ABC CORPORATION

Cliente: XYZ Group **Empresa: GDSA Corp**

November 2025 - XYZ Group

Cyber Hygiene Report

Summary

Executive Summary

The Cyber Hygiene Report presents a summarized overview of the threat hunting efforts performed by the GDSA Group Team to evaluate the cyber hygiene status of the XYZ Group Corporation’s, environment. Leveraging their cybersecurity expertise, the Threat Hunting Team conducted these operations with the main objective of detecting and addressing possible external threats, unauthorized system changes, network misuse, privileged software exploitation, and security circumventions. The insights and suggestions detailed in this document are intended to strengthen the overall security posture and support a resilient cyber hygiene program for our clients.

Technical Summary

Tools commonly associated with cyber threats can pose serious risks to corporate environments, even when used with legitimate intent. These tools often offer capabilities that bypass traditional security controls, making them attractive not only to administrators but also to adversaries. Their presence in the environment without proper justification, control, and monitoring can create blind spots in detection and increase the likelihood of successful attacks.

Focus: Discovery Phase

In the Discovery phase, adversaries seek to map the internal environment to identify hosts, users, services, and system configurations. This reconnaissance step allows them to understand how the environment is structured and how best to move laterally or escalate privileges. When tools capable of performing these actions are left unchecked, they may enable silent exploration and planning of future attacks. It is therefore crucial to review and restrict their usage and to monitor any unexpected behavior as part of a strong defensive posture.

Tools Found

Discovery Tools:

Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act. They also allow adversaries to in order to discover how it could benefit their current objective.
explore what they can control and what's around their entry point. Native operating system tools are often used toward this post-compromise information-gathering objective.
Tools found in the environment:

- Advanced IP Scanner: 100 host(s)
- Lansweeper: 1 host(s)
- PDQ Inventory: 1 host(s)
- RVTools: 48 host(s)
- S3 Browser: 2 host(s)
- dsquery: 5 host(s)
- nmap: 94 host(s)

Operational Update: Previous vs Current Week

New tools added in the environment:

- Advanced IP Scanner: 22 hosts
- RVTools: 2 hosts
- S3 Browser: 1 hosts
- dsquery: 1 hosts
- nmap: 6 hosts

Tools removed from the environment:

- Advanced IP Scanner: 27 hosts
- RVTools: 2 hosts
- S3 Browser: 1 hosts
- dsquery: 1 hosts
- nmap: 17 hosts

Final Recommendations – XYZ Group Corporation

To further strengthen the cyber hygiene of the XYZ Group environment, we recommend the following actions:

EDR

- Ensure deployment of EDR agents across all organizational assets.
- Ensure deployment of EDR agents across all organizational assets.
- Maintain a routine schedule for reviewing and updating all EDR agents.
- Apply preventive policy configurations carefully to the agents, balancing security with operational continuity to avoid unintended business disruptions.

Privileged Applications

- Enforce the Principle of Least Privilege (PoLP), granting access to privileged applications strictly based on user roles and responsibilities.
- Keep privileged applications regularly updated and patched, ensuring known vulnerabilities
are addressed and the latest secure versions are in use.
- Implement strong access controls, including multi-factor authentication and strict authorization rules, to protect access to these applications.
- Implement strong access controls, including multi-factor authentication and strict authorization rules, to protect access to these applications.
- Utilize secure communication protocols such as encrypted channels for activities like file sharing, data transfer, and remote system administration.
- Conduct periodic security evaluations of privileged applications to detect and resolve configuration issues or potential security gaps.