The Ultimate Guide to Cybersecurity Assessments

Brite

`

Table of Contents

`

Why Security Assessments?

A strong Cybersecurity program is about more than just compliance. It is a continuous evaluation of risks and finding ways to easily identify and mitigate those risks that have the biggest impact on your organization. Assessments are one way to help an organization continuously improve and strengthen their cybersecurity approach. They can help identify security vulnerabilities, create new security requirements, spend cybersecurity budgets more intelligently, conduct due diligence and improve both communication and decision-making.

Benefit of Third-Party Assessments

The fast-paced nature of cybersecurity teams often means that assessments get pushed aside. That is where a third-party like Brite comes in. Our security assessments, like the one outlined below, ensures that you are not missing critical gaps in your approach of protecting the organization.

A BriteProtect Security Assessment provides a 360 degree look at your current security posture, mapped against a relevant framework (like CIS Critical Controls, ISO 27001, etc.) through an interview style evaluation. Each compensating control area is then scored and ranked based on importance to the overall organization.

We have simplified this process to limit the time, effort and energy required from your team. Our experienced analysts utilize the information provided to deliver a gap analysis and recommended roadmap for improvement, including the potential funding required. To deliver accurate results and meaningful recommendations, assessments should be performed regularly and by a third party. The result is a comprehensive report and strategic security plan developed by Brite's VCISO to help organizations prioritize security efforts.

`

Assessment Overview

Inventory and Control of Hardware Assets

Question: Does the organization utilize an active discovery tool to identify devices connected to the network that updates the hardware asset inventory?

Why we are asking: It's important to know what devices are connected to the network at all times to ensure that all devices are authorized and suspicious activity does not go unnoticed.

Priority: Medium

Inventory and Control of Software Assets

Question: Does the client maintain an up-to-date list of all authorized software that is required in the enterprise for all business purpose on any business system?

Why we are asking: It is important to know what software is being installed on your corporate devices to ensure both that the software isn't malicious and so that it can be patched upon new releases of vulnerabilities.

Priority: Medium

Continuous Vulnerability Management

Question: Does the organization utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network at least weekly to identify all potential vulnerabilities on the organization's systems?

Why we are asking: The first step to quick remediation of a vulnerability is to know that it exists. Frequent scanning ensures vulnerabilities can be remediated within the proper time frame.

Priority: High

Controlled Use of Administrative Privileges

Question: Does the organization use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges?

Why we are asking: It is important to confirm that only authorized individuals have elevated privileges to minimize insider threat risks. This also decreases the chances of the network being compromised.

Priority: High

`

Secure Configuration for Hardware and Software

Question: Does the client maintain documented, standard security configuration standards for all authorized operating systems and software?

Why we are asking: It is important to have a standard security configuration to know what is authorized on the network to prevent malicious software and ensure authorized software with vulnerabilities can efficiently be patched.

Priority: Medium

Maintenance, Monitoring, and Analysis of Audit Logs

Question: Has the organization ensured that local logging has been enabled on all systems and networking devices?

Why we are asking: Logging is essential for proper investigation in the event of any suspicious activity or a security breach on the network.

Priority: Medium

Email and Web Browser Protections

Question: Has the organization ensured that only fully supported web browsers and email clients are allowed to execute, ideally only using the latest version of the browsers and email clients provided by the vendor?

Why we are asking: Only safe and secure web browsers and email clients should be used to protect against vulnerabilities and malicious code.

Priority: Medium

Malware Defenses

Question: Does the organization utilize a centrally managed anti-malware software to continuously monitor and defend each of the employee's workstations and servers?

Why we are asking: Ensuring proper security measures are taken against dangerous and business impacting software or code safeguards your data.

Priority: High

`

Limitation and Control of Network Ports

Question: Can the organization certify that only network ports, protocols and services listening on a system with validated business needs are running on each system?

Why we are asking: Ports that don't need to be open can result in a security breach unless the proper measures are taken. Open ports allow for easy connections and backdoor access to cyber-attacks.

Priority: Medium

Data Recovery Capability

Question: Can the organization ensure that each of the key systems are backed up as a complete system through processes such as imaging, to enable quick recovery of an entire system?

Why we are asking: Imaging critical systems is key in the recovery process after a disaster and for rollbacks in failed remediation attempts of critical infrastructure.

Priority: High

Secure Configurations for Network Devices

Question: Does the organization maintain standard, documented security configuration standards for all authorized network devices?

Why we are asking: It is important to have a security baseline for all devices so that only authorized and non-malicious devices will be able to join the network.

Priority: Medium

Boundary Defense

Question: Does the organization deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the network boundaries?

Why we are asking: It is important to only allow connections from trust IP addresses so that any malicious IP addresses will not be able to connect or attack to the network.

