Carbon Black.

WHITE PAPER

A GUIDE TO ASSESSING SECURITY MATURITY

PRESENTED BY COALFIRE

DOUG HUDSON
JASON MACALLISTER
MANDY POTE

COALFIRE

North America | Europe
877.224.8077 | info@coalfire.com | Coalfire.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

WHY DOES CYBERSECURITY MATTER?

Cybersecurity is an unavoidable part of daily business operations for organizations of all sizes and industries. As reliance on information technology expands, so does an organization's exposure to malicious actors. Hackers with sufficient capability and motivation can exploit vulnerabilities to breach the confidentiality of sensitive data, damage the integrity of information systems, and disrupt the availability of business operations. A cybersecurity breach can cost an organization millions of dollars in end-user productivity loss, repair of IT infrastructure, reputation damage, system downtime, lawsuits, fines, and regulatory actions.

To better guard against cybersecurity threats, organizations must consider their cybersecurity program as a key component to their business strategy. Organizations should leverage one of many available cybersecurity frameworks to assess maturity, identify gaps, and develop strategies to mitigate and manage their risk in accordance with their risk tolerance. While impossible to completely eliminate the risk of cybersecurity threats, an effective cybersecurity framework provides organizations a roadmap for protecting their key assets.

NIST CYBERSECURITY FRAMEWORK (CSF) OVERVIEW

What Is NIST CSF?

The National Institute for Standards and Technology (NIST) published version 1.0 of their Cybersecurity Framework (CSF or Framework) in February 2014 in response to Executive Order (EO) 13636 as an effort to improve cybersecurity of critical infrastructure. This Framework has since been adopted by organizations in all industries as a guideline for managing cybersecurity-related risks. NIST released its most current version 1.1 of the Framework CSF in April 2018.

Why Use NIST CSF?

Although the Framework is voluntary, it is a highly recognized platform for assessing and managing cybersecurity risks. Each version of the Framework is subject to a public comment period where cybersecurity experts in various industries provide feedback and improve the Framework to better meet the objectives of a mature cybersecurity program. The Framework assists organizations in identifying, understanding, managing, and reducing risks to cyber-attacks. NIST provides a common language for addressing and understanding cybersecurity risk management, making it especially helpful for communicating risks to stakeholders. Establishing clear lines of communication to upper-management is an essential first step for incorporating cybersecurity into an organization's overall mission.

How Does NIST CSF Assess Maturity?

The NIST CSF establishes a Framework Core to help organizations easily assess their current cybersecurity maturity against five security Functions: Identify, Protect, Detect, Respond, and Recover. Each Function consists of various Categories and Subcategories that break the Functions into prescriptive technical activities or "controls."

Each Framework Function represents a "slice" of an organization's cybersecurity management "pie." Only when considered together do they represent a holistic approach to managing security risks. An organization

Figure 1: NIST CSF Functions

can assess their cybersecurity environment against all five Functions and the respective Categories to build a current profile. The current profile indicates what the organization does well, as well as reveals control gaps that should be addressed and remediated. From there, the organization can prioritize resources to remediate vulnerabilities to achieve a target cybersecurity state.

By leveraging a standard maturity model, such as the Capability Maturity Model (CMM), an organization can determine their current maturity level against the NIST CSF Functions. The CMM maturity levels provide a benchmark rating method, which enables an organization to determine their capability and compare their capabilities to competitors or the industry.

CAPABILITY MATURITY MODEL (CMM) OVERVIEW

What is CMM?

The CMM is a standard maturity model solution used by organizations and governments for over 25 years to identify capability gaps. The CMM was originally developed for the Department of Defense as a tool for assessing a contractor's capability to implement a contracted software project. Although initially designed for software development, the CMM is easily adopted to assess maturity against any business function, including cybersecurity.

How Does CMM Assess Maturity?

