G.Bina
SECURITY Thought Leaders

Decision Support System (DSS) for Cybersecurity

Cyber threats have become a major problem for every organization. There are many technological solutions and defenses and a lot of advice and many advisors. But, how can an organization understand whether its defenses meet existing and future threats and risks? Where investments should be made in terms of the security budget?

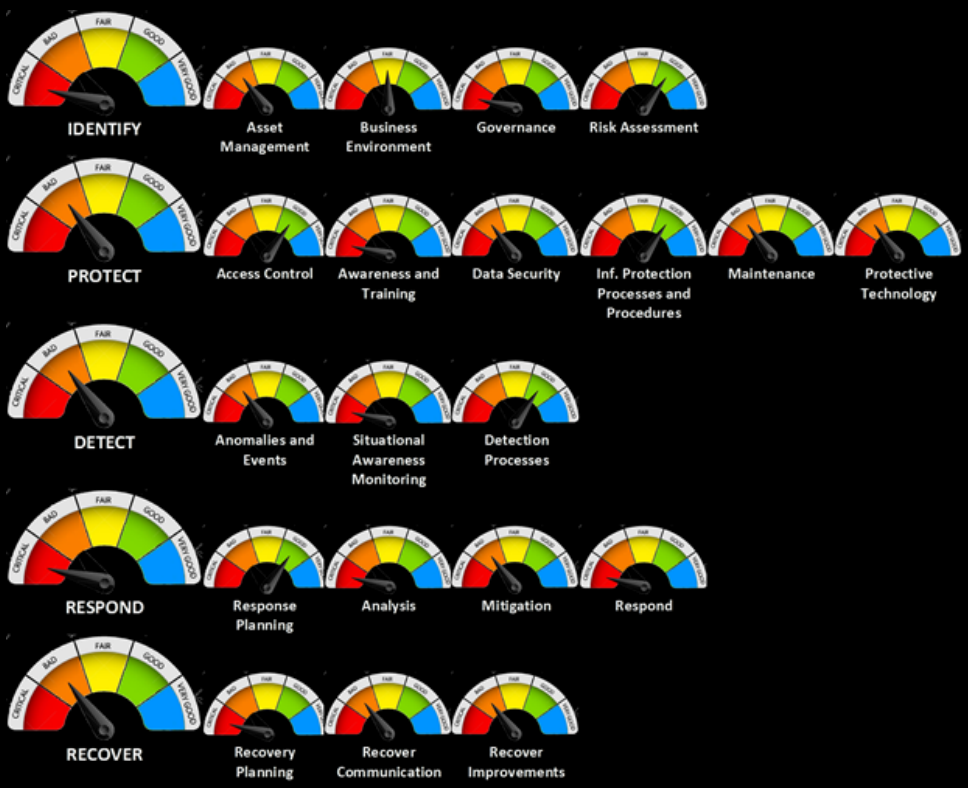
G. Bina's Decision Support System (DSS) aims to support IT and security officers as well of senior managers identify their organization's cyber-threat landscape, determine their cyber-defense maturity level, and take knowledgeable and prioritized decisions. Implementation of DSS involves four major steps:

1. Identify and Map Client's Cyberspace Threats

We first analyze an organization's threat landscape using G. Bina's cyber intelligence capabilities. We then analyze the risk level of each threat, relying on proprietary algorithms, which incorporate cyber security and business operations analytics.

