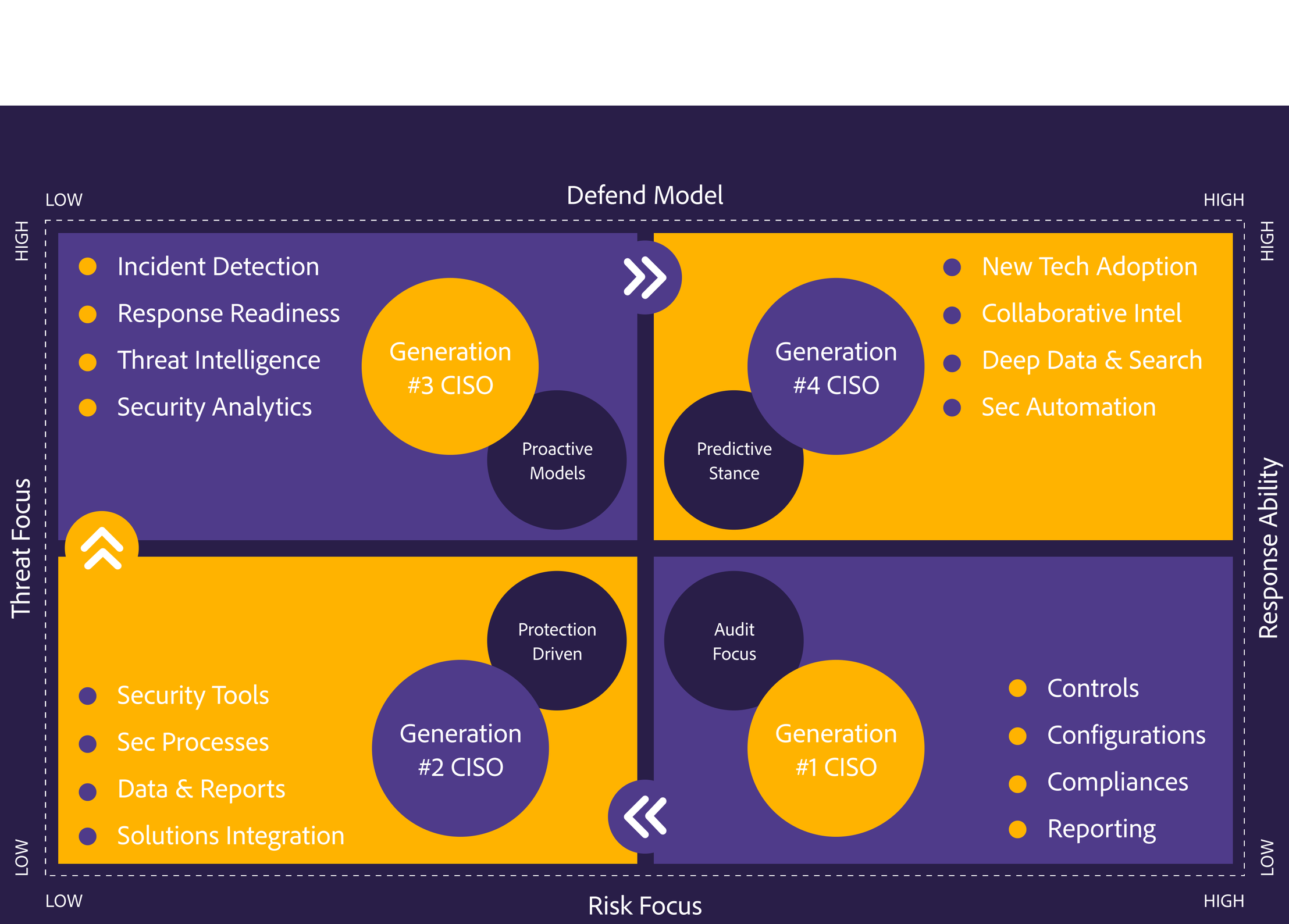
Castellum Labs

WHITE PAPER 2021

CISO Role <> Evolution Map

CISO is one leadership role, which has gone through more changes on competence, skills and maturity curve than any other leadership role in enterprises.



