Pro CISO ®

PRO CISO®

Cyber Security insights
October 2022

https://prociso.com – LinkedIn - AaaSK@prociso.com

TABLE OF CONTENTS

VULNERABILITIES OF THE MONTH

WHICH SHOULD BE REMEDIATED URGENTLY

“Text4Shell”: A Vulnerability in Java library Apache Commons Text RCE (CVE-2022-42889)

Applications that use the Apache Commons Text library (or that depend on libraries using it) are impacted. This vulnerability, in specific conditions, allows an attacker to execute arbitrary code on the victim's machine (Remote Code Execution or "RCE"). Recommendation: Upgrade to Apache Commons text 1.10.0
Reference:
https://www.lunasec.io/docs/blog/text4shell-java-rce-cve-2022-42889/
https://lists.apache.org/thread/n2bd4vdsgkqh2tm14l1wyc3jyol7s1om

Image src: https://www.lunasec.io/

OpenSSL warns about critical vulnerabilities affecting OpenSSL 3.0 and above

OpenSSL is a software library for applications that secure communications over networks, providing open-source application of the TLS (Transport Layer Security) and SSL (Secure Sockets Layer) protocol. The patch OpenSSL 3.0.7 was released on 01 of November.
We recommend organizations to create inventory their technologies to identify if any are using OpenSSL version 3.0+. Organizations should immediately install it on all affected technologies.

https://www.openssl.org/blog/blog/2022/11/01/email-address-overflows/

Reference: https://www.openssl.org/news/vulnerabilities.html

EMERGING THREATS

New cryptojacking campaign observed targeting vulnerable Docker and Kubernetes infrastructure

Uncovered by CrowdStrike, new campaign called “Kiss-a-dog,” used multiple command-and-control (C2) servers to launch attacks that attempted to mine cryptocurrency, utilize user and kernel mode rootkits to hide the activity, backdoor compromised containers, move laterally in the network and gain persistence.

Reference:
https://www.crowdstrike.com/blog/new-kiss-a-dog-cryptojacking-campaign-targets-docker-and-kubernetes/

Pro CISO® can help you establish and manage Cyber Security resilience program to improve Cyber Security posture of your business.

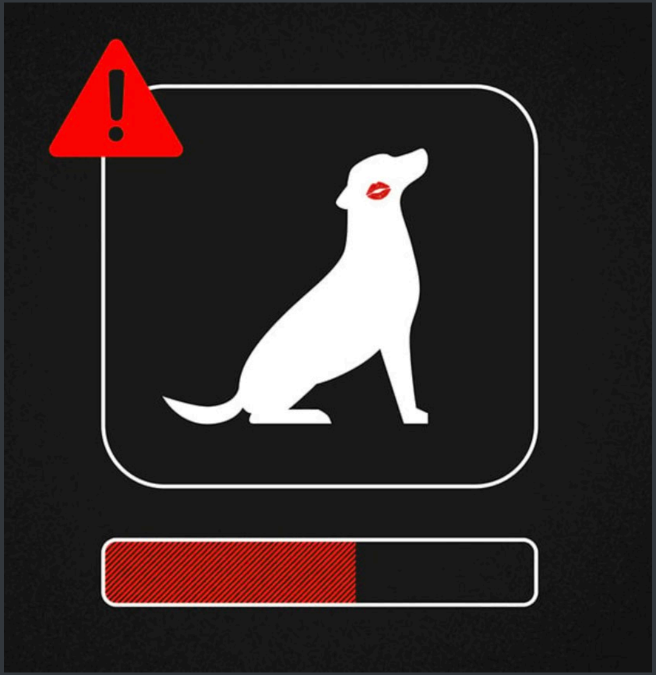


Image src: https://www.crowdstrike.com/

EMERGING THREATS

Microsoft Confirms Azure Misconfiguration Led to 65,000+ Companies' Data Leak

"This misconfiguration resulted in the potential for unauthenticated access to some business transaction data corresponding to interactions between Microsoft and prospective customers, such as the planning or potential implementation and provisioning of Microsoft services" Microsoft said.
Microsoft is directly notifying impacted customers and provided them with instructions for contacting Microsoft with questions or concerns. If you did not receive a Message center communication, the investigation did not identify an impact to you or your organization.

