CaspiPoT

SECURITY GUARD

Defend Your Business Against the Latest Cyber Threads

Power behind CaspiPoT

Caspisec

(Cyber Security Company)

www.caspisec.com

Machinarium

(Software Development Company)

www.machinarium.com

RedLabIS

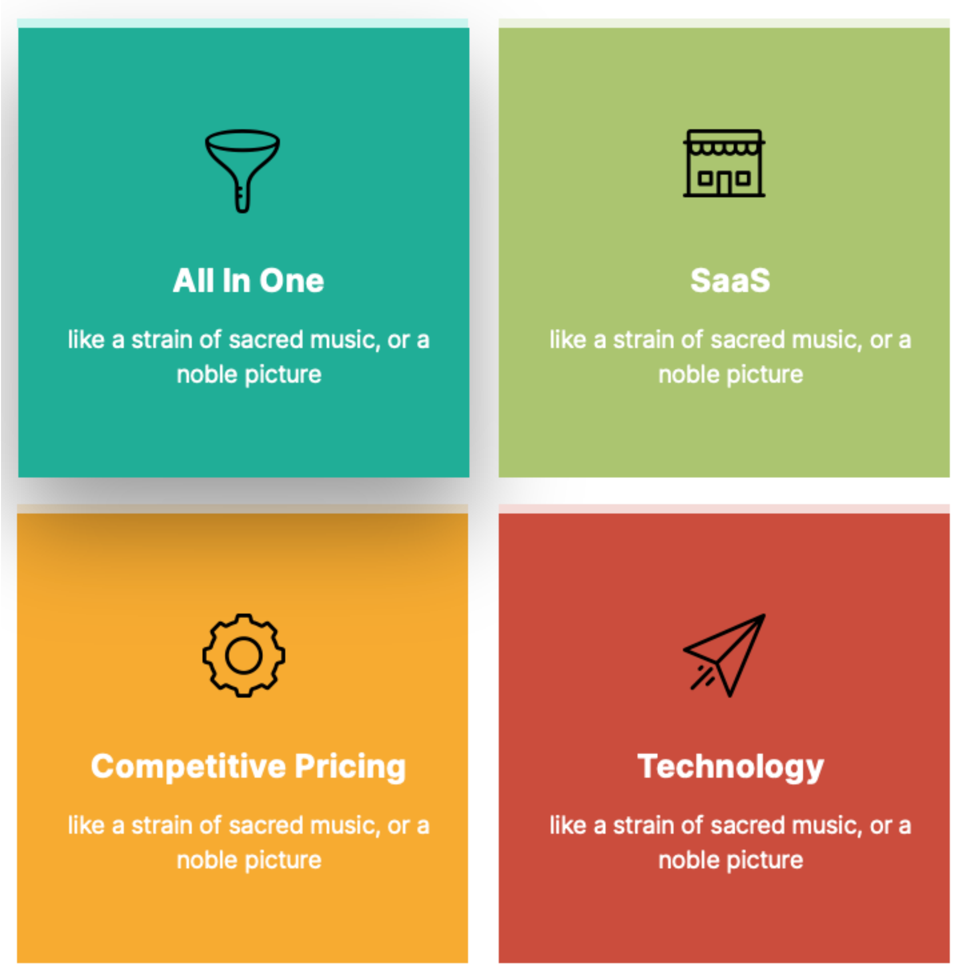
(MDR & MSSP’s Copmapany)

www.redlabis.com

joined their forces for building a global security product.

Effective Approach for Your Cyber Security with CaspiPoT Security Guard

CaspiPoT is an all in one SaaS security solution where you can create your honeypot services within minutes, track the attackers and gather information with attack surface monitoring & breach data control.



All In One

like a strain of sacred music, or a noble picture

SaaS

like a strain of sacred music, or a noble picture

Competitive Pricing

like a strain of sacred music, or a noble picture

Technology

like a strain of sacred music, or a noble picture

A Powerful Defense Against Cyber Attacks

ARE YOU READY FOR CYBER THREATS?

As the digital landscape continues to grow and evolve, so do the threats posed by cyber threats. One of the most important approaches to mitigating these threats is attack surface monitoring, honeypot systems and breach datas. This involves analyzing an organization's entire digital footprint to identify potential vulnerabilities and areas of susceptibility to be exploited by attackers.

The main benefit of honeypot systems is that they allow organizations to detect and analyze attacks in real-time, without compromising their actual systems.

By deploying honeypot systems, organizations can stay ahead of attackers and prevent them from causing any real damage. Additionally, honeypot systems can act as a deterrent to attackers, making it less likely that they will target an organization in the first place.

Vulnerability Detection

Dynamic Environments

Brand Reputation

With planned additions, shadow IT and potential rogue assets the attack surface is constantly evolving.

- ASM is always checking for new servers, sites, domains, subdomains, data leaks and devices that are added (or removed) to the attack surface.