CMM divides maturity into five distinct levels: Initial, Repeatable, Defined, Managed, and Optimized. The model provides a continuum across five levels, where Level 5 represents the pinnacle. The figure below depicts each of the levels and the associated characteristics:

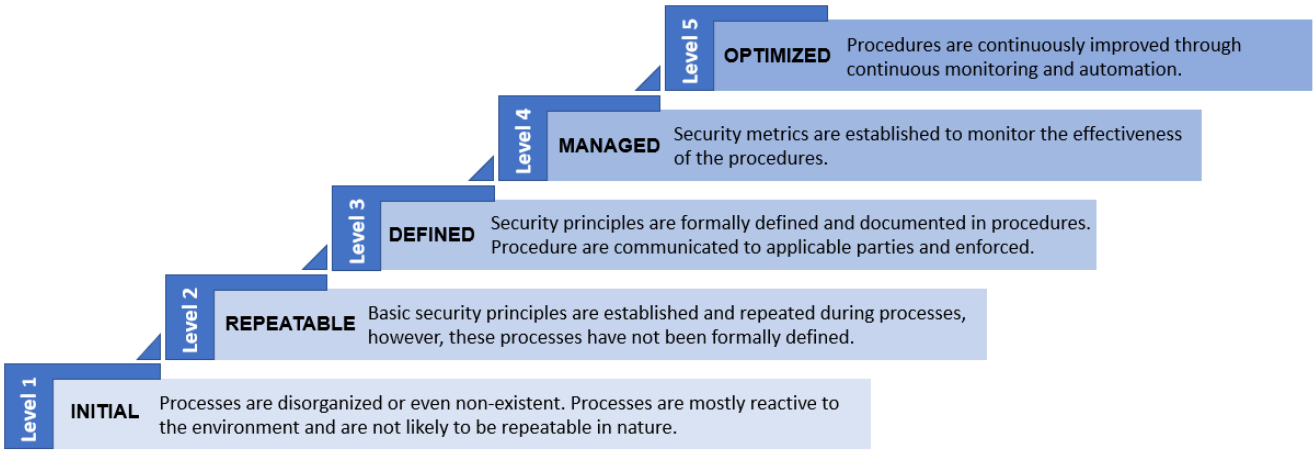

Figure 2: CMM Levels

As an organization improves its people, processes, and technology, it moves up the maturity levels. If assessing against cybersecurity functions, organizations sustaining advanced levels of maturity typically experience reduced risk to cyber-attack and compromise.

ASSESSING CYBERSECURITY MATURITY

Utilizing the chart below, an organization can align its cybersecurity capabilities against each of the NIST CSF Functions to produce a representative maturity rating.