Reference:
https://msrc-blog.microsoft.com/2022/10/19/investigation-regarding-misconfigured-microsoft-storage-location-2/
https://thehackernews.com/2022/10/microsoft-confirms-server.html

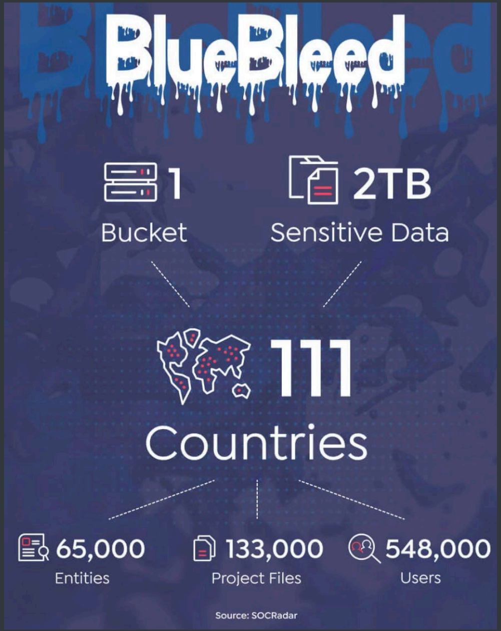


Image src: Socradar.io

Pro CISO® can help you establish and manage Cyber Security resilience program to improve Cyber Security posture of your business.

RANSOMWARE TRENDS

Raspberry Robin malware part of larger ecosystem facilitating pre-ransomware activity

Microsoft has discovered recent activity indicating that the Raspberry Robin worm is part of a complex and interconnected malware ecosystem, with links to other malware families and alternate infection methods beyond its original USB drive spread. These infections lead to follow-on hands-on-keyboard attacks and human-operated ransomware activity. Microsoft revealed that nearly 3,000 devices in almost 1,000 organizations have seen at least one Raspberry Robin payload in the last 30 days.

Reference: https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/

Pro CISO® can help you establish and manage Ransomware resilience program to improve Cyber Security posture of your business.

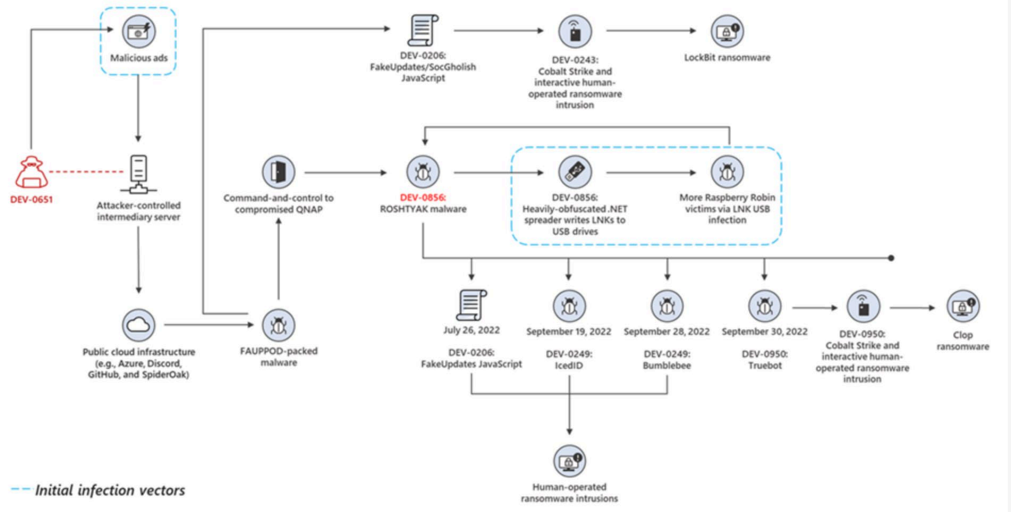

Malicious ads
DEV-0651
Attacker-controlled intermediary server
Public cloud infrastructure (e.g., Azure, Discord, GitHub, and SpiderOak)
FAUPPOD-packed malware
Command-and-control to compromised QNAP
DEV-0206: FakeUpdates/SocGholish JavaScript
DEV-0243: Cobalt Strike and interactive human-operated ransomware intrusion
LockBit ransomware
DEV-0856: ROSHTYAK malware
DEV-0856: Heavily-obfuscated .NET spreader writes LNKs to USB drives
More Raspberry Robin victims via LNK USB infection
July 26, 2022
DEV-0206: FakeUpdates JavaScript
September 19, 2022
DEV-0249: IcedID
September 28, 2022
DEV-0249: Bumblebee
September 30, 2022
DEV-0950: Truebot
DEV-0950: Cobalt Strike and interactive human-operated ransomware intrusion
Clop ransomware
Human-operated ransomware intrusions
Initial infection vectors