2. Assess Client's Cybersecurity Maturity

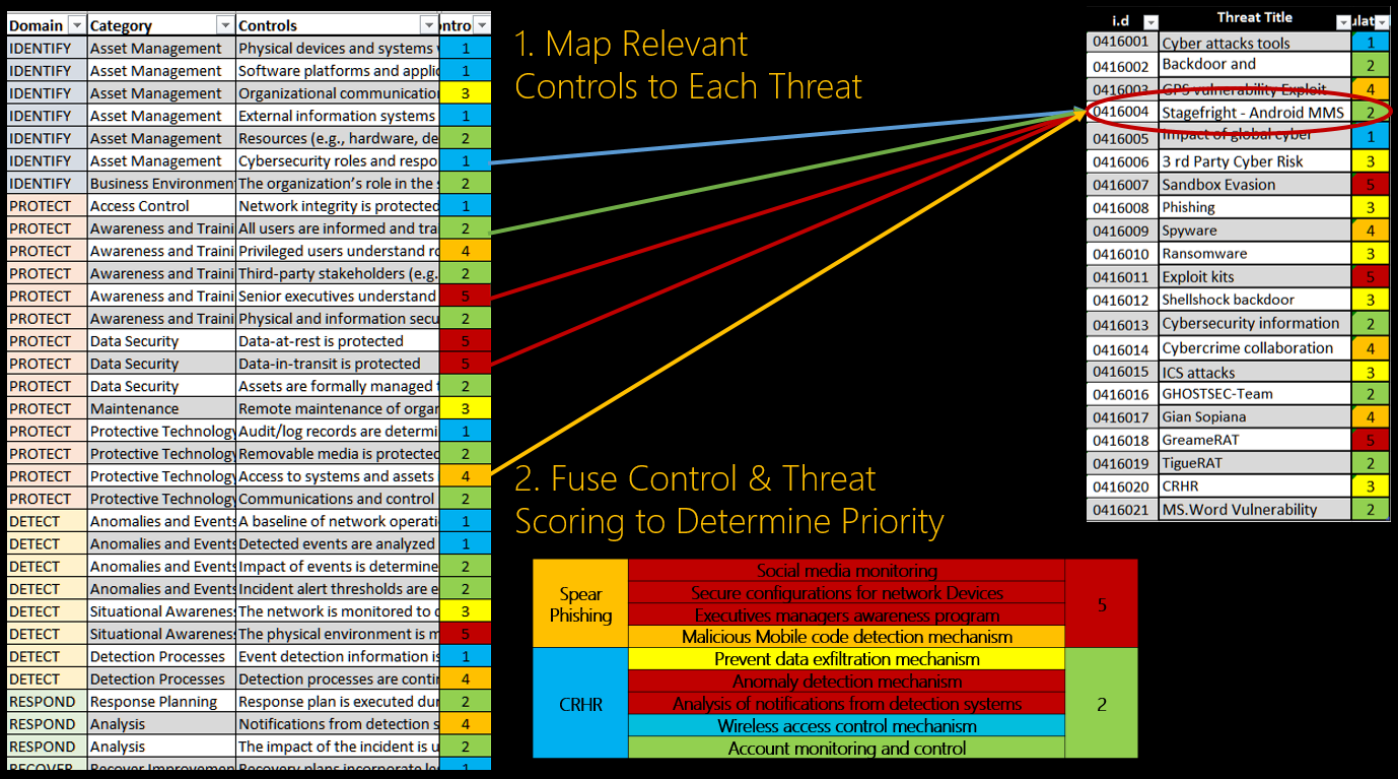
A client's cyber defense capabilities are then presented in a matrix structured by domains, categories and a series of actual defense controls.[1] Consequently the overall defense maturity is evaluated, providing a cyber defense maturity as illustrated in a dashboard view on the right.



[1] May be based on NIST/EST-C2N2 or any other adequate framework

3. Analyze Client's Cybersecurity Maturity Correlated with Threats

In this step G. Bina maps the relevant controls to each identified threat and risk. This allows an understanding of which controls (technologies, processes, procedures and policies) are in place and where gaps may exist. This will provide the client team – the senior manager or the IT expert – an effective and clear view of actual security gaps in a prioritized manner.



