises.
- Integration with Arctiq MDR and/or SOC services.

3. Ongoing Detection & Response

- Real-time monitoring of Mimic deception alerts within Arctiq's SOC.
- Tiered containment playbooks triggered via SOAR integration.
- Monthly ransomware threat intelligence briefings (sector-specific).

4. Post-Incident Analysis

- Root cause analysis of Mimic alerts that caught lateral movement.
- Adversary behavior mapping to MITRE ATT&CK.
- Executive reporting with risk reduction narratives.

Strategic Impact for Clients

✓ Earlier detection without more noise

✓ Strengthens compliance alignment with zero-trust and ransomware-specific guidelines

✓ Disrupts adversary workflows at the reconnaissance stage

✓ Turns every deceptive engagement into an intelligence opportunity

Arctiq + Mimic: Better Together

Mimic delivers surgical deception. Arctiq operationalizes it. Together, we help organizations:

- Detect ransomware operators before damage is done.
- Reduce dwell time to minutes.
- Translate deception into measurable risk reduction.

Disrupt ransomware before it spreads—partner with Arctiq and Mimic to turn your environment into a trap, not a target.

Book a Consultation