Image src: https://www.bleepingcomputer.com/

CYBERSECURITY ADVISORIES

Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization

From November 2021 through January 2022, CISA responded to advanced persistent threat (APT) activity on a Defense Industrial Base (DIB) Sector organization's enterprise network. During incident response activities, CISA uncovered that likely multiple APT groups compromised the organization's network, and some APT actors had long-term access to the environment. APT actors used an open-source toolkit called Impacket to gain their foothold within the environment and further compromise the network, and also used a custom data exfiltration tool, CovalentStealer, to steal the victim's sensitive data.
Reference: https://www.cisa.gov/uscert/ncas/alerts/aa22-277a

Top CVEs Actively Exploited By People's Republic of China State-Sponsored Cyber Actors

This joint Cybersecurity Advisory provides the top Common Vulnerabilities and Exposures (CVEs) used since 2020 by People's Republic of China (PRC) state-sponsored cyber actors as assessed by NSA, CISA, FBI. PRC state-sponsored cyber actors continue to exploit known vulnerabilities to actively target U.S. and allied networks as well as software and hardware companies to steal intellectual property and develop access into sensitive networks.
Reference: https://www.cisa.gov/uscert/ncas/alerts/aa22-279a

#StopRansomware: Daixin Team

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and Department of Health and Human Services (HHS) are releasing this joint advisory to provide information on the "Daixin Team," a cybercrime group that is actively targeting U.S. businesses, predominantly in the Healthcare and Public Health (HPH) Sector, with ransomware and data extortion operations.
Reference: https://www.cisa.gov/uscert/ncas/alerts/aa22-294a

PRO CISO® MANAGED VULNERABILITY MANAGEMENT

VULNERABILITY SCANNING

Frequent scans of infrastructure, applications and the Cloud for new vulnerabilities

PRIORITIZE PATCHING

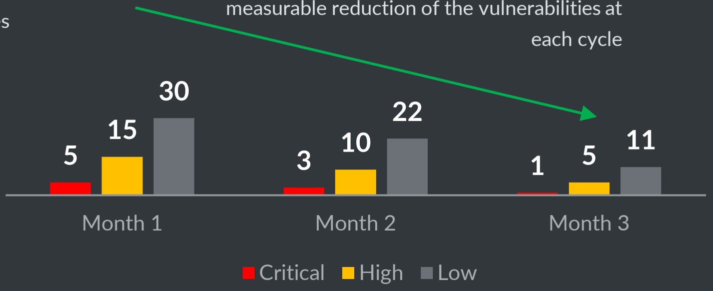
Personalized recommendations for implementing remediation actions based on severity, criticality, exposure, exploitability.

THREAT INTELLIGENCE

Proactive alerting of new exploits, zero-days, via the Pro CISO® Threat Intelligence Alerting service

VULNERABILITY EXPOSURE REDUCTION

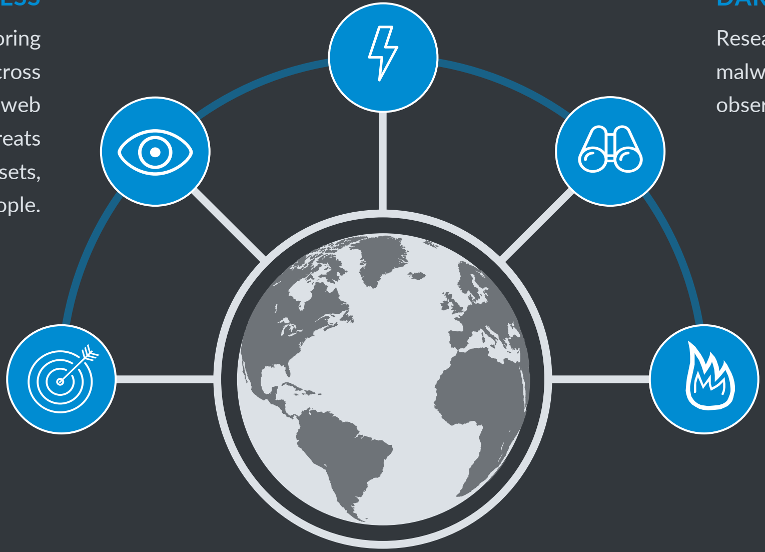
Drives effective IT patching, provides measurable reduction of the vulnerabilities at each cycle



Pro CISO® Managed VM

Powered by Qualys.

