CASE STUDY

MANDIANT®
A FireEye® Company

Large Automobile Maker Enriches Its Security Posture

Response Readiness Assessment in action

CHALLENGE

The automobile industry experiences frequent cyber attacks that target technology-related intellectual property. During these attacks, vehicle owners' personal identifiable information is also targeted.

One large automobile manufacturer understood the reality of today's cyber landscape in which threat actors are persistently advancing their tactics, techniques, and procedures (TTPs). This manufacturer recognized the importance of proactively and periodically assessing its security team's ability to effectively detect and respond to targeted attacks.

Response Readiness Assessment
The FireEye Mandiant Response Readiness Assessment evaluates an organization's incident response (IR) capabilities — including their security operations center (SOC) and IR functions. The assessment compares IR capabilities against leading practices to identify gaps and determine how best to improve program processes, staff skill sets, and technology moving forward.

IR process evaluation triggered security program improvements
After the automobile manufacturer experienced a major breach, its executive leadership team determined their security program had substantial gaps across their people, processes and technology. Since they represented a prominent brand, executives realized their organization would remain a significant attack target.

FireEye Mandiant was called on to evaluate the manufacturer's incident response program and to provide best practice recommendations for improvement. To do so, Mandiant experts focused on six core security capability areas (Fig. 1) — governance, visibility, communications, intelligence, response and metrics — needed to achieve an effective and sustainable incident response program. Enhancements to these six core areas would improve the security team's response time by helping them quickly and properly detect, investigate and contain attacks performed by sophisticated threat actors.

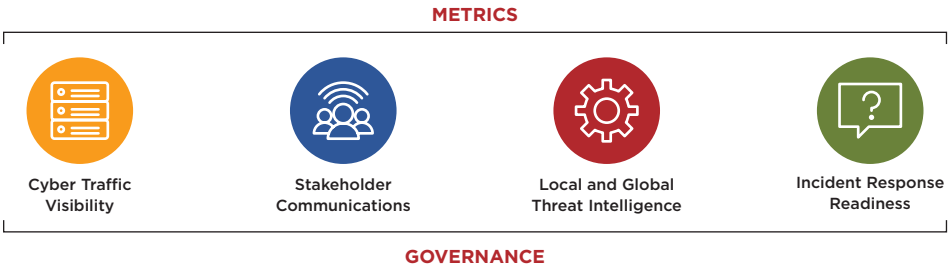

Figure 1. Six core capabilities model.

FireEye

Critical capability gaps uncovered
During a three week engagement, Mandiant consultants uncovered operational gaps across all six capability areas. They started the assessment with a review of client-provided documentation defining the organization's existing IR processes and playbooks, crisis communications plan, internal security compliance policies, network diagrams and organizational charts.

They conducted a Tabletop Exercise with the client's security leadership team. This three-hour workshop tested the team's incident response plan through scenario gameplay. Participants were challenged with multiple scenarios based on real-world experience in a roundtable environment. As a result, inefficient response processes across the six core capability areas were identified.

- **Governance:** The responsibilities of an incident response team (IRT) must align with the incident response function's mission statement and business goals. The manufacturer's IRT roles and responsibilities did not, and fell short of supporting the organization's need for enhanced security coverage. At times, the IRT was even tasked with performing activities outside of the mission's scope, which hampered the team's ability to focus on incident detection, investigation and containment efforts. The organization also lacked a 24/7 SOC which would have provided a unified and continuous operations capability.
- **Visibility:** To quickly detect and scope incidents, an organization must maintain full visibility of threats across their network 24/7. This automobile manufacturer had limited threat visibility because it only used endpoint antivirus detection software rather than more advanced endpoint detection and SIEM technologies.
- **Communications:** A robust response plan depends on the security team sharing information with the right external and internal entities, at the right time. This client's security program was operating without a formal escalation matrix in place, which resulted in a lack of formalized security communications to key stakeholders in the event of an incident. While the organization maintained a solid crisis communications plan (to restore operational normalcy), a cyber security communications plan was missing.
- **Intelligence:** A detailed understanding of attacker capabilities, techniques and intent dramatically improve response quality and speed, and enable an organization to better anticipate an attacker's next move. The client's security team lacked dedicated personnel to monitor the local and global threat landscape. This security team also lacked the integration of intelligence into their operations and incident response processes, which would improve detection and response capabilities.
- **Response:** A successful incident response incorporates people, processes, and technology to detect, investigate, contain and remediate security incidents. This client lacked technological mechanisms to promptly detect incidents that might affect critical assets and needed formal processes, such as playbooks, that would prescribe methodologies for an efficient and repeatable response based on incident categories.
- **Metrics:** Metrics help organizations measure how efficiently they respond to incidents. In this case, the client did not have a performance metrics strategy that included formal processes to measure the success of its security program. The manufacturer had no way to evaluate whether its IR capability aligned with its defined functional IR and overall business missions. For example, data logs to help detect network compromise across all phases of the attack lifecycle were missing, and never considered a formal requirement.