Evolution Map of CISOs

Castellum Labs

WHITE PAPER 2021

The "Needs & Expectations" from a CISO have changed almost every two years during the last one decade. That is a rate of upgrade, which beats down even the smart phone market. It is a tough and arduous road for people, who are either in role or aspiring to get onto that road.

Combine this with another fact of businesses across industry sectors. Companies in most of the industry sectors, started becoming serious to CISO and equivalent positions only during the last decade. This change in companies stance to CISO role, came into a reality only after, treating cyber security only as compliance devil for more than two decades.

That meant, organizations pushed mid level management, into CISO roles, because of two factors, one lack of requisite budgets and two lack of real significance placed on role. This led to a situation, where quite many CISOs didn't have the time and opportunity, to gather right exposure, at strategic level. And, still had to fill in positions which demanded strategic capabilities combined with complex operational capabilities, in tough, challenging & risky circumstances.

Castellum Labs

WHITE PAPER 2021

The Origin of the Role

When one looks at the origin of Cyber Security function in companies, and, what all it was expected to accomplish and deliver, in early days, that explains the limitations and also the stance of many of the CISOs, even today.

Cyber Security started out mostly as a hygiene factor, and, then grew further through a push by standards bodies, governmental requirements, into compliance activities. For a long time security remained focused on hygiene modeled security operational activities.

First Generation - "The Check listers"

Our first generation CISOs mostly came with both the background and mindset of preparing, maintaining & updating docs which were around hygiene and best practices, as mandated by external bodies, communities & regulation authorities.

This generation was mostly focused on repeated attempts at creating processes for checks & controls of the configurations, security processes, and, documentations as mandated by their industry, industry associations, and, compliance frameworks. This generation of CISOs did a good job, till CySec needed activities which were limited to secure configurations, host and, network hardening and backups.

Over a period of time some of people (CISOs) who were indoctrinated into cyber security, with dimension of "Checklists", found a new reality, which they had to to deal with as part of their role. This realist was need of latest security products and technologies which were needed to be acquired, to bolster org's capabilities beyond hygiene factor modeled security.

First Generation Quadrant Placement

This generation CISOs will have most of their focus on risk management, mostly from audit & compliance point of view. While these CISOs will have lesser or lower focus on threats & a security approach modeled around threat landscape, their org's will also be on lower side, on "Respond Capability" in the face of a real threat, which has knocked at their door.

Most of first gen CISOs, will have their team cultures built around, "demands of auditors".

Castellum Labs

WHITE PAPER 2021

Third Generation - "Detection & Response"

This generation shaped up, when locking and protecting the assets was not good enough and identifying, what is happening in an enterprise setup, taking measures to detect the potential adversary, and, stopping them in their tracks became critical.

A host of new models of security were developed around detection capabilities & then equal amount of technologies and tools were adopted for the same.

For further progression, to deal with next gen threat landscape, CISOs needed to transition from their tools buying mindset to "Real Time Detection Program" based security.

This generation suddenly found marginal availability of budgets, which company board was willing to spare, if the products were suggested by CISO , and, they gave a comfort factor to board. Second generation of CISOs were mostly product buyers, who would be spending a lot of time, evaluating technologies, mostly around protection, to lock and latch their assets from the prying eyes.

Second Generation Quadrant Placement

This generation will largely be product buyers and mostly for protection. This will have low focus on risk management & this generation will also be low on threat understanding. Since their attention is on acquiring technologies, which promise to protect.

Protection is "Not Enough"

Next major transition in world of Cyber Security was introduced, when continuous and innovative evolution of threats & communities made it apparent, that best of the protection will not stand a change, in the face of a committed adversary. People realized that, their security has to go beyond protecting digital assets, through blocking, limiting access & simple signature based security measures.