PRO CISO® MANAGED THREAT INTELLIGENCE SERVICE



THREAT ALERTING

Identification of potential attacks, data leakage, brand imitation and reputation, phishing attacks, external system vulnerability and VIP alerts to classify and respond to targeted threats.

OPERATIONAL AWARENESS

Reconnaissance and active monitoring of thousands of threat sources across the surface, deep and dark web produces real-time visibility into threats targeting your network, brand, assets, and people.

DARK WEB AND OSINT

Research the latest trends including malware, campaigns, TTPs, IOCs, and observables.

EXTERNAL EXPOSURES

Continuous monitoring and analysis of the company's domains, IP addresses, DLP indicators, mobile applications, social media pages, secret projects, technologies in use, VIP names and emails to identify and validate threats to the organization.

PRODUCT EXPLOITATION

Detection of product and supply chain exploitation techniques, PoCs and attacks.

Pro CISO® Managed TI

Powered by munitio SAGA®

PRO CISO® MANAGED PRIVILEGED ACCESS

RAPID INTEGRATION

Leveraging the flexibility of the Cloud, you can rapidly and progressively integrate infrastructure and systems with the PAM solution

CONTROL ACCESS

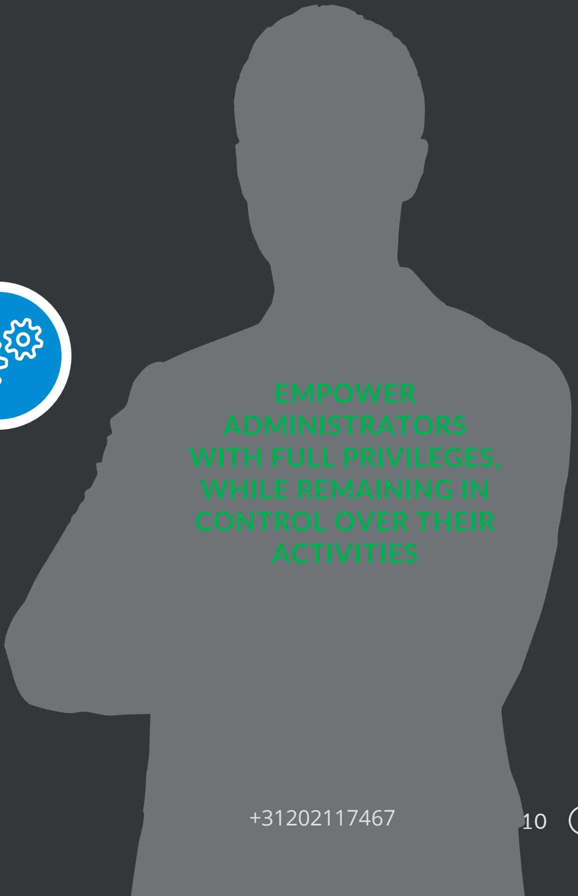
Centrally manage administrator and 3rd party access only to the authorized resources

MONITOR ACTIVITY

Register all activities performed by administrators, for review preventively or in reaction to an incident

Pro CISO® Managed PAM

Powered by cyberelements



EMPOWER ADMINISTRATORS WITH FULL PRIVILEGES, WHILE REMAINING IN CONTROL OVER THEIR ACTIVITIES

PRO CISO® MANAGED ZERO TRUST NETWORK ACCESS

Seamless employee and 3rd party secure remote access to company applications and assets that are hosted on-prem or in the Cloud

