Attestation of Security Assessment

14 January 2025

PROJECT DEFINITION AND SCOPE OVERVIEW

TrueBlue, Inc. ("TrueBlue") engaged GuidePoint Security, LLC ("GuidePoint") to perform an External Penetration Test of TrueBlue's perimeter network assets associated with the Enterprise network. An External Penetration Test is comprised of automated and manual activities that focus on the discovery, target profiling, target examination, risk validation, impact evaluation, and remediation assurance of TrueBlue's external information assets. The scope of this assessment included 22 network ranges and 525 individual IP addresses. From the in-scope assets given, GuidePoint discovered 281 live hosts.

Testing was conducted between September 23 and October 1, 2024. This assessment was conducted using a hybrid-evasive approach. In this approach, the assessment begins with TrueBlue's defensive teams having minimal internal knowledge that the assessment is taking place and GuidePoint uses techniques to avoid detection or triggering security controls. Once this phase is complete, controls are configured to only provide alerts for suspicious activities originating from GuidePoint without interfering with the testing. This configuration gives the organization visibility into the effectiveness of its security monitoring capabilities while allowing the rest of the assessment to continue in the most efficient way possible to maximize value.

FINDINGS AND RECOMMENDATIONS

After the external penetration test concluded on October 1, 2024, GuidePoint determined that two high-risk, and four low-risk findings were present in the TrueBlue environment. TrueBlue immediately performed remediation activities based on GuidePoint's recommendations. TrueBlue then requested that GuidePoint evaluate remediation efforts to determine whether any of the previously identified vulnerabilities continue to pose a risk to the target environment.

GuidePoint performed post-remediation testing on January 13-14, 2025, and confirmed that of the six findings found in the initial assessment, both high-risk and two low-risk findings have been completely remediated. The remaining two low-risk findings are marked as "untested" for the assessment. The TrueBlue team has provided accompanying information which has been documented in a management note and compensating control.

APPROACH

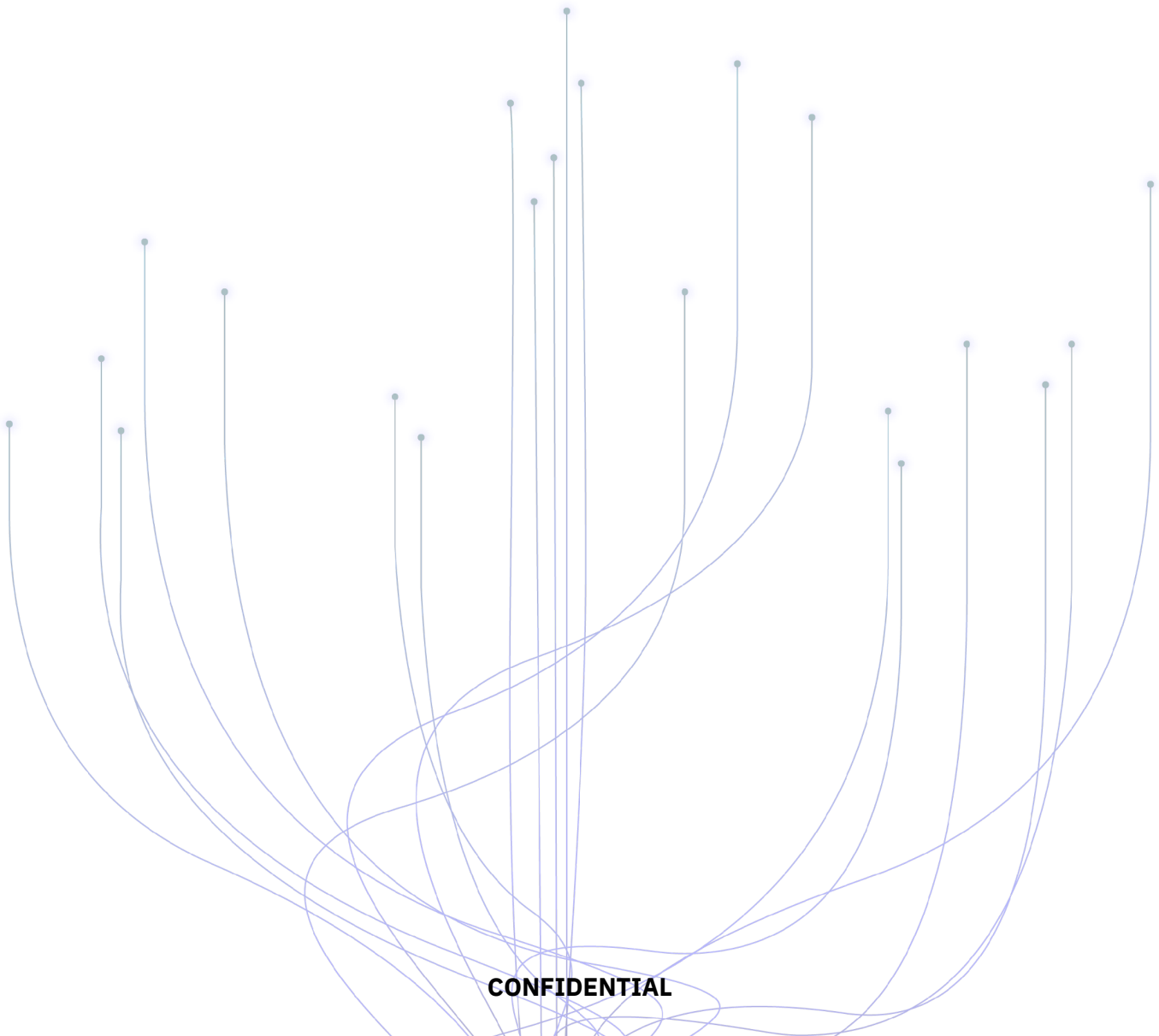
The following summarizes the details of the scope and approach of this assessment.

Assessment Scope and Approach Summary	
Discovered Live Hosts	281
Information Disclosure	Partial-Visibility
Evasive Technique	Hybrid-Evasive

REMEDIATION SUMMARY

GuidePoint conducted remediation testing between January 13-14, 2025, to verify the remediation status of the originally identified findings. The table below summarizes the current state of these findings based on the observations made by GuidePoint during post-remediation testing:

High	Medium	Low	Total
0	