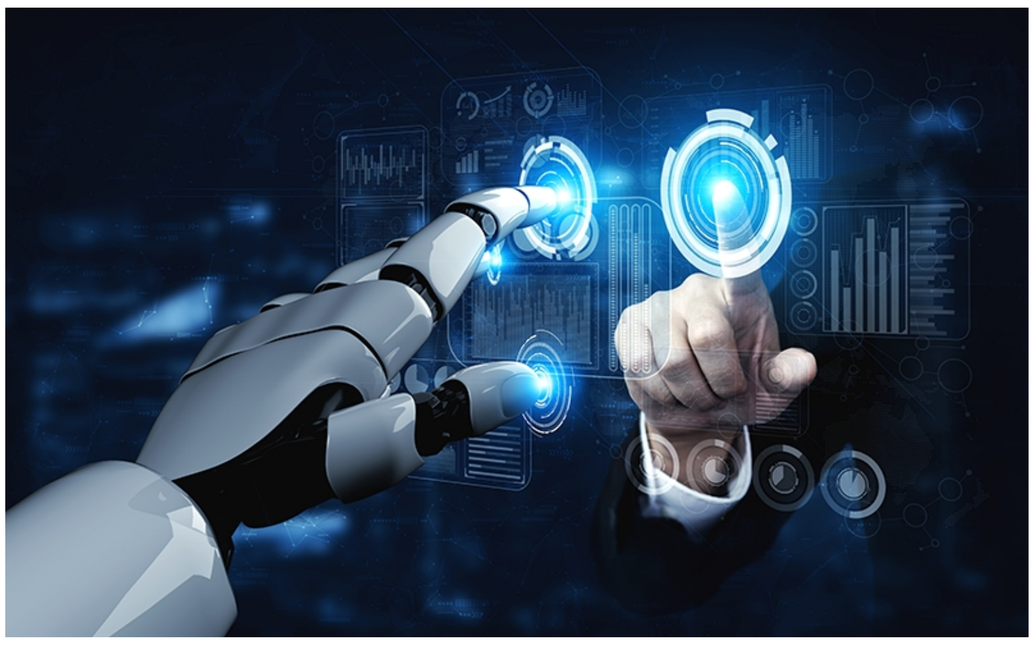
Transition into Protective Stance

One of the first set of security technologies, which got beyond host access & network access controls and basic monitoring, were mandated by need of a protective stance taken by orgs.

A multitude of products which worked on the premise of blocking threat/bad actors & traffic came into being, and, changed the world of CISOs.

Second Generation - "Lock and Latch"

A generation of CISOs grew in an environment, which focused on acquiring products, which can protect servers/hosts, data, & network perimeter with a range of incremental protective measures using restrictive models.



This generation suddenly found marginal availability of budgets, which company board was willing to spare, if the products were suggested by CISO , and, they gave a comfort factor to board. Second generation of CISOs were mostly product buyers, who would be spending a lot of time, evaluating technologies, mostly around protection, to lock and latch their assets from the prying eyes.

Second Generation Quadrant Placement

This generation will largely be product buyers and mostly for protection. This will have low focus on risk management & this generation will also be low on threat understanding. Since their attention is on acquiring technologies, which promise to protect.

Protection is "Not Enough"

Next major transition in world of Cyber Security was introduced, when continuous and innovative evolution of threats & communities made it apparent, that best of the protection will not stand a change, in the face of a committed adversary. People realized that, their security has to go beyond protecting digital assets, through blocking, limiting access & simple signature based security measures.

Key Services Areas

Application Security

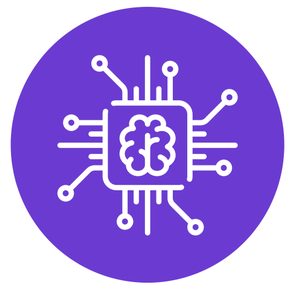
Managed AppSec Programs

Cloud Security

Cloud Security Design & Governance

SOC Monitoring

Managed Detection and Response



Threat Intelligence

Contextual Threat Intel & Hunting

Our Technology Platforms

appFORT

Continuous Application Security

watchOUT

Darkweb Monitoring

threatNIXD

Next Gen SOC Monitoring

Continuous Unified View of your Cyber Security

Get in touch with us to know more on our Cyber Security offerings

WHITE PAPER 2021

Castellum Labs

+91 97009 70397

info@castellumlabs.com

www.castellumlabs.com