

Incident Response (IR)

Overview

Cyber crime represents one of the most critical threats to businesses today. Attacks are so vast and complex that it has become impossible to detect every attack by hand. These attacks can cause downtime, or can create holes in system security for further breaches, and can eventually lead to financial losses, loss of credibility, or even jail time in extreme cases.

Incident Response (IR)

Incident Response ("IR") is initiated by or with the consent of the Customer upon the occurrence of a suspicious event or condition indicating a possible compromise of the Customer's digital security. A system alert, the Customer, or other indicators may signal this event or condition. Customers may purchase IR whether or not they have equipment installed in a SAVVIS Data Center and regardless of equipment components and architecture.

Incident Response Service Elements

The IR performed by SAVVIS will depend upon the nature of the security incident. SAVVIS will consult with the Customer to determine the most appropriate response. This may include:

- Site hardening.
- Modification of firewall and IDS rules.
- Modification of the OS security controls.
- Analysis of logs, system statistics and files.
- Collection of data and intrusion investigation.
- Collection of evidence and forensic analysis.
- Reporting and recommendations.

SAVVIS IR Team

Our Incident Response team is on call 24/7 by SAVVIS' world class IR Team for any potential activity. When an alert arrives, it is triaged by the SAVVIS Managed Security Team who will determine if your network and/or application host is under attack or has been breached. The IR Team will then immediately notify you and implement the incident response and cyber forensics plan created specifically for your business. SAVVIS Intrusion Detection Services are configured and installed per your specifications and are reviewed and updated on a semi-annual basis. Access to

ADVANTAGES:

- » Forensics and evidence collection expertise.
- » Can be used to assist with:
 - Analysis of logs, system statistics, and files
 - Development of a response plan
 - CIRT Training
 - Reporting
 - Liaising with law enforcement
- » Modification of security operations plans

your alert reports for the previous 60 days are provided via a secure web-based interface. Working with SAVVIS to monitor and manage your intrusion detection systems provides positive return on investment by augmenting your IT resources while relieving employees from 24/7 alarm monitoring.

For more information visit www.savvis.net or call 1-800-SAVVIS-1.

