Mandiant has been at the forefront of cyber security and cyber threat intelligence since 2004. Our incident responders have been on the frontlines of the most complex breaches worldwide. We have a deep understanding of both existing and emerging threat actors, as well as their rapidly changing tactics, techniques and procedures. The Security Program Assessment draws on this expertise to deliver tailored, actionable recommendations that will improve your security posture, reduce risk and minimize the impact and cost of a security incident.

Overview
We combine industry standards with our expertise and intelligence to evaluate your program across 10 critical security domains. During the assessment, Mandiant consultants review documentation, perform interviews and facilitate interactive workshops to understand your organization’s current security maturity and ensure future improvements are driven through functional collaboration. We deliver strategic and tactical recommendations, along with an implementation roadmap, to meet your organization’s short- and long-term security goals.
WHAT YOU GET

- **Executive Summary:** A summary of findings and recommendations along with key insights.
- **Observations and Gap Analysis:** Using industry frameworks as a benchmark, the gap analysis identifies domains that need further development and provides a maturity development plan to help strengthen security posture and reduce risk.
- **Security Program Roadmap and Recommendations:** A strategic and tactical plan with recommendations on sequencing and prioritization for enhancing security maturity across all 10 domains.
- **Frontline Insights:** A deep understanding of global attacker behavior through extensive incident response experience and visibility into actionable threat intelligence.

**Our Approach**

We conduct an in-depth evaluation of the organization’s information security programs across 10 critical security domains, each mapped to industry standards and frameworks. After our in-depth analysis and workshops, we provide findings prioritized into short-, medium- and long-term recommendations designed to improve the organization’s security posture, based on its risk profile and level of security maturity at the time of assessment.

Recommendations will include guidance on how to fully utilize existing tools and resources as well as suggestions for new tools and processes that can be implemented to improve security posture and reduce risk.

**Assessment Process**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Step 2</th>
<th>Step 3</th>
<th>Step 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation collection, review and analysis</td>
<td>Interactive workshops and executive meetings</td>
<td>Develop report and recommended execution strategy</td>
<td>QA and deliver report</td>
</tr>
</tbody>
</table>

| | 1 WEEK | 2 WEEKS | 2 WEEKS | 1 WEEK |

To learn more, visit: [www.FireEye.com/services](http://www.FireEye.com/services)