Security Configuration Management

White Paper

Doc: GYT-MKT-004
Release: 02
Date: 26th January 2022

Confidential: GYTPOL and approved recipients

Total pages:	5

Doc. Title:	Security Configuration Management Whitepaper

Doc. No.:	GYT-MKT-004	**Classification:**	Confidential
Revision:	02	**Restriction:**	GYTPOL and approved recipients
Date:	26th January 2022	**Customer:**	

Owner:	Matthew Album	**Reviewers/ Approvers:**	Yakov Kogan Gilad Raz Tal Kollender
Author:	Matthew Album		

Background

These days, cyber security is often an agenda item at the board level of organizations, and it is gaining importance. Fueled by the continuous reporting of successful cyber-attacks, where organizations in both the private and public sector have had their operations paralyzed, or their valuable data stolen. The remedy is often to pay the ransom demand in untraceable crypto currency or face the alternative, which has a much higher cost to the organization.

The executive board will allocate limited budget funds and will hire a Chief Information Security Officer (CISO) with a clear objective, to ensure their organization will not be the next victim of a cyber-attack.

Seasoned CISOs will adopt an established security framework, select a set of IT Security tools, and implement a robust set of procedures and controls to minimize their attack surface (amongst other things). Yet, even with all these security defense systems in place, organizations still suffer major cyber-attacks.

A major reason for this is due to what is often referred to as bad cyber hygiene. A key element of this revolves around security gaps due to **misconfigurations.** This is a neglected attack vendor in most organizations. As a result of this, hackers exploit misconfigurations which now play a part in nearly every successful cyber-attack.

This paper describes how Misconfigurations can be both predicted and remediated in an automated manner by using a Security Configuration Management Platform.

How Hackers Think

GYTPOL researched the techniques used by different types of hackers and security professionals in both the military, enterprise and "dark web" sectors. We analysed information related to successful attacks and the lessons learned resulting from them.

The results showed a common pattern.

1. **Endpoints are the Entry Points** – Hackers use endpoints as the gateway into an organization. Typically, the PC / laptop used by an employee. Malware or email phishing are the well-known attack techniques which are now commonly protected by tools. However, hackers are now regularly exploiting misconfigurations to crack these devices and with a general shift to hybrid working, breaching the home network environment makes it an easy job for the hacker.

2. **Lateral Movement** – Once the endpoint has been breached, the objective of the hacker is to reach the heart of the organization's IT environment where they will execute the cyber-attack. Typically, the targets are infrastructure services such as the Active Directory, Domain Controllers but also Database Servers, Web Servers and Cloud Workloads. This is achieved by performing lateral movement. Hackers will scan and detect for OS misconfigurations and human errors to gain access and elevated privileges to achieve this goal.

Overall, from the point of breach, a hacker will be plotting inside a network from 3-9 months before executing the attack.

What are Misconfigurations

The National Institute of Standards and Technology (NIST) defines misconfigurations as "*A setting within a computer program that violates a configuration policy or that permits or causes unintended behavior that impacts the security posture of a system*"

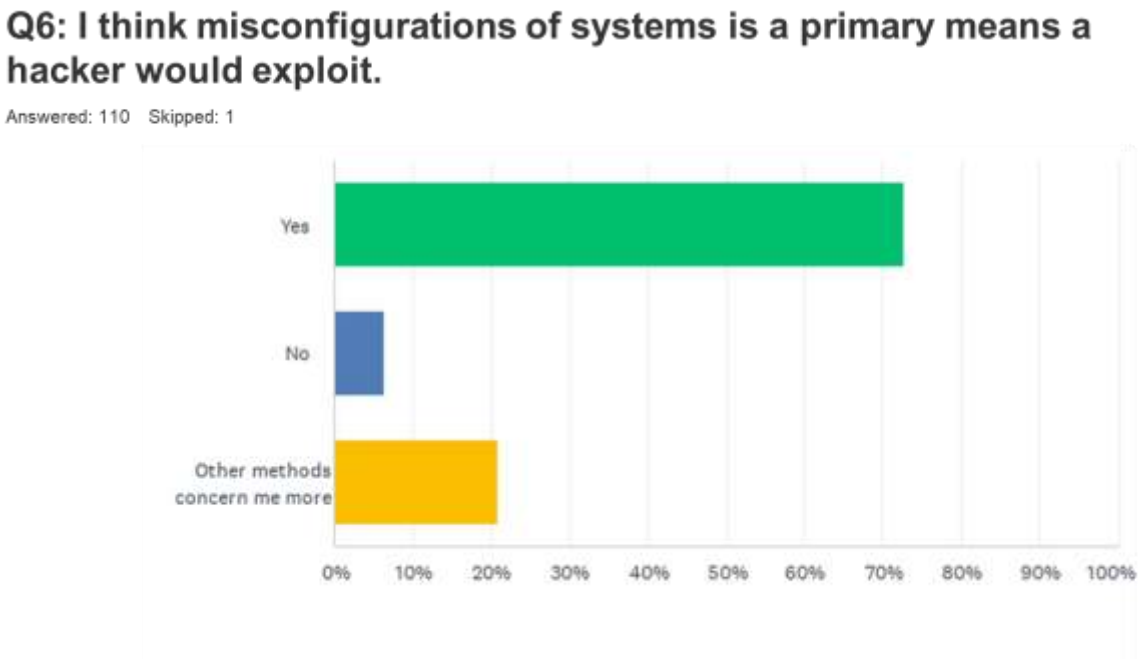
There are numerous root causes of misconfigurations, some of which are shown in the diagram above.

