INCIDENT RESPONSE
POLICY & PLAYBOOKS

ANTICIPATE. IMPROVE. PREPARE.

The adversary evolves--you must as well. Improve your organization's incident response operations by standardizing and streamlining processes with this engagement. CrowdStrike Services analyzes your current plans and capabilities, then works with your team to develop standard operating procedure "playbooks" that guide your activities during incident response.

The playbooks CrowdStrike Services prepares are relevant to your particular organization. Additionally, we can create playbooks that are completely specific to your organization, on request.

Our incident response policy and playbooks creation can be packaged with other proactive assessments, lowering overall cost with delivery efficiencies.

HOW WE DO IT: DATA COLLECTION, ANALYSIS AND DISCUSSION

We start with a gap analysis between your current Standard Operating Procedure (SOP) and the incident response plan we would expect to find in your organization.

We then create an incident response plan framework that includes SOPs relevant to your operations, and identify and fill gaps in areas of response that you have not yet defined.

Certain playbooks are developed for your organization based on our experience conducting incident responses across different verticals. During the playbook creation process, we utilize our knowledge of which parts of your environment will be the most relevant to an attacker and defender.

To find opportunities for improvement, CrowdStrike Services first reviews your existing incident response plans, related documentation and standard operating procedures. A review of that documentation enables us to prepare questions and discussion points.

Before meeting with your team, we review relevant IR process documentation and response team member resumes.

This effort will reveal much about pre-existing security and incident response processes within your organization. For example, you may send us information about your processes and architecture, your people and tools structure, and any penetration test reports or previous assessments your organization may have conducted.

EXAMPLES OF DATA AND DOCUMENTATION WE MAY REVIEW INCLUDE:

- Customer requirements
- Security operating plans
- Team member resumes
- Firewall rule sets
- Network intrusion detection configuration design and installation
- Active Directory, Open Directory or LDAP architecture and object configuration

CrowdStrike Services' review of this material enables us to understand the basics of your organization's defensive posture. With this knowledge, we construct an agenda of discussions with your personnel. The document review process takes about ten business days. During that time, we determine the people on your team we need to interview and will coordinate a schedule of interviews at your site. These staff discussions take one or two consecutive days. We usually interview about six to eight groups over the course of two days on site – if we need more time, or to interview more people, we will advise you.

Following our documentation review and associated interviews, we will construct preliminary drafts of the in-scope playbooks, then schedule time to walk through these process flows with your team during a white-boarding session. Upon completion of these sessions, we will finalize the playbooks and deliver them to you.

ACTIONABLE GUIDANCE AND DELIVERABLES

In addition to status updates and meetings, CrowdStrike Services provides:

- Up to five incident response plans or playbooks
- Findings from our analysis

LEARN HOW CROWDSTRIKE STOPS BREACHES: VISIT WWW.CROWDSTRIKE.COM/SERVICES

Speak to a representative to learn more about how CrowdStrike Services can help you prepare for and defend against targeted attacks.

CROWDSTRIKE

LET'S DISCUSS YOUR NEEDS
Phone: 1.888.512.8906
Email: sales@crowdstrike.com
Web: http://www.crowdstrike.com/services

Ver: 04-08-16