Domain	Category	Controls	ntro
IDENTIFY	Asset Management	Physical devices and systems	1
IDENTIFY	Asset Management	Software platforms and applic	1
IDENTIFY	Asset Management	Organizational communicatio	3
IDENTIFY	Asset Management	External information systems	1
IDENTIFY	Asset Management	Resources (e.g., hardware, de	2
IDENTIFY	Asset Management	Cybersecurity roles and respo	1
IDENTIFY	Business Environmen	The organization's role in the	2
PROTECT	Access Control	Network integrity is protected	1
PROTECT	Awareness and Traini	All users are informed and tra	2
PROTECT	Awareness and Traini	Privileged users understand r	4
PROTECT	Awareness and Traini	Third-party stakeholders (e.g.	2
PROTECT	Awareness and Traini	Senior executives understand	5
PROTECT	Awareness and Traini	Physical and information secu	2
PROTECT	Data Security	Data-at-rest is protected	5
PROTECT	Data Security	Data-in-transit is protected	5
PROTECT	Data Security	Assets are formally managed	2
PROTECT	Maintenance	Remote maintenance of orga	3
PROTECT	Protective Technology	Audit/log records are determi	1
PROTECT	Protective Technology	Removable media is protected	2
PROTECT	Protective Technology	Access to systems and assets	4
PROTECT	Protective Technology	Communications and control	2
DETECT	Anomalies and Events	A baseline of network operati	1
DETECT	Anomalies and Events	Detected events are analyzed	1
DETECT	Anomalies and Events	Impact of events is determine	2
DETECT	Anomalies and Events	Incident alert thresholds are e	2
DETECT	Situational Awarenes	The network is monitored to d	3
DETECT	Situational Awarenes	The physical environment is m	5
DETECT	Detection Processes	Event detection information is	1
DETECT	Detection Processes	Detection processes are conti	4
RESPOND	Response Planning	Response plan is executed du	2
RESPOND	Analysis	Notifications from detection s	4
RESPOND	Analysis	The impact of the incident is u	2

i.d	Threat Title	plat
0416001	Cyber attacks tools	1
0416002	Backdoor and	2
0416003	GPS vulnerability Exploit	4
0416004	Stagefright - Android MMS	2
0416005	Impact of global cyber	1
0416006	3 rd Party Cyber Risk	3
0416007	Sandbox Evasion	5
0416008	Phishing	3
0416009	Spyware	4
0416010	Ransomware	3
0416011	Exploit kits	5
0416012	Shellshock backdoor	3
0416013	Cybersecurity information	2
0416014	Cybercrime collaboration	4
0416015	ICS attacks	3
0416016	GHOSTSEC-Team	2
0416017	Gian Sopiana	4
0416018	GreameRAT	5
0416019	TigueRAT	2
0416020	CRHR	3
0416021	MS.Word Vulnerability	2

Control	High	Medium	Low
Situational Awareness Monitoring	6	6	2
Awareness and Training	5	6	2
Governance	4	2	1
Anomalies and Events	4	4	1
Protection Processes and Procedures	0	0	0
Recovery Planning	3	0	0
Mitigation	3	2	0
Business Environment	3	1	0
Analysis	2	6	0
Data Security	2	3	1
Detection Processes	2	4	0
Respond Improvements	1	1	0
Access Control	1	1	0

Consequently, we count the number of instances each defense control was identified as relevant to mitigate a threat.

G. Bina is aware that clients budget is always limited, and hence we are focused on providing advice with a clear prioritizing tool that identifies how and where efforts and budget should be concentrated.

4. Generate a prioritized cybersecurity action & investment plan

The final output would include: Priority plan of what needs to be done in conjunction with budget constraints and an action plan of how it should be done.

5. Why Consider DSS?

Because our service is:

- Threat Driven – driven by focused intelligence specifically gathered and analyzed.
- Intuitively understood – illustrated graphic view, making it easy to explain to managers
- Quick to implement – fast to implement, providing security snapshot & prioritized action plan.
- Cost Effective – It costs a fraction of an overall Risk Assessment, most importantly making for simpler decision-making