Enterprise Strategy Group by TechTarget | MANDIANT NOW PART OF Google Cloud

The Defender's Advantage Self Assessment Results

Organizations combat cyber adversaries in their own environment, which gives them an intrinsic defender's advantage. However, security teams often struggle to capitalize on this due to lack of resources and expertise required to activate the six critical functions of cyber defense.

Cyber security leaders and practitioners alike must learn how to optimize and activate the six critical functions to ensure their security program can effectively prevent and rapidly repel inevitable attackers.

Here are the results from your assessment.

The Defender's Advantage: <confidenceScore_defendersAdvantage>

The Defender's Advantage is the concept that organizations are defending against attacks in their own environment. This provides a fundamental advantage arising from the fact that they have control over the landscape where they will meet their adversaries. Organizations struggle to capitalize on this advantage. They often don't have a good understanding of who and what they are defending against and lack understanding of their organizational landscape and their capabilities to disrupt or minimize the impact of a breach. Without this understanding, cyber defenses can be disorganized and ineffective at truly protecting the business.

The negative impacts of poor cyber defense capabilities include:

- Increased vulnerability to attacks from not knowing the active threats to their organization.
- Lack of confidence in the ability to manage cyber risk.
- Disorganized response to compromise, increasing the cost to the business in money and reputation.
- Duplicative efforts by cyber defense functions creating confusion and operational waste.

With coordinated cyber defense efforts, guided by intelligence, organizations can understand their risks and improve their capabilities to reduce the impact of attacks. This increases confidence that the Cyber Defense organization can enable the business to continue operating in the face of threats.

Threat Intelligence: <confidenceScore_threatIntelligence>

Many organizations do not know how to operationalize intelligence or use it inconsistently. Even though they subscribe to many intelligence sources, they don't know how to use the information to determine who is attacking them and how, if they are vulnerable to the attacks, and the business impact of an attack. Additionally, the full value of the intelligence is diminished if not properly utilized by other cyber defense functions.

The negative impacts of haphazard use of threat intelligence can include:

- Ineffective whack-a-mole approach to defense driven by headlines.
- Implementing tools without a plan for realizing the benefits of them.
- Time and resources wasted defending against the wrong threats.

Organizations require a clear understanding of the threats their specific organization faces and the business risk of a compromise. Threat intelligence should guide cyber defense and be delivered in a consumable way, utilized by each critical function to execute their activities. This guidance on prioritized actions has a large impact on reducing risk to the business. An intel function should also include a continuous feedback loop from the other critical functions and industry inputs to evolve their Threat Profile to keep up with active attackers.

Steps to achieve an effective Threat Intelligence function include:

1. Acquire the right Threat Intelligence feeds.
2. Understand how to provide that intelligence to each function for their specific consumption needs.
3. Create a Threat Profile that takes into account the threat landscape (active attackers), vulnerabilities in their own environment, business risk and impact of a compromise.

Command and Control: <confidenceScore_commandControl>

Organizations often have siloed cyber defense teams that are not tied into the business. Additionally, each cyber defense team has inconsistent processes and procedures that can overlap or conflict with other functions. The result is the lack of a common front against attackers causing the inability to provide a measured response in the event of a breach.

The negative impacts of a disjointed Command and Control function include:

- Chaos during a breach resulting in longer response times and larger impact to the business.
- Confusion created by duplicate or conflicting processes.
- Information not being shared between groups or rolled up to business stakeholders in a coordinated effort.

By creating a central Command and Control function, organizations can provide coordinated and optimized processes and procedures to increase cyber defense team efficiency. Synchronized activities reduce duplicate or conflicting efforts during a breach as well as during ongoing operations. Additionally, the centrally organized function provides a consolidated view of how the cyber defense organization is performing and their ability to protect the business.

Steps to achieve an effective Command and Control function include:

1. Define the mission of your Cyber Defense team and socialize it.
2. Establish a Command and Control team to standardize processes.
3. Document communication plans for breaches as well as day-to-day operations.
4. Outline and gather metrics that matter to drive changes that will best benefit the business operations and innovation.

Hunt: <confidenceScore_hunt>

When organizations focus hunt efforts on single indicators of compromise (IOCs) they can miss the big picture of threat campaigns targeting their business. Additionally, when hunt teams work in a silo they are not realizing the value of broader findings from other cyber defense functions, specifically threat intelligence and respond). This can be caused by the lack of skilled resources with experience carrying out properly structured hunt activities or over-burdened staff that treat hunting as an afterthought activity .

The negative impacts of an unstructured hunt function include:

- Wasted time hunting for general threats that are not relevant to the business.
- Inefficient hunt activities due to lack of defined hunt process.
- Hunt outputs that are not utilized by other cyber defense functions because that communication plan has not been established

Optimized hunt capabilities focused on threats that matter to the organization. The activities effectively identify current or past compromise to guide incident response or mitigation activities. Additionally, hunt teams can increase the value of their activities

when the outputs are leveraged by other cyber defense functions to speed investigations and reduce the impact of the exposed compromise.

Steps to achieve a fully leveraged Hunt function include:

1. Develop a Threat Hunting Program and Processes with documented inputs and outputs.
2. Define how the output of hunt activities will inform the other functions of Cyber Defense.
3. Leverage automation to perform repetitive hunt activities.
4. Fill gaps in threat hunting skills with external expertise.