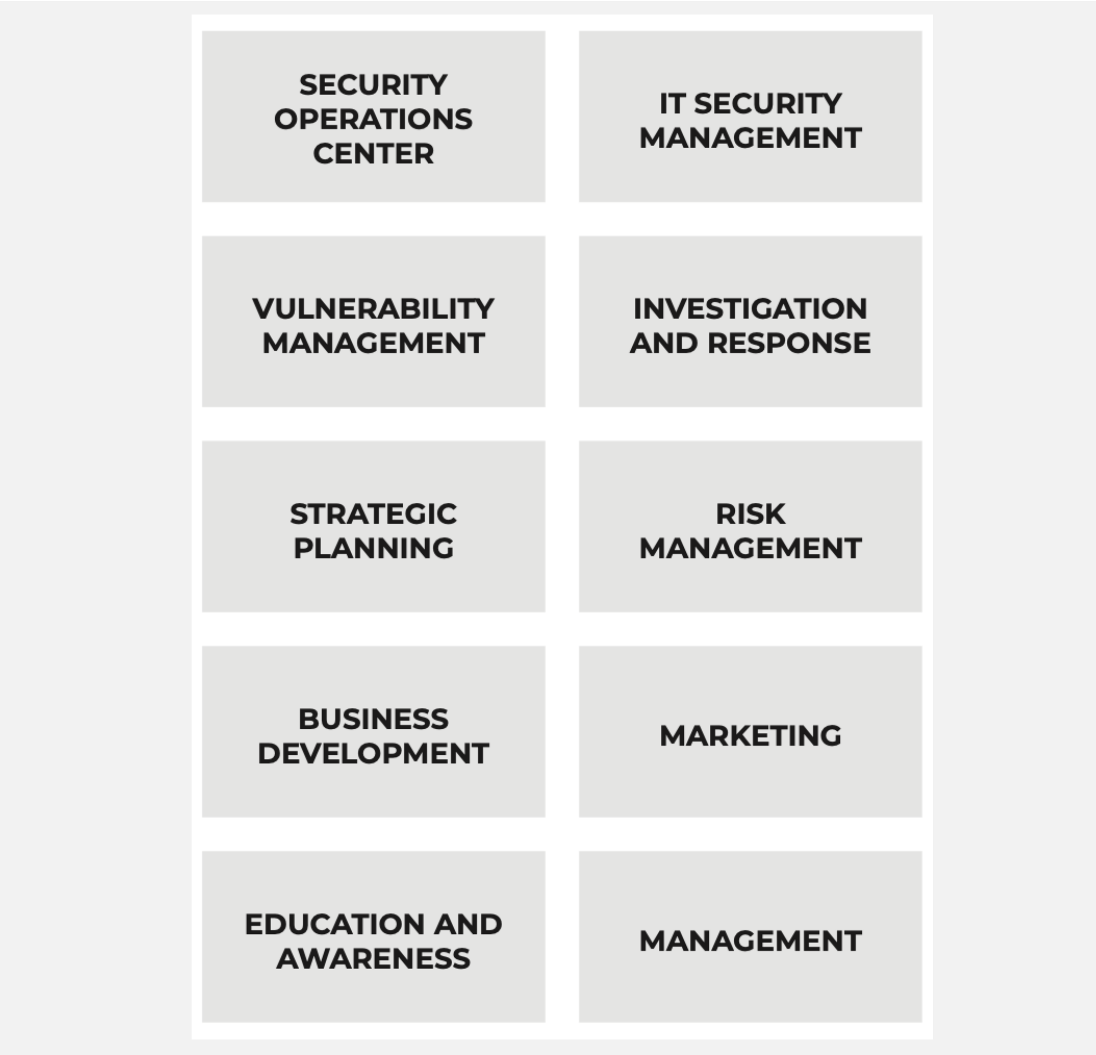
Data breaches and fake web properties are also used by threat actors to affect the cybersecurity of an organization.

- ASM monitors for a company's exposure in any new 3rd party data leaks in addition to providing historical breach information that can impact an organization's cyber risk.

- Identifying active lookalike web properties and determining if they are a malicious or phishing site can also help an organization protect their customers and themselves from threat actors.

Application and device vulnerabilities are the loopholes used by threat actors to gain access to your organization.

- Known items such as web servers, cloud services, VPN's and applications, that the IT and Security teams have inventoried and actively manage.
- Unknown items such as developer test systems, shadow IT services, forgotten services or remote office devices, that IT and security teams are not managing.
- Rogue Assets that have been created by threat actors who have installed malware on your devices or created systems to impersonate your brand.



SECURITY OPERATIONS CENTER	IT SECURITY MANAGEMENT
VULNERABILITY MANAGEMENT	INVESTIGATION AND RESPONSE
STRATEGIC PLANNING	RISK MANAGEMENT
BUSINESS DEVELOPMENT	MARKETING
EDUCATION AND AWARENESS	MANAGEMENT

A honeypot system is a decoy system that is designed to look like a legitimate target for attackers.

The main benefit of honeypot systems is that they allow organizations to detect and analyze attacks in real-time, without compromising their actual systems

By deploying honeypot systems, organizations can stay ahead of attackers and prevent them from causing any real damage. Additionally, honeypot systems can act as a deterrent to attackers, making it less likely that they will target an organization in the first place.

MODULAR STRUCTURE

EASY TO USE

Due to its robust reporting capabilities, it automates and isolates the information required for cyber security procedures.

PROACTIVE

Potential threats from escalating into assaults and causing damage to the company, guarantees early response and avoids probable loss by identifying threats at every level that may disrupt an organization's workflow via the use of strong sensors.

COMPLEMENTARY ACTOR OF YOUR SECURITY

CaspiPoT offers access to all results and unique reports on your company, including those that are currently public. This manner, you may conduct historical analyses of your organization's security processes and develop long-term strategic goals.

ACTIONABLE

Each warning provided from our platform enables you to rapidly react to emerging threats and security vulnerabilities by providing the insight necessary for your operation and minimizing the risks associated with your process. Additionally, it streamlines your process by providing security breach indicators that assist with the assessment, incident detection, response, and investigation tasks required for a secure operation.

Integrations

paloalto NETWORKS

f5

CISCO

FORTINET

SOPHOS

MikroTik

JUNIPER NETWORKS

CLOUDFLARE®

AT&T

LogRhythm

IBM

splunk>

- Open API
- Dashboard
- Alert Notifications
- Daily Reporting

Caspi PoT

www.caspipot.com