VPN REPLACEMENT

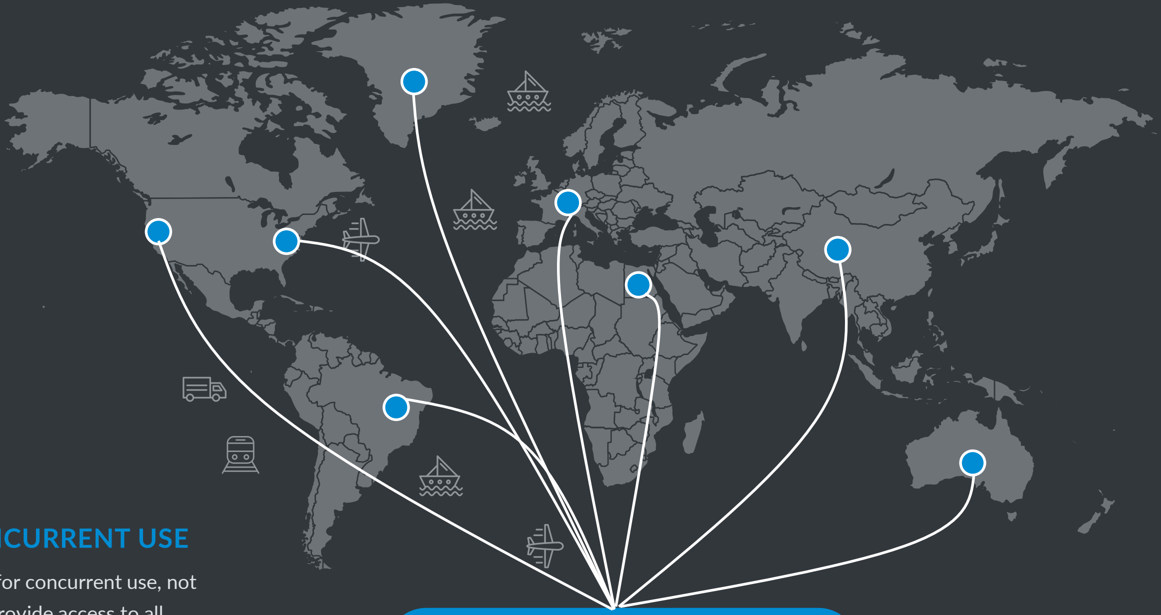
ZTNA provides granular access only to specific applications and individual systems, not the entire network, as do VPN solutions.

COMPROMISE MITIGATION

ZTNA will identify malicious traffic generated by a compromised laptop and isolate it from the network.

PAY PER CONCURRENT USE

Customers only pay for concurrent use, not the total users. Provide access to all employees and 3rd parties, but only pay the peak concurrent usage of the service.



Pro CISO® Managed ZTNA

Powered by cyberelements

PRO CISO® SECURITY TESTING

Security testing based on industry standards, tools and methodologies

HARDWARE TESTING

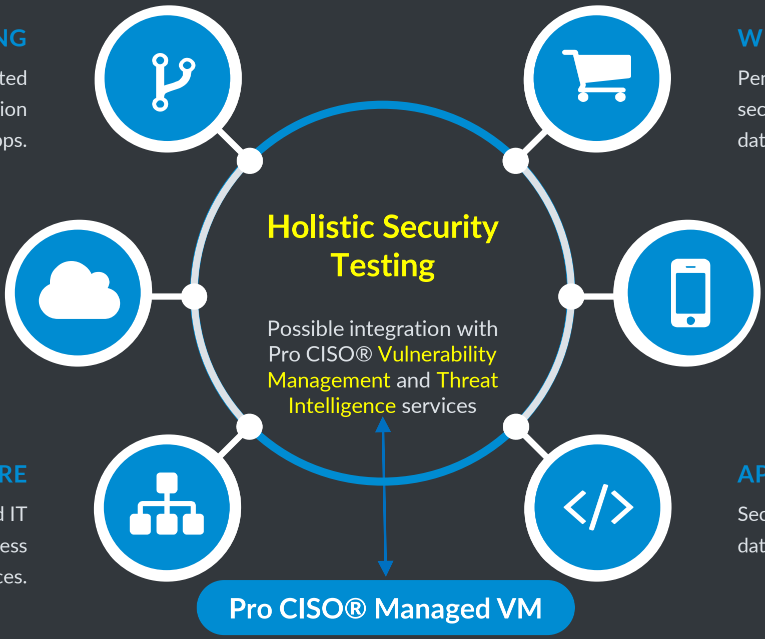
Physical security testing of IoT devices and connected consumer products, including end-2-end integration with the backend and the frontend mobile apps.

