Case Study:
How GYTPOL Revolutionized Security Management for a Large Credit Union with 4000 Employees

Customer Profile

A Large Credit Union, a significant financial institution in the US, boasts an expansive national network of branches.
It employs a dedicated team of 5,000 +, operating multiple data centers to cater to a diverse client base.

The Challenge

The Credit Union faced a lack of consistency concerning security policies and configurations.
They needed a tool capable of detecting and swiftly remediating vulnerabilities with minimal disruption to ongoing operations. In addition, they needed an automatic remediation system for misconfigurations.

The Solution

Two years ago, after weeks of extensive research, the credit union discovered GYTPOL, a security misconfiguration tool offering visibility into their security framework, rapid vulnerability remediation, and automatic adjustment of misconfigurations.
They've been a customer since.

With GYTPOL, the credit union has managed to:

- Detect vulnerabilities due to misconfigurations and easily identify underperforming GPOs and discrepancies between GPO definitions and actual policies.
- Validate the status of their configurations across the entire network, including workstations, servers, Mac, Linux, VDIs, and Active Directory.
- Quickly identify and address Zero-Day vulnerabilities without any negative impacts.
- Quickly able to cross-reference findings from Red team exercise, utilizing GYTPOL to auto-remediate, zero impact, one-click
- Despite having other tools like EDR, VA, and PenTesting, the credit union found unique value in GYTPOL.
  It provided comprehensive knowledge-based explanations of risk exposures, enabling swift remediation, and reversals, if necessary, for a broad range of vulnerabilities.

Case Study:
How GYTPOL Revolutionized Security Management for a Large Credit Union with 4000 Employees

Results

When faced with internal and regulatory audits related to desktop and server configurations, the credit union was well-equipped with GYTPOL.
It allowed them to promptly present auditors with evidence of their control status and performance across all desktops and servers.

The credit union also saved 16 weeks in remediation time this year alone and is on track to save an estimated three years and 31 weeks of time and resources by using GYTPOL instead of traditional remediation tools.

"Internal audit teams and now the regulators have begun audits on us related to configurations of desktops and servers," says the credit union's CISO. "GYTPOL solution [is the] perfect answer to their questions and demonstrate the effectiveness [in] handling misconfigurations since you can't patch and must fix."

Further, the CISO commented, "If any one of your controls fails, like EDR, or you have an insider, then GYTPOL is [the] last line of defense."

Moreover, GYTPOL's remediation capabilities ensure operational changes were made without disrupting the workflow.
The credit union performed numerous remediations using GYTPOL, and its built-in revert feature acted as a safety net, assuring the credit union could return to the pre-remediation state if necessary.

A significant test of GYTPOL's remediation capabilities arose when handling a large-scale Log4J vulnerability. GYTPOL streamlined the remediation process, proving more efficient than any other solution on the market.

While other vulnerability tools produced false negatives, GYTPOL accurately identified and addressed the vulnerability from the outset.

Conclusion

In the dynamic financial technology landscape, the Large Credit Union found a reliable partner in GYTPOL. By significantly enhancing security management and audit readiness, the credit union now stands better prepared for cybersecurity challenges, thereby safeguarding its reputation and the trust of its clientele. This case study demonstrates the power of a strategic technological partnership in fortifying defenses and streamlining operations.