BlueVoyant

CASE STUDY:

NIST CYBERSECURITY ASSESSMENT

Holistic cybersecurity is essential to reducing overall risk

1. ORGANIZATIONS CANNOT PROTECT AGAINST EVERYTHING

Threats today are becoming increasingly sophisticated as the traditional attack surface of an organization expands to cloud, mobile, and IoT domains. As security budgets tighten, cyber leaders must prioritize their security efforts for maximum value.

2. TOOLS ARE NOT ENOUGH

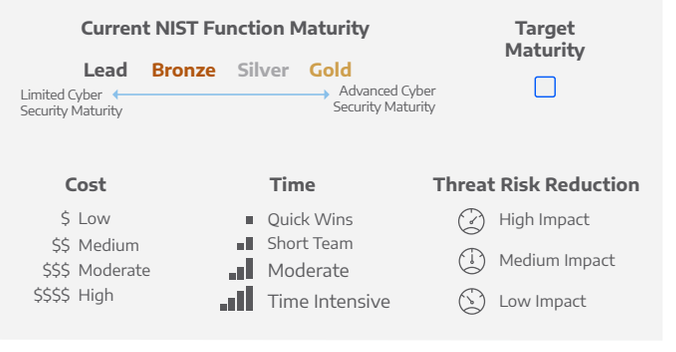
Cyber technology today augments organizational security programs but do not completely protect from threats and attacks. Without addressing other critical elements such as organizational structure, culture, or the human factor, you cannot completely address cybersecurity risk.

3. EVERY INDUSTRY FACES UNIQUE CYBERSECURITY CHALLENGES

Financial organizations are more lucrative targets for Cybercriminals while SCADA and manufacturing companies often pique the interest of nation state adversaries. Holistic cybersecurity requires tailoring security controls to the most likely threats.

NIST CYBERSECURITY ASSESSMENT

The NIST Cybersecurity Framework (CSF) is the de facto standard used to identify, assess, and mitigate cybersecurity risk that exists in organizations throughout the world. The NIST standard uses a holistic approach that measures your organization's effectiveness across the incident response lifecycle. When conducted alongside the deployment of our MSS offering, our experienced consultants will document the added maturity of our solutions while identifying prioritized gaps the help your organization protect against the threats most applicable to you.



Potential Enhancement	Description	Build Cost	Time	Resource	NIST Functional Improvement	Threat Risk Reduction
Vulnerability Management Program	Processes and technology which allow for the protection of organization assets from cybersecurity threats.	$$$		Build: 2 FTE Operate: 2 FTE	Identify Protect	
Cybersecurity Documentation	Formal and approved documentation which guide and enable the cybersecurity program.	$$		Build: 2 FTE Operate: 1 FTE	Identify Detect Respond	
Cybersecurity Staffing Uplift	Staff support which enable the operation of the cybersecurity program.	$		Build: 1 FTE Operate: 5 FTE	Identify Protect Detect Respond Recover	

BlueVoyant

CASE STUDY

Client Challenges

A growing startup experienced a cybersecurity incident which resulted in the leak of sanitized data. Recognizing how future events would be perceived by potential investors, the organization wanted to protect against these risks but was restricted by costs.

Approach

Combined delivery
Performing an assessment alongside the deployment of our MSS service allows us to leverage synergies to provide a cost effective holistic look at cybersecurity.

Organizationally relevant threats
Our knowledge of the industry and deep threat intelligence background enabled profiling of the organization against the everchanging threat landscape.

Focus on what matters
Pairing our technical recommendations against the organization's threat profile provided focused guidance for on how to best protect the organization.

Results

The organization has implemented a long-term security roadmap in line with their growth strategy and has not experienced another significant cybersecurity event.

For more information please visit:
www.bluevoyant.com

Secure your business now:
sales@bluevoyant.com

About BlueVoyant

BlueVoyant is an analytic-driven cybersecurity company whose mission is to protect businesses of all sizes against agile and well-financed cyber attackers by providing unparalleled visibility, insight, and responsiveness. BlueVoyant provides Advanced Threat Intelligence, Managed Security Services and Incident Response through offices in the United States, the United Kingdom, Israel, and Spain.