GYTPOL's research determined that ***default settings*** and ***human errors*** in both Operation Systems and Service Infrastructures are the most important and critical misconfigurations which are targeted by hackers.

Security Configuration Management is important

The MITRE ATT&CK[1] is a popular framework and fast becoming a de facto standard used by IT Security professionals to map all the different categories of attacks that are known to us. The CISO will use this to select the right combination of tools and controls to provide protection coverage and reduced attack surface. The framework identifies many categories related to misconfigurations, yet the common IT Security tool used by organizations especially for endpoint protection do not provide coverage for misconfigurations.

A report conducted by Dr Chase Cunningham (formerly a senior security analyst at Forrester) which surveyed IT Security professionals said that 80% of the respondents felt that misconfigurations are a primary means that a hacker would exploit.



Other reports conducted by IBM[2] on thousands of customers in over 130 countries found that "***Human Error*** *was a major contributing cause in 95% of all breaches*". Similar finding was reported by the European Union Agency for Cybersecurity (ENISA) Report[3] that "*In 2020 and 2021, we observed a spike in non-malicious incidents, as the COVID-19 pandemic became a multiplier for* ***human errors and***

***system misconfigurations**, up to the point that most of the breaches in 2020 were caused by errors.*"

Challenges in Security Configuration Management

Security gaps due to misconfigurations are a well-known attack vector in the IT Security community. It is a pain-point where CIOs and CISO's are challenged with finding a robust and reliable solution which can provide both the visibility and remediation capability.
One common use case for Security Configuration Management is the need to enforce security baselines.

Defining Security Baselines.

There exist several different definitions as to what constitutes a Security Baseline. For our purposes, it can be considered as a minimum set of security controls required for all endpoint PCs and Servers in an organization. Baselines for these devices are created with hardened *golden images* wrapped around a set of security policies. To define this baseline, organizations will adopt well known standards such as CIS, NIST, ISO 27001 etc.

Whilst these are necessary starting points, these standards struggle to keep up to date with the fast-moving trending techniques of hackers. Once a hacker identifies (for example through social engineering) that an organization is using one of the standards in their baselines, they will exploit the weakness in those standards to easily breach them.

Organizations can enhance their security baseline by adding an additional layer of security controls on top of the compliance standards. To achieve this, it needs to be frequently updated to remain current by having the relevant knowledgeable security experts and the associated cost required of implementing the controls.

GYTPOL

Enforcing Security Baselines.

Defining a robust and effective security baseline is only one part of the story. You need to ensure it is always enforced on all your endpoints and servers. This requires:

- Continuous monitoring on all devices at all times to validate they are all compliant in accordance with your security baseline.
- Devices that are not compliant, need to be rapidly remediated, preferably in an automated manner without causing any impact.

Without a Security Configuration Management platform, both these points bring serious challenges to organizations.

Pen-testing procedures with either red team (offensive security focused) or blue team (defensive security focused) are limited as they normally focus on a small sample of devices (as opposed to all devices). Pen-testing are also one-time events carried out 2-4 times a year as opposed to continuous monitoring. Remediating devices which are non-compliant requires a time consuming and resource intensive activity. The larger the organization, the longer it takes to remediate all non-compliant devices. As this time gap widens, it increases the risk exposed to the organization. Remediation also comes with it's own risks such as knowing whether the resulting fix will impact an existing (legacy) application or business operation.

GYTPOL Validator

GYTPOL Validator is a Security Configuration Management platform. It has been designed to enable organizations to deploy robust security baselines and ensure all devices always remain compliant with automated, zero impact remediation.

Some highlights of GYTPOL are described below:

Security Baseline Definition

- Uses hacker logic to include the most important and critical security controls.
- Includes hundreds of unique indicators.
- Regular updates to the definition ensure the baselines are the latest and most relevant.
- Support for standard definitions such as CIS, ISO 27001 etc.

Enforcing Security Baselines

- 24x7 Continuous monitoring and visibility of all endpoint PC devices and Servers which is lightweight and uses minimal resources. Including remote devices which are off network.
- 24x7 Continuous monitoring of infrastructure service components (eg Active Directory)
- Full Remediation capabilities including:
    - **Rapid** remediation for all devices.
    - **Automate.** Option to automate remediation when devices fall out of compliance.
    - **Predictive Impact.** Provides indicators so you can confidently remediate without impact.
    - **Undo.** Revert to previous state.

References

1. MITRE ATT&ACK Framework

   https://attack.mitre.org/

2. IBM Cyber Security Intelligence Index Report.

   https://thehackernews.com/2021/02/why-human-error-is-1-cyber-security.html

3. ENISA Threat Landscape 2021

   https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021