Detect: <confidenceScore_detect>

A common fear of cyber defense organizations is missing security incidents that will have a high financial cost and negative business impact if a breach occurs. The fear is rooted in overwhelmed analysts and part-time monitoring efforts. Additionally, some organizations are overly invested in tools that are not delivering the promised visibility and high-value alerts and/or are struggling to integrate them into their existing environment.

The negative impacts of an ineffective Detect function include:

- Analysts are overwhelmed with alerts and become blind to alerts that matter.
- Hiring more SOC analysts increases cost to the business
- Overworked SOC team and personnel churn

Organizations can decrease the fear of missing incidents by allowing software to analyze all alerts and events at machine speed. This can increase the value of existing controls in the environment by removing the need to tune them down to meet analyst capacity. Will less noise distracting analysts, they are better able to focus on higher-level tasks increasing job satisfaction and morale leading to increased staff retention.

Steps to achieve an efficient Detect function include:

1. Leverage automation to and reduce unattended alerts by automatically scoping alerts for further investigation while suppressing false positives
2. Reduce security engineering burdens with multi-sourced alert investigations derived from your existing security sensors.
3. Prioritize incident investigations based on asset and account criticality along with attack stage progression.

Respond: <confidenceScore_respond>

Organizations are often notified by an external party that they have been compromised (M-Trends 2022 https://www.mandiant.com/m-trends). When evidence of compromise is identified, organizations without an updated and practiced incident response plan are forced to move quickly with an improvised response plan. Without the proper preparation and experience the tendency is to jump to remediation efforts in misguided attempts to stop the breach.

The negative impact of an immature respond function include:

- Delayed response initiation without a proper process for handling external breach notification.
- Lengthened containment and remediation efforts due to uncoordinated remediation and premature remediation actions
- Organizations left vulnerable to repeat compromise due to incomplete remediation efforts.

Ultimately, organizations need to be capable of minimizing the financial impact and reputational damage of a breach and quickly reestablish business operations after a disruption. A mature respond function can provide this to the business and fully eradicate the threat from the environment to avoid repeat compromise.

Steps to achieve a strong respond function include:

1. Develop a robust incident response plan and update it regularly.
2. Repeatedly test the plan through executive and technical tabletop exercises mimicking different real-world scenarios.
3. Establish incident response retainers so you have experts on speed-dial to help your response efforts.

Validate: <confidenceScore_validate>

Organizations falsely believe that implementing tools equals increased maturity and protection. Without validating controls, they cannot verify they are providing the expected value. If organizations do perform validation, they often fail to repeat validation activities that are aligned with the latest threats from the industry and business specific inputs from what the other cyber defense functions are seeing. Furthermore, they forget that their people are a major contributor to their effectiveness, and their capabilities must be validated as well.

The negative impacts of an incomplete validation function include:

- False sense of security especially at the CxO/Board level if they are only being shown metrics around tooling or event volumes.
- Gaps in security controls leaving the organization vulnerable to attack where they thought they were protected.
- Staff and procedures that fail during a major incident.

Organizations that are confident in their ability to defend the organization and effectively respond to compromise with their existing controls and operations can provide objectively tested and measured validation of the effectiveness of security controls and their value. They can identify vulnerabilities and configuration issues that are targeted by attackers that are not covered by their controls and ensure their staff is ready to perform the necessary response procedures for varied attack scenarios.

Steps to achieve a strong validation function include:

1. Implement continuous security validation to test efficacy and value of security controls.
2. Perform regular penetration testing and red team exercises on networks, applications, and critical assets.
3. Validate your team's capabilities through virtual simulations of real attack scenarios.

Conclusion

Mandiant helps to accelerate cyber defense transformation through improved processes and technology alignment that uplevel threat detection, containment and remediation capabilities. Our cyber defense expertise helps you mature your organization across cyber defense development and operations, executive services and process development. Our experts also validate the effectiveness of your security program and provide hands-on support to implement critical changes and best practices for functional/staff readiness.

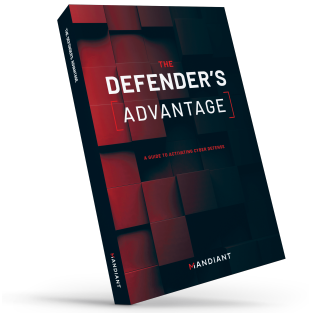
Mandiant Consulting helps organizations get back to business after a security incident. They apply their frontline expertise to help organizations transform their cyber defense capabilities to mitigate threats and reduce business risk - before, during and after an incident.

Additional Resources

No matter the level of confidence an organization has in its cyber defense capabilities, the first step to moving forward has proven to be a Mandiant Cyber Defense Assessment.

Mandiant delivers this assessment by performing the following actions backed by industry best practices and frontline expertise:

- Documentation review of incident response, threat hunting, and threat intelligence plans and playbooks
- Cyber defense workshops and skills matrix exercises with internal stakeholders to understand existing people, process, and technology capabilities
- Analysis of critical log samples to validate configurations for effective threat detection and response
- Tabletop exercises to assess end-to-end response actions and incident-related decision-making
- Simulated attacks to assess the effectiveness of threat detection controls mapped against the MITRE ATT&CK framework



For more in-depth information and guidance on the six critical functions of cyber defense, download a copy of our award-winning book, **The Defender's Advantage**.

Mandiant
833.3MANDIANT (362.6342)
info@mandiant.com

MANDIANT
NOW PART OF Google Cloud