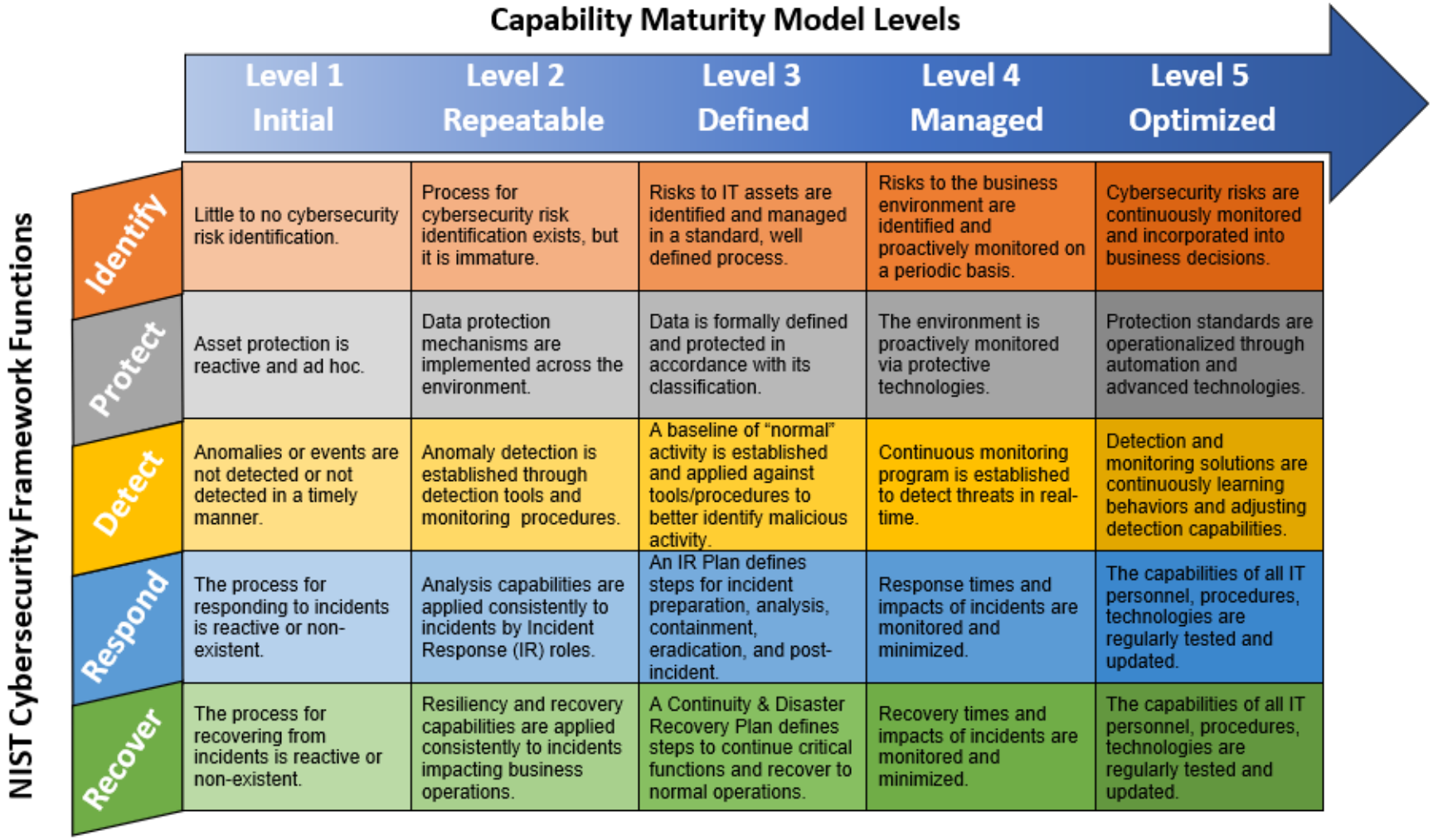

Figure 3: Assessing Cybersecurity Maturity

IMPROVING CYBERSECURITY MATURITY

A CONSOLIDATED APPROACH

Once the current maturity level is established, an organization can begin to develop strategies for improving their cybersecurity maturity. To succeed in improving to the next level of cybersecurity maturity, an organization must take a holistic approach to where and how they invest time and resources.

A cybersecurity roadmap must include the three elements for successful organizational transformation: people, process, and technology. Neglecting one or two will slow cybersecurity maturity improvement and could introduce vulnerabilities in the cybersecurity environment.

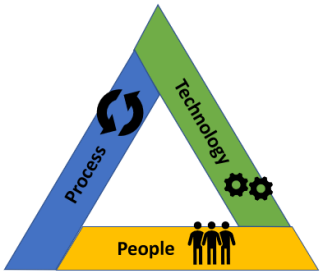

Figure 4: PPT Triad

The following section focuses on the "Technology" portion of the triad and describes how endpoint security technologies applied to the NIST CSF can improve cybersecurity maturity. It is important to keep in mind that while endpoint security technologies are effective in improving cybersecurity posture, the elements of "People" and "Process" are also essential for a mature cybersecurity program.

ENDPOINT SECURITY TECHNOLOGIES

Why Is Endpoint Security Important?

Endpoint security protects an organization's endpoint devices (e.g. workstations, mobile devices, tablets, servers, etc.) against threats and vulnerabilities (both internal and external). Attacks on endpoints attempt to compromise the confidentiality, integrity, and availability of information and IT assets in order to compromise or exfiltrate sensitive information and data. These attacks can lead to reputational and financial damage to organizations.

According to the *2018 State of Endpoint Security Risk*[1], sponsored by Barkly, threats to endpoints have increased at an alarming rate. In 2018, 64% of respondents confirmed their company experienced at least one successful attack on their endpoint(s) that compromised sensitive data and/or their IT infrastructure.

The cost of responding to and recovering from a successful attack on an endpoint has increased from an average of $5 million to $7.1 million per attack. These costs are attributed to end-user productivity loss, theft, system downtime, damage and repair of IT infrastructure, brand damage, lawsuits, fines, and regulatory actions.

Cybersecurity with Endpoint Security

Advanced endpoint security technologies, when combined with the computational power and operational efficiency of the cloud, provides an improved proactive alternative to traditional anti-virus solutions for protecting threats. As part of a comprehensive security program designed to reduce enterprise risk, organizations should consider leveraging an endpoint protection platform to collect the necessary data once and use that data to improve security in multiple different ways. The following sections describe how different endpoint security capabilities delivered from a cloud-native endpoint protection platform can be applied to various parts of the NIST CSF Functions, Categories, and Subcategories to improve cybersecurity maturity.