CLOUD SECURITY POSTURE

Review of the security posture of the Customer's public cloud implementation to identify exposure of data and incorrect security configurations.

INFRASTRUCTURE

Security review of the on-prem Security, Network and IT infrastructure, to verify the presence and effectiveness of security controls and best practices.



Holistic Security Testing

Possible integration with Pro CISO® Vulnerability Management and Threat Intelligence services

Pro CISO® Managed VM

WEB APP PENTESTING

Penetration testing of web applications to identify security flaws that could be used by attackers to exfiltrate data or gain access to the network.

MOBILE APP PENTESTING

End-2-End testing of mobile apps to verify the overall security of the app on the device and the integration with its backend or connected device.

API TESTING

Security testing of APIs exposed by Customers when sharing data with partners or integration with mobile apps.

PRO CISO® RANSOMWARE READINESS ASSESSMENT

Hands-on methodology to assess and quickly mitigate the specific risks that a Customer would be exposed to, when facing a ransomware attack

01 ASSESS CROWN JEWELS

Determine the most important data and assets that are vital for the Customer's business. Identify the types of data and the subjects authorized to access them.

02 ASSESS THE ATTACK SURFACE

Perform threat modeling exercises to identify the attack vectors that the Customer is exposed to because of the nature of its business and how it operates.

03 MAP EXISTING CONTROLS

Verify the effectiveness of the existing security controls, backup strategy, with regards to a possible ransomware attack perpetrated by a threat actor.

04 SUGGEST MITIGATIONS

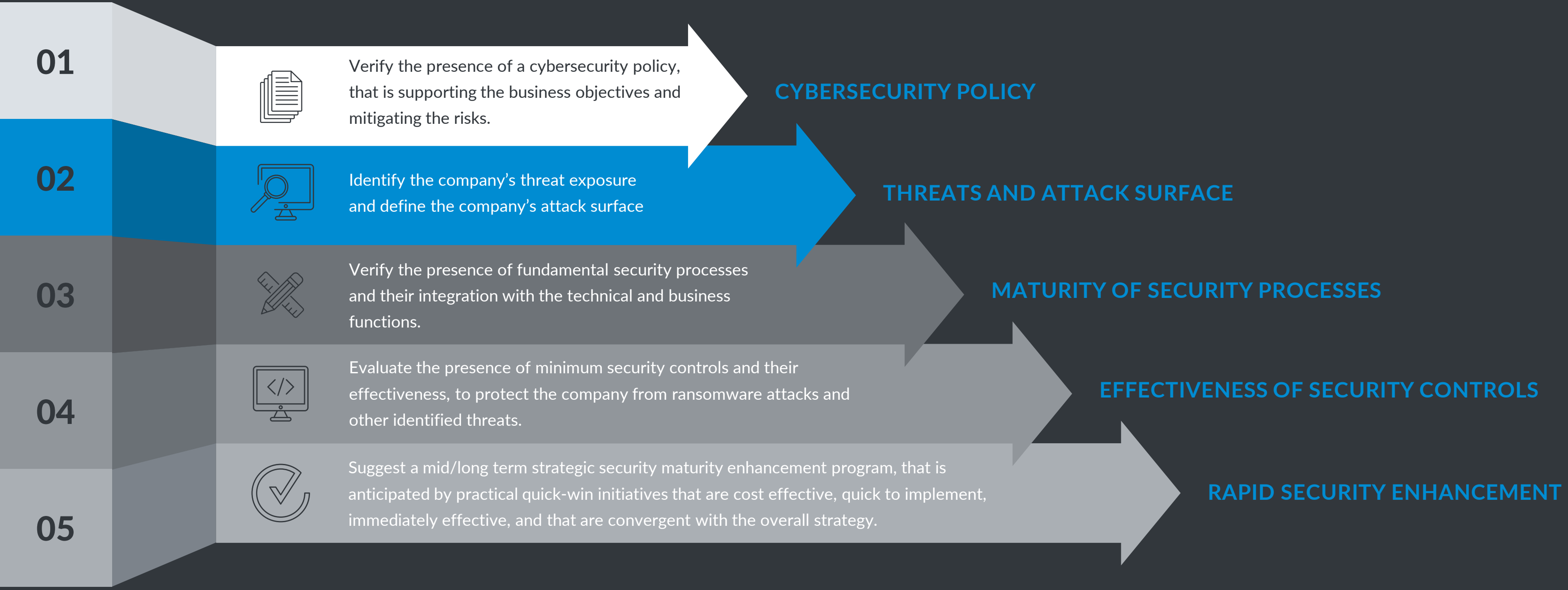
Identify the most appropriate security controls, tactical quick-wins, and their priority, to minimize the impact of a ransomware attack.

