INCIDENT RESPONSE CHECKLIST

Are you **prepared**?

Many organizations are not prepared for an incident. They have an understanding of some basic steps they may need to perform, but are not ready when an incident occurs.

Having a **plan**

Verbal or "tribal" knowledge is a common practice for organizations to base their response efforts on. Documentation is not in place, and when an event occurs response efforts are disorganized at best. Organizations must have a plan and document that plan. This plan should be reviewed regularly and upon any major changes to personnel and/or the infrastructure. Specific incidents should also have developed and tested playbooks for planned execution. These playbooks should include common scenarios that the organization may face.

Having the **tools**

All organizations have limited budget to protect their environment, so having solutions and controls in place that provide as much coverage for both daily operations and evidence for incident response is vital.

☑ Log Aggregation

This most common solution is part of SIEM. Many organizations will utilize a trusted third-party to execute on this to provide the man-power needed to monitor and respond to events that are identified and continuous review and improvements to the solution.

☑ Firewalls

Firewalls with functionality around data loss prevention (DLP), IDS/IPS, etc. have become the normal for organizations. The licensed functionality and their configurations are important to response capabilities. The configurations can allow for better detection of suspicious/malicious attacks and containment capabilities.

☑ Additional Security Stack

While not a commonly implemented solution or control, some SIEM and firewall solutions are starting to track this information. While not as useful as a full packet capture, it provides responders with information usable by investigators about network traffic and service use.

☑ End-Point Solutions

From anti-virus, anti-malware, and end-point detection and response (EDR) solutions, implemented capabilities are improving to protect end-users and servers against the latest known malware. Many of the latest anti-malware and EDR solutions will also tout their ability to protect against variants of known malware or zero-day attacks.

☑ Packet Flow

While not a commonly implemented solution or control, some SIEM and firewall solutions are starting to track this information. While not as useful as a full packet capture, it provides responders with information around network traffic, service use, and information usable by investigators.

World Headquarters
7311 West 132nd St, Suite 305
Overland Park, KS 66213

CT Office
1 Hartfield Blvd, Suite 300
East Windsor, CT 06088

UK Office
A8 Ively Road, Farnborough
Hampshire, GU14 0LX, UK

Contact Us
+1 800-940-4699
+44 800-358-4915
info@foresite.com

FORESITE