[1] https://cdn2.hubspot.net/hubfs/468115/whitepapers/state-of-endpoint-security-2018.pdf

IDENTIFY

The NIST CSF Identify Function assists in formalizing a process of identifying and managing cybersecurity risk to systems, people, assets, data, and business processes. Having a clear understanding of the business environment and the related cybersecurity risks enables an organization to focus, prioritize, and align risk mitigation efforts with its risk management strategy and business needs. Categories within this Function include: **Asset Management** and **Risk Assessment**.

Asset Management

The objectives of the Asset Management Category are to inventory, manage, and classify all assets in the enterprise (i.e. data, hardware, software, external systems, and resources). Meeting these objectives allows an organization's management to make informed decisions around protecting critical assets.

A consolidated endpoint security solution helps achieve the objectives of Asset Management by enabling an organization with a centralizing platform to view, update, and manage the security of its endpoints. Many organizations utilize multiple endpoint agents on their assets, resulting in multiple tools (e.g. Microsoft's System Center Configuration Management – SCCM) and/or asset inventories. As part of a holistic deployment, endpoint security solutions are deployed to all appropriate endpoints, requiring an accurate asset inventory. Consolidating this with a fully integrated platform enables the organization to have a single and complete source of truth for their assets. With all assets in a centralized tool, management has visibility into their environment and is better positioned make more informed decisions.

Risk Assessment

The objectives of the Risk Assessment Category are to identify and document threats to enterprise assets and determine the likelihood and impact of those threats to identified cybersecurity risk. Meeting these objectives allows an organization's management to take appropriate action on those risks (i.e. acceptance, avoidance, mitigation, and transference).

An advanced endpoint security solution offers real-time assessment of the threats in the environment. These threats can be quantified to further understand the likelihood and impact of the threat if it were to successfully exploit an organizational asset. With comprehensive insight, management can make better decisions to respond to the threat in line with the organization's risk tolerance.

PROTECT

The Protect Function outlines appropriate safeguards to ensure delivery of critical infrastructure services and defend against threats to business processes, critical assets, data, and information. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Categories within this Function include: **Data Security** and **Protective Technology**.

Data Security

The objectives of the Data Security Category are to protect the confidentiality, integrity, and availability information (data) in accordance with the organization's risk management strategy. A lack of adequate protection can result in fines, penalties, and loss of brand reputation.

Endpoint security solutions are one of the key technology solutions required to protect data-at-rest stored on endpoints. Next-generation endpoint products include both the traditional anti-virus and the intelligence to protect endpoints against known and unknown attacks. The traditional anti-virus part of these solutions restricts unauthorized access infiltrating the environment through malware, spyware, and viruses. The next-generation intelligence part involves integrity checking mechanisms to verify activity on the hardware and software is legitimate and authorized. Endpoint security solutions give an organization visibility for protection sensitive data from sophisticated threat attacks.

Protective Technology

The objectives of the Protective Technology Category are to utilize technical solutions to manage and enforce the security of sensitive assets and ensure the resilience of systems supporting key business processes. Protective technologies allow organization to rely on their security mechanisms to meet business standards, processes, and expectations.

An organization's Configuration Management Program should be built around the principle of least functionality. Essentially, systems should be configured to provide only essential functions and capabilities. Endpoint security configuration management is an essential piece to the Configuration Management Program, as endpoint security solutions block and alert on unknown, unauthorized, or malicious activities occurring on or within the organization's IT environment. This creates a hardened environment and allows an organization to meet the configuration management requirements, thus improving their overall cybersecurity maturity and reduce risk.

DETECT

The NIST CSF Detect Function enables the timely discovery of cybersecurity events and threats in the environment. Categories within this Function include: **Anomalies and Events** and **Security Continuous Monitoring**.

Anomalies and Events

The objectives of the Anomalies and Events Category are to detect and analyze threats in the environment. A well-developed process for analyzing threats allows an organization to take quick action to contain and eradicate a threat before it can cause significant damage.

Endpoint security solutions are valuable tools for identifying and detecting anomalies and events in assets throughout the environment. Endpoint security solutions are backed with threat intelligence feeds based on big data analytics in order to segregate "normal" user behavior from anomalous activity. These solutions alert on unauthorized or suspicious behavior to enable the organization to perform further analysis in real-time. These rapid detection solutions allow organizations to make proactive decisions to further protect their information and information assets.