Priority: High

`

Data Protection

Question: Has the organization deployed an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals?

Why we are asking: Having a network tool that blocks the exfiltration of sensitive information that shouldn't be leaving the network will help prevent attempts to steal company data or classified information.

Priority: Medium

Control Access Based on the Need to Know

Question: Does the client segment the network based on the label or classification level of the information stored on the servers and locate all sensitive information on separated Virtual Local Area Networks (VLANs)?

Why we are asking: Segmenting networks for proper and efficient access ensures the information stored on them is protected and safe.

Priority: Medium

Wireless Access Control

Question: Does the organization maintain an inventory of authorized wireless access points connected to the wired network?

Why we are asking: Maintaining an inventory of authorized wireless access points to ensure only authorized devices can connect in a safe and secure manner.

Priority: High

Account Monitoring and Control

Question: Does the organization maintain an inventory of each authentication systems, including those located onsite or at a remote service provider?

Why we are asking: Knowing exactly what and where authentication systems are available will provide quick handling in the event of a disaster.

Priority: Medium

`

Implement a Security Awareness and Training program

Question: Has the organization created or implemented a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization?

Why we are asking: Reoccurring security awareness program and training to creates employees who are knowledgeable in mitigating phishing and cyber-attacks from occurring on their devices.

Priority: Medium

Application Software Security

Question: Does the employees only use up-to-date and trusted third-party components for software developed by their organization?

Why we are asking: Ensuring software and third-party components used by an organization are trustworthy and safe to use mitigates known vulnerabilities.

Priority: Medium

Incident Response and Management

Question: Does the organization have written incident response plans with defined roles of personnel as well as phases of incident handling/management?

Why we are asking: Written incident response plans ensure the organization is prepared in the event of a cyber-attack or incident and that the proper steps to mitigate the incident are taken.

Priority: High

Penetration Tests and Red Team Exercises

Question: Does the organization perform periodic Red Team exercises to test readiness of both identifying and stopping attacks quickly and effectively?

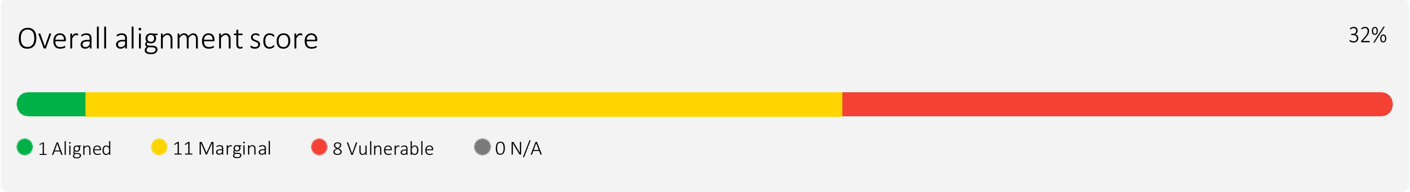
Why we are asking: Practicing what would happen in the case of an incident prepares the organization for when an incident or cyber-attack does happen.

Priority: High

`

Alignment Score

The results of the assessment are compared against the cybersecurity framework controls. They are rated as aligned, marginal or vulnerable. From these results, a current security posture with Brite's Alignment score is provided in a detailed report. As compensating controls are implemented, the alignment score will improve over time.