Actions taken
After Mandiant consultants completed the Response Readiness Assessment, a recommendations report was delivered to the C-suite, outlining a two-year custom roadmap with areas of improvement across the organization's security operations and IR capabilities — some of which were implemented shortly after this engagement:

1. **Implemented 24/7 Global Security Monitoring:** To improve the organization's governance capability, the manufacturer aligned its IR mission with corporate objectives and implemented a "follow the sun" operations model. The main security operations center was located in one time zone, and now has operations in three separate time zones, employed by staff members who possess a clear line of responsibility and reporting structure.

   The client implemented a formal case management system from detection to closure and moved from manual to automated processes that ultimately reduced staff time spent on tracking incidents. This allowed them to re-focus efforts on containment and remediation actions.

   A SIEM was implemented to aggregate and correlate logs from disparate technologies to support incident response investigation and containment efforts.

2. **Enabled Prescriptive Execution:** The client's response capability was enhanced through the implementation and adoption of security incident playbooks. These playbooks cover targeted attacks, malware, phishing, compromised credentials, compromised systems, intentional insider threat and security policy violations.

The automobile manufacturer's security team used the playbooks to guide specific cyber breach response processes, including identifying affected systems within the network, investigating attacker execution, capturing alerts, applying basic and dynamic analysis and deploying escalation procedures.

3. **Engaged Intelligence:** Mandiant experts worked with the client to formalize their threat intelligence capability. This involved implementing best practice processes that elevated the manufacturer's intelligence gathering and categorization processes for indicators of compromise (IOCs). Once the security team understood how to properly assess the fidelity of collected cyber threat intelligence and apply it, their security controls were modified to create a proactive defense plan.

4. **Gained Visibility:** Before the assessment, the client lacked the ability to consistently monitor unique endpoint activities, such as abnormal workstation-to-workstation communications, executed programs and invoked processes. After the assessment, an endpoint detection and response (EDR) tool was deployed to provide visibility into endpoint activities across the organization.

5. **Instituted Success Metrics:** The client carefully implemented a performance metrics program to measure security operations and incident response effectiveness, referred to in the industry as DRAIN/CVR. These metrics (Table 1) allow the client to make informed solution investment decisions to reduce the overall time to remediation — a critical metric that measures how long it takes from the detection of an incident to remediation.

6. **Implemented Reporting System:** Mandiant consultants helped the client build a closed-loop reporting system of threat intelligence findings. Before the assessment, the security team could not reach or properly work with other business functions to effectively resolve cyber events. After exploring the differing needs of various business partners (internal functions and external agencies), Mandiant experts created a stakeholder analysis framework designed to improve engagement by highlighting how threat intelligence could be used across the organization. These newly found partnerships and processes ensured key stakeholders were built into the formal cyber communications plan moving forward.

Table 1. Description of performance metrics.

Metric type	Metric	Purpose
Detect	Measure detection capability effectiveness	Determines if the detection capabilities are appropriate
Review	Time from detection to analyst review	Assists with determining if staffing levels are appropriate
Analyze	Time to analyze the incident	Determines if the IRT has the right expertise
Identify	Time it takes to identify affected assets	Determines the accuracy of asset inventories
Notify	Time to notify contacts	Tests communication processes to stakeholders
Collect	Time to collect live response data	Determines if the right technologies are established for data collection
Validate	Time to validate an intrusion	Assists with identifying if personnel have the right skill sets
React	Time to initiate response efforts	Determines if the remediation processes are consistently applied and at the right level based on the identified incident

Conclusion

After suffering a harmful breach, this automobile manufacturer committed to maturing its cyber security posture and improving its incident response capability. To do so, they turned to FireEye, launching a series of Mandiant Response Readiness Assessments. These assessments and resulting roadmaps facilitated the deployment of advanced IR capabilities, enabling effective responses to advanced persistent threats (APTs).