Security Continuous Monitoring

The Security Continuous Monitoring Category objectives include monitoring the organization's network, endpoints, and connections (internal and external) to detect threats and vulnerabilities in the environment. An effective continuous monitoring program allows an organization to identify threats in real-time and take timely action.

A comprehensive Security Continuous Monitoring Program is incomplete without an endpoint security solution. Endpoint security solutions reside on endpoints in the environment (i.e. workstations, servers, mobile devices, etc.) and continuously monitor activity, comparing activity against a "normal" baseline to detect threats. These solutions improve cybersecurity maturity and reduce risk by providing organizations with improved visibility into their environment while reporting and alerting on any suspicious activities.

RESPOND

The Respond Function includes activities to take appropriate action to a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Categories within this Function include: **Analysis** and **Mitigation**.

Analysis

The Analysis Category objectives include the ability to effectively triage and investigate alerts from detection systems. A triage process allows an organization to determine the impact of alert and prioritize responses.

In addition to the advanced threat protection capabilities, most endpoint security solutions offer in-depth analysis on identified threats. Supported by big data analytics and advanced forensics, endpoint security solutions provide immediate access to the complete picture of an attack, including root cause, vulnerability source(s), number of hosts impacted, etc. This aids in improving an organization's analysis and investigation processes, improving response time from days to minutes. As a result, organizations with effectively implemented endpoint security solutions experience a higher level of cybersecurity maturity and reduced cyber risk.

Mitigation

The objectives of the Mitigation Category are to contain and mitigate incidents. Containing incidents is essential for limiting the impact and the breadth of damage to assets and IT infrastructure.

Once an attack penetrates the environment, the clock starts, as most malicious hackers can steal data or do significant damage to IT infrastructure within the first 12 hours. With this tight timeframe, every minute counts. To counter these attacks, many endpoint security solutions offer the capability of "live response," or real-time remediation services. Endpoint security threat responders provide services to isolate threats and stop processes, which reduces potential overall damage to an organization's operations. The ability to isolate and block threats in near real time is a substantial benefit to organizations deploying and maintaining an efficient endpoint security solution.

RECOVER

The Recover Function includes the activities necessary to maintain resiliency plans and to restore capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. A Category within this Function includes: **Recovery Planning**.

Recovery Planning

Recovery Planning Category objectives include establishing and executing sound processes in response to an event in order to efficiently return to normal operations. The impact of a cyber event or incident is significantly reduced based on the speed at which an organization can return to normal operations.

Advanced endpoint security solutions assist with all phases of incident response (e.g. preparation, detection, analysis, and mitigation), making recovery a streamlined process. Organizations that include their endpoint security solution's forensic capabilities into their Incident Response Plan(s), Business Continuity Plan(s), and Disaster Recovery Plan(s) allow them to make quick decisions, respond effectively, remediate efficiently, rapidly recover, and improve their overall cyber security maturity.

CARBON BLACK'S ENDPOINT PROTECTION PLATFORM (EPP)

Delivered as a cloud-native solution using a single agent, the Carbon Black (CB) Predictive Security Cloud (PSC) is an endpoint protection platform that provides everything an organization needs to prevent, investigate, remediate, and hunt threats in real time. The PSC can be strategically aligned to the various security objectives of any cybersecurity framework, including the NIST CSF. The PSC offers an organization complete visibility into the environment to identify and protect key assets, detect and respond to threats, and recover to normal business operations efficiently. These technical solutions empower

organizations to identify and remediate vulnerabilities to close security gaps and strengthen enterprise cyber maturity.

An organization's security maturity should scale as the organization grows without requiring significant retooling. As such, it is advantageous for an organization to choose security toolsets that can scale to the increased security risks associated with business growth. The PSC can support the endpoint security requirements of organizations of all sizes via its scaling capabilities and improvement add-on features.

Below is an example of how the PSC can be used to improve an organization's security program maturity. Each level describes a maturity level with respect to Carbon Black in alignment with the matrix found in Figure 3. This example focuses on endpoint protection, which is one crucial piece of an organization's security program. A similar approach can be applied to other aspects of an organization's defense-in-depth security strategy.

