Case Study

Mid-Market Specialty Finance Firm Uses Optiv’s Incident Response to Recover from Breach

OVERVIEW
A mid-market specialty finance firm providing debt solutions to businesses in a variety of verticals needed support. The firm was in the final recovery stages from a recent security breach and navigating a change in management. They partnered with Optiv to deploy incident response (IR) solutions to handle the breach recovery. The breach provoked a desire for more proactive efforts in threat detection and response, however the security team did not have the bandwidth to accomplish this in-house.

Due to the firm’s small security team, 24x7x365 staffing was not feasible. The security team knew the answer would be a Managed Security Service Provider (MSSP) but needed to assess what level of service made the most sense for their business.

HOW OPTIV HELPED
Fortunately, the firm had Optiv’s IR services on retainer, allowing new management to get up to speed quickly, while avoiding any impact to daily operations. The firm drew upon Optiv’s cybersecurity expertise to drive policy changes leading to a more robust security program. Employing a co-managed Security Information and Event Management (SIEM) system enabled the client to rest easy knowing that false positives and low-level alerts would be resolved. Since Optiv was also responsible for managing system updates, the security team could reclaim valuable resources for other projects.

RESULTS
• True 24x7x365 coverage for all security and device alarms monitored by Optiv
• Reduction in engineering costs
• Smooth transition for new security team lead
• Day-to-day operations and bottom line escaped impact from the incident

INDUSTRY
Financial

CHALLENGES
• Limited in-house staff with no capacity for 24x7x365 support
• Ongoing recovery from a recent breach
• New Security Team lead joining in the aftermath of an incident
• Desire for more proactive detection and response

SOLUTION
• LogRhythm’s Co-Managed SIEM offering to provide 24x7x365 monitoring, triage and escalation of critical security events
• Carbon Black’s Managed Endpoint Detection and Response (MEDR) services to ensure the ability to detect, investigate and respond to threats
• Optiv Incident Response team to accelerate breach recovery

NEXT STEPS
• Develop a proactive ability to detect and respond to alerts
• Employ continuous penetration testing

Who secures your insecurity?
Optiv is a security solutions integrator – a “one-stop” trusted partner with a singular focus on cybersecurity. Our end-to-end cybersecurity capabilities span risk management and transformation, cyber digital transformation, threat management, cyber operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler and more cost-efficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are leading a completely new approach to cybersecurity that enables clients to innovate their consumption models, integrate infrastructure and technology to maximize value, achieve measurable outcomes, and realize complete solutions and business alignment. For more information about Optiv, please visit us at www.optiv.com.
©2019 Optiv Security Inc. All Rights Reserved.