05 ATTACK SIMULATION

Simulate a realistic attack scenario, to verify the actual readiness of the organization for responding to a Ransomware attack.

PRO CISO® CYBER INSURANCE READINESS

Prioritized cybersecurity enhancement program that will facilitate response to formal insurance requirements and reduce the premium, while rapidly elevating resilience to cyber attacks.



01 Verify the presence of a cybersecurity policy, that is supporting the business objectives and mitigating the risks.

CYBERSECURITY POLICY

02 Identify the company’s threat exposure and define the company’s attack surface

THREATS AND ATTACK SURFACE

03 Verify the presence of fundamental security processes and their integration with the technical and business functions.

MATURITY OF SECURITY PROCESSES

04 Evaluate the presence of minimum security controls and their effectiveness, to protect the company from ransomware attacks and other identified threats.

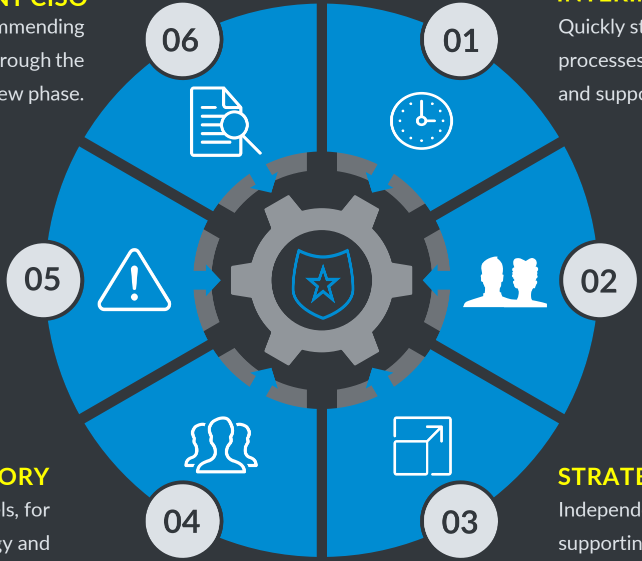
EFFECTIVENESS OF SECURITY CONTROLS

05 Suggest a mid/long term strategic security maturity enhancement program, that is anticipated by practical quick-win initiatives that are cost effective, quick to implement, immediately effective, and that are convergent with the overall strategy.

RAPID SECURITY ENHANCEMENT

PRO CISO® VIRTUAL CISO

Rapidly introduce an experienced Chief Information Security Officer (CISO) into the organization, as a virtual role, or as an interim one, while in the process of hiring the permanent CISO.



01 INTERIM CISO

Quickly step into a vacant CISO role, review the business processes and related security risks, cover the daily activities, and support the CISO hiring process.

02 DEPUTY CISO

The wing-man to the overloaded CISO, executing the defined security program, or offloading the governance of very broad and complex projects.

03 STRATEGY REVIEW

Independent review of the cybersecurity strategy and supporting program, that has the objective of protecting the business from cyber threats.

04 BOARD ADVISORY

Advisor to the Board of Directors or C-Levels, for suggesting the most effective cybersecurity strategy and for recommending the most cost-efficient solutions for the specific business and regulatory context.

05 PRACTICAL GUIDANCE

Provide an immediate solution to a burning problem, by recommending or implementing practical security remedies that are quick to implement, require low resources and that are effective and efficient.

06 HIRE THE PERMANENT CISO

Support the CISO hiring process, by recommending candidates and/or providing support through the interview phase.

CONTACT US

PRO CISO®

Cybersecurity insights

Threat Intelligence
powered by
SAGA®

munitio

AaaSK@prociso.com
https://prociso.com
LinkedIn

+31202117467