Aligning security operations and incident response with corporate objectives greatly benefited the organization. The manufacturer significantly advanced security monitoring capabilities around the clock, integrated threat intelligence into their daily operations, developed formal metrics to monitor and mature their incident response processes, implemented SIEM technology to enhance incident analysis, improved mechanisms to track incidents across the full attack lifecycle and developed crucial stakeholder communication plans.

These improvements received a highly positive appraisal rating from the organization's executives. They continued to improve their response capability year-over-year by hiring Mandiant consultants to conduct recurring Response Readiness Assessments each year (Fig. 2). The manufacturer's advancements in security maturity took several years of dedication and effort by its cyber security staff, executive management and the board.

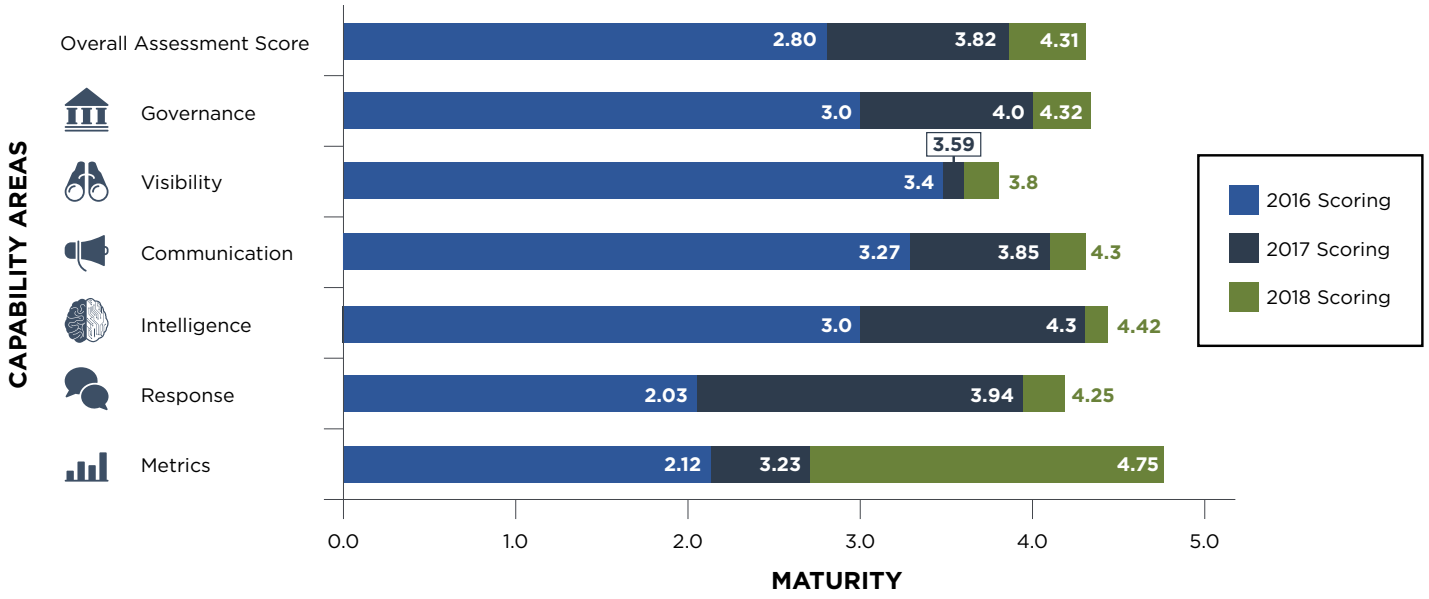

Figure 2. Measured improvement of six capability areas.

To learn more about FireEye, visit: **www.FireEye.com/services**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FireEye