LEVEL 1 - INITIAL

At an early stage, an organization that is just beginning to address their approach to security has limited understanding of the security posture of the organization. Also, there may be limited budget to spend for implementing security safeguards. The organization believes that the best course of action for addressing immediate security concerns is to protect their endpoints. The organization would like to prevent as much known malware as possible to keep the users' endpoints running smoothly and minimize how often they need to reimage infected machines. At this stage, the organization is trying to evolve from simply reacting to issues as they arise to more proactively addressing known issues.

Out of the box, next generation antivirus + endpoint detection and response (NGAV+EDR) on the PSC not only automatically prevents known attacks, but uses advanced predictive models to block emerging, never-before-seen attacks that traditional anti-virus solutions often miss. The organization can leverage this protection to remain secure against new ransomware and file less attacks, without requiring much analyst expertise. If the organization needs more human resources to help triage events and prioritize alerts, they can leverage the PSC's managed alert monitoring and triage service for added confidence.

LEVEL 2 - REPEATABLE

As the organization desires greater maturity, perhaps due to an increase in understanding of responsibility for employees and sensitive assets, the security function of the organization calls for more documented processes, as well as a more layered approach to security. At this stage, the organization is trying to evolve from simply reacting to issues as they arise to more proactively addressing known issues. Carbon Black's NGAV+EDR offering on the PSC allows customers to fine tune and granularly customize policy rules so an organization can assess its risks and secure its endpoints accordingly.

To improve operational awareness, the organization may also want more visibility into the current state of their endpoints at this stage. When news breaks that a common application or browser extension has been exploited, the organization's security professionals can use the PSC's real-time endpoint query tool to quickly identify which machines are running vulnerable software and act in a timely manner to remotely ensure that proper patches are installed. Because this offering is also available on the PSC, no new agent deployment is necessary; the added functionality is simply enabled, and the team can get to work.

LEVEL 3 - DEFINED

The organization has established dedicated resources with a standalone security team, and the security program is becoming more formalized with documented and integrated processes for detecting and responding to threats. Based on the improved visibility and understanding of the environment, the organization is now able to integrate processes based on attacker behavior and threat intelligence.

Beyond awareness and visibility of the organization's assets, the organization is more aware of the risks that are present that threaten those assets. The organization can move beyond simply reacting to issues that arise to a more defined process of preventing issues. The organization can assign resources to ad-hoc threat hunting, leveraging the PSC's advanced hunting and incident response capabilities. To get started, the organization can use the PSC's MITRE ATT&CK feed to help map their hunting to the detection framework.

LEVEL 4 - MANAGED

With dedicated resources and a standalone security team with a maturing security program, the organization desires to ensure that documented and integrated processes are effective. Rather than responding to individual incidents and ensuring that endpoints are individually protected, the organization becomes more proactive in managing the solution. The organization wants to confirm that they can scale the security program and address emerging growth and complexity as well as threats. To assist the organization in gaining management efficiency, the organization accesses the raw endpoint event data to integrate with the rest of the security stack. The organization can now observe the effectiveness of endpoint security within the context of activities from other sources and correlate the events of the endpoint security.

With the focus of the organization on customization, the organization's security team can use the PSC to create custom watchlists that detect suspicious activity, so they can immediately act to shut down the attack. With PSC, this can be done from anywhere in the world according to the organization's incident response plan. The organization can also collaborate with other security professionals in their same industry with the Carbon Black User Exchange Community. Additional insights can be provided through the Carbon Black Threat Analysis Unit.

LEVEL 5 - OPTIMIZED

With an ever-changing threat landscape, the job of a security professional is never quite finished. At this level of maturity, the organization may be more capable of anticipating threats and addressing them prior to exposure. The security team has developed and documented processes, is managing the processes, has increased integration to facilitate improved operation, can measure the effectiveness of the solution against targeted security goals, and is now automating as many processes as possible to improve efficiency and reduce or eliminate response time. A mature security program strikes the best possible balance between man and machine, leaving grunt work to the machines and the informed decision making to the humans. In this way, the organization is optimizing their approach to security, which allows them to proactively reassess risks and continuously improve their security program.

Leveraging just one endpoint agent and one cloud-based console, the PSC delivers unfiltered visibility into every endpoint of the organization. Without ever having to redeploy to use a new service, the PSC scales and provides more advanced capabilities to the organization as they mature their security program. The organization has positioned itself to not only stay secure today, but to remain resilient as threats change over time. As the security team is more aware of what is happening in their environment, they can better harden their security posture with each new threat using one consolidated endpoint protection platform.

CONCLUSION

A comprehensive cybersecurity program is essential for organizations to protect their critical systems, data, business processes, and people. The NIST CSF is just one example of a framework that organizations can follow and provides significant value due to its defense-in-depth approach of identifying the environment, protecting the environment, and detecting and responding to, and recovering from, threats. Aligning the CMM with the NIST CSF gives organizations greater insight into their maturity levels, allowing organizations to set clear maturity objectives and better manage enterprise risk.

Endpoint security is one crucial aspect of a comprehensive defense-in-depth security approach. As an organization matures, each layer or facet of the organization's security functions together toward the common goal of proactively securing the organization's assets and protecting the organization's mission. Carbon Black's PSC provides capabilities that can help mature an organization's security program with respect to endpoint security through detection and identification of threats, protection of endpoint assets, timely response to detected cybersecurity incidents, and restoration of endpoints to normal operation.

ABOUT CARBON BLACK

Carbon Black (NASDAQ: CBLK) is a leader in cloud endpoint protection dedicated to keeping the world safe from cyberattacks. The CB Predictive Security Cloud® (PSC) consolidates endpoint protection and IT operations into an extensible cloud platform that prevents advanced threats, provides actionable insight and enables businesses of all sizes to simplify operations. By analyzing billions of security events per day across the globe, Carbon Black has key insights into attackers' behaviors, enabling customers to detect, respond to and stop emerging attacks.

More than 5,300 global customers, including 35 of the Fortune 100, trust Carbon Black to protect their organizations from cyberattacks. The company's partner ecosystem features more than 500 MSSPs, VARs, distributors and technology integrations, as well as many of the world's leading IR firms, who use Carbon Black's technology in more than 500 breach investigations per year.

For further information on Carbon Black's product offerings, please see contact a representative:

Email: contact@carbonblack.com

Phone: 716-393-7400

Website: carbonblack.com

REFERENCES

NIST CSF Framework: https://www.nist.gov/cyberframework/framework

NIST CSF Framework: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Carbon Black Endpoint Security Material: https://www.carbonblack.com/resources/definitions/what-is-endpoint-security/

2018 State of Endpoint Security Report: https://cdn2.hubspot.net/hubfs/468115/whitepapers/state-of-endpoint-security-2018.pdf

ISACA's Building Capability with CMMI: http://www.isaca.org/KNOWLEDGE-CENTER/BLOG/Lists/Posts/Post.aspx?ID=667&utm_referrer=direct%2Fnot%20provided&utm_referrer=

ABOUT THE AUTHORS

Doug Hudson | Senior Director, Cyber Risk Advisory

Doug Hudson (doug.hudson@coalfire.com) is a Senior Director with Coalfire's Cyber Risk Advisory practice. Doug brings more than 20 years of experience of working in strict and ever-changing regulatory environments, including financial services, retail operations, telecom, cloud/tech, healthcare, and pharmaceuticals. He focuses on advising the board, C-suite, and information risk executives and related advisory committees on risk management, incident response, cybersecurity strategy, governance, overall technology management, and compliance. He currently holds a CISSP certification.

Jason Macallister | Senior Consultant, Cyber Engineering

Jason Macallister (jason.macallister@coalfire.com) is a Senior Consultant with Coalfire's Cyber Engineering practice. Jason brings over 20 years of experience in IT consulting and engineering. Jason is primarily responsible for leading client engineering engagements focusing in cloud and virtualization technologies, advising clients on infrastructure design recommendations, technical security control implementation, network security enhancements, and perimeter security improvements.

Mandy Pote | Senior Consultant, Cyber Risk Advisory

Mandy Pote (mandy.pote@coalfire.com) is a Senior Consultant with Coalfire's Cyber Risk Advisory practice. Mandy brings over 5 years of experience as a trusted advisor in the field of IT Risk Management. Her focus on business process and supporting technology has provided clients with expertise in the areas of security control design and remediation, policy and procedure development, and enterprise risk assessments. She currently holds CISSP and CRISC certifications.

Published January 2019.

ABOUT COALFIRE

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 16 years and has offices throughout the United States and Europe. Coalfire.com

January 8, 2019