SOLUTION BRIEF

SilverSky Managed Incident Response

Businesses continue to struggle with the ability to respond to security incidents, due to a lack of formal planning, preparation and resources.

Roughly 30% or organizations have established a mature incident response program.

However, an organization's speed and response time to an incident within the first 48 hours is one of the most critical elements in minimizing business disruption from an incident. The ability to effectively make decisions, rapidly enable resources and efficiently initiate response activities will ultimately determine an organizations overall success in navigating through an incident and minimizing downtime. According to the National Institute of Standards and Technology (NIST), there are four key phases that organizations need to consider when developing a mature incident response program:

Preparation
A plan must be in place, continuously updated and tested to effectively prevent and respond to events.

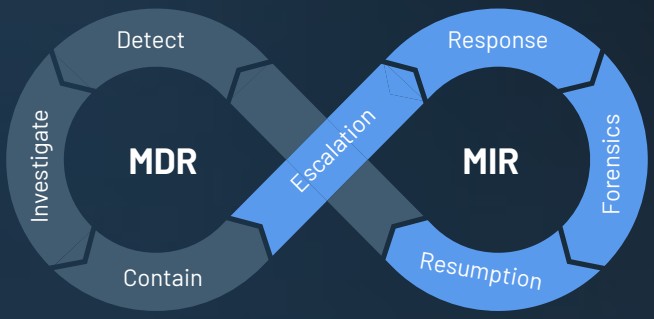
Detection and analysis
Security Operations plays a key role to detect and determine if an incident has occurred and its severity.

Containment and eradication
Having proper resources and processes to contain the event and resume business operations.

Post-incident recovery
A continuous improvement process involving all relevant parties with the goal of improving incident handling in particular.

It is critical that an organization develop a process that integrates their detection capabilities with their ability to respond and recover from breaches. All too often security operations are not in sync with incident responders and forensic resources resulting in critical time lost and prolonged recovery time.

That is why SilverSky has developed the managed incident response (MIR) service as an extension to the Lightning Platform managed detection and response (MDR) services. Together these two solutions provide a complete lifecycle service addressing all four critical phases of NIST's incident response maturity.



SOLUTION BRIEF

How It Works

SilverSky's managed incident response service works in conjunction with your existing SilverSky MDR to reduce the time to detect, respond and recover from cyber incidents.

The two services together combine all the key elements of incident response preparation, detection and analysis, containment and eradication and post incident recovery into one lifecycle solution. Tradition security operations centers alone are limited in the ability to provide full response and typically can only perform temporary isolation of an incident. While containment of an event is a critical step in the incident response process, there is still the need for response and recovery actions like identifying the root cause, remediation of event and recover of business operations. Our SilverSky MIR service was designed to pick up where traditional security operations ends. We provide integrated procedures and access to incident responders who work in tandem with SilverSky's security operations to assist you in recovering promptly from any incidents that may occur. Should you need more help or additional services, SilverSky has a full suite of scalable, managed security services you can leverage on-demand.

Service Overview

SilverSky will implement the following processes and service elements:

Preparation:

- ☑ Incident Response Plan Development
- ☑ Incident Response Tabletop Exercises

Detection Analysis:

- ☑ In the event of a formal incident requiring the assistance of a skilled 3rd party IR team, this will be provided through SilverSky's partnership with S-RM, a global incident response firm. The MIR service includes two components to reduce the timeframe of engaging S-RM Incident Response resources when an incident is declared.
  - IR retainer with 6 hours of Incident Response to be used as a fast start to receive assistance from S-RM
  - Pre-negotiated IR hourly rates

Containment and Eradication:
As an extension to your cyber incident response team, the S-RM team will assist in establishing standard process flows around detection, investigation, perform temporary containment, incident escalation, response, forensic and resumption processes.

Post Incident Recovery:
SilverSky will help maintain the incident response plan that aligns with the service by allocating a block of hours to review plans based on table top exercise results and specific incident concerns.

SilverSky's MIR stands vigilant to defend your business during an incident.

linkedin.com/company/silversky

twitter.com/silversky

www.silversky.com

SILVERSKY

1-800-234-2175

learn@silversky.com

3015 Carrington Mill Boulevard
Suite 400
Morrisville, NC 27560