Overall alignment score

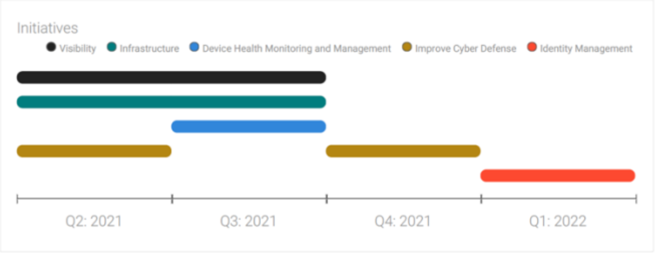
32%

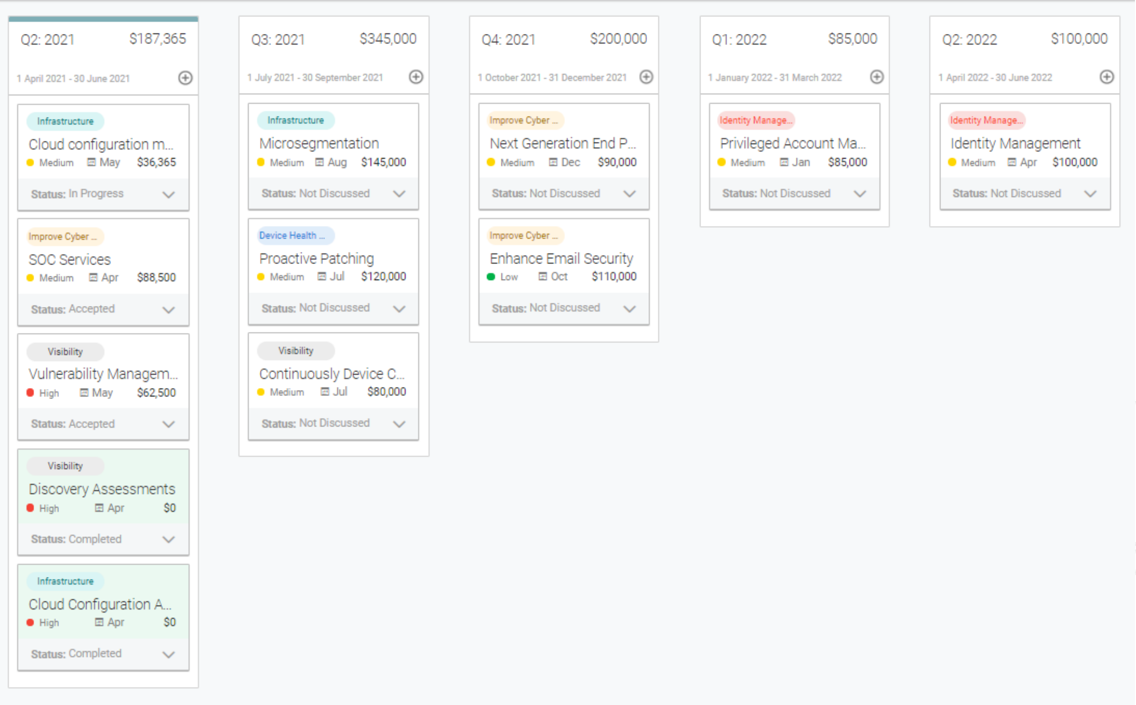
🟢 1 Aligned 🟡 11 Marginal 🔴 8 Vulnerable ● 0 N/A

Example Alignment Score

Roadmap

Information is only valuable if an organization can put it into action. After an assessment interview is completed, Brite's vCISO carefully analyzes the current position, maps it against the biggest organizational risk and prioritizes projects. General budgetary numbers are assigned to the initiatives based on the organizations scope. These timelines are assigned in a collaborative effort. The result is a clear, concise cybersecurity roadmap.




Q2: 2021 $187,365
1 April 2021 - 30 June 2021

Infrastructure
Cloud configuration m...
Medium May $36,365
Status: In Progress

Improve Cyber ...
SOC Services
Medium Apr $88,500
Status: Accepted

Visibility
Vulnerability Managem...
High May $62,500
Status: Accepted

Visibility
Discovery Assessments
High Apr $0
Status: Completed

Infrastructure
Cloud Configuration A...
High Apr $0
Status: Completed

Q3: 2021 $345,000
1 July 2021 - 30 September 2021

Infrastructure
Microsegmentation
Medium Aug $145,000
Status: Not Discussed

Device Health ...
Proactive Patching
Medium Jul $120,000
Status: Not Discussed

Visibility
Continuously Device C...
Medium Jul $80,000
Status: Not Discussed

Q4: 2021 $200,000
1 October 2021 - 31 December 2021

Improve Cyber ...
Next Generation End P...
Medium Dec $90,000
Status: Not Discussed

Improve Cyber ...
Enhance Email Security
Low Oct $110,000
Status: Not Discussed

Q1: 2022 $85,000
1 January 2022 - 31 March 2022

Identity Manage...
Privileged Account Ma...
Medium Jan $85,000
Status: Not Discussed

Q2: 2022 $100,000
1 April 2022 - 30 June 2022

Identity Manage...
Identity Management
Medium Apr $100,000
Status: Not Discussed

`

In Conclusion

It is always a good idea to take a step back and realistically evaluate how secure your organization is, not just to meet compliance. The continuous evaluation of risks will ease the pain to mitigate those risks and reduce the impact of an attack on the organization.

Since security teams are often pulled in many directions, a third party like Brite can dedicate the time and energy necessary. Use our teams to help identify security vulnerabilities, create new security requirements, spend cybersecurity budgets more intelligently, conduct due diligence and improve communication and decision-making.

About Brite

Technology and people are at the core of everything we do. We're committed to proactively protecting communities and organizations through innovative technology solutions delivered by our talented team. By partnering with thoroughly vetted industry-leading technologies, we're able to provide proven solutions, coupled with tested processes, enabling our clients to better achieve *their goals and objectives*.

www.Brite.com/BriteProtect | SalesInfo@Brite.com | 1.800.333.0498