UNISYS | Securing Your Tomorrow®

Unisys Incident Response Ecosystem

Cyber threats continue to become more sophisticated and intensify with each passing year. Organizations of all sizes face a variety of unique challenges and need to be prepared to respond when an incident occurs. The worst time to realize that you aren't as prepared as you need to be is during a breach. Without a proven incident response plan or strategy, critical decisions are being made without a coordination, priority or direction. This can lead to poor decisions being made that can affect the duration and impact of an incident. In the unfortunate case that your company suffers a breach, you need to be ready with a plan to address it quickly.

87% responded to at least one incident in the past year

50% reported a dwell time of less than 24 hours

53% of organizations are reporting their security operations centers (SOCs) as mature or maturing in their ability to respond

Source: 2017 SANS Incident Response Survey

A security incident is an imminent threat to your organization's information systems or network. The ability to provide an effective response to such a threat is crucial for any enterprise. Proactive engagement in IR policy reviews, table top exercises, and operational benchmarking can help improve your ability to respond before the incident occurs. When an incident does occur, having access to skilled resources to assist in the investigation and remediation is essential. Without additional support, operations teams are taxed with time-consuming investigative activities such as log collection and analysis. Planning ahead for burst resource capacity ensures that these response activities can be completed – without dragging your operations team from their day jobs. Planning ahead with proactive improvement and an emergency resource plan not only builds confidence in your IR capability, but it provides you with a defensible position with executive leadership that you've considered the possibilities of an incident and acted accordingly.

You can achieve this and more with Unisys as your trusted partner, ensuring that when you have an incident, you're prepared to take the appropriate action. Unisys Incident Response Ecosystem is an annual subscription service that provides organizations with a defensible position by proactively maturing the IR program and deploying incident handlers at a moment's notice. Unisys IR consultants work with your team on quarterly consulting engagements to refine your organization's IR plan, prepare your team to respond and improve your IR maturity.

If an incident occurs during the year, you can leverage our emergency response services to quickly bring skilled resources onsite to assist with time-sensitive response activities. The Unisys Incident Response Ecosystem provides up to 120 hours of onsite consulting, assisting IR efforts with services such as log review, data collection, patching and communications.

OPERATIONALIZE YOUR ORGANIZATION'S INCIDENT RESPONSE CAPABILITY

PRACTICAL VALUE

- 120 Hours of on-site incident response emergency support
- Quarterly incident response activities focused on preparation and response to an event

DEFENSIBLE POSITION

- Assurance of Unisys as a Safety Net
- Proactive incident response activities providing continuous improvements in security

In addition, Unisys offers one of the following proactive consulting activities each quarter, to continually improve and mature your IR capability:

Incident response policy review - Review of existing incident response documentation against industry best practices to identify gaps and provide recommendations to mitigate identified issues.

Endpoint assessment - A phase-based methodology to assess the present state of the endpoint security environment, identify unknown threat activity, and suggest remediation.

Threat hunting - Leveraging industry standard best practices to detect suspicious or potentially malicious activity within the network environment.

Table-top exercise - Onsite scenario driven exercise designed to help organizations improve their cyberattack preparedness and resilience through practical exercise and experience.

Consulting gap assessment - Delivers maturity and capability score based on evaluation of an organizations existing security program.

Operational benchmark - Assessment of an organizations operational readiness to detect and respond to modern cybersecurity threats.

For a robust security posture contact **security@unisys.com** or visit **www.unisys.com/mss**

For more information visit www.unisys.com

© 2018 Unisys Corporation. All rights reserved.

Unisys and other Unisys product and service names mentioned herein, as well as their respective logos, are trademarks or registered trademarks of Unisys Corporation. All other trademarks referenced herein are the property of their respective owners.

Printed in the United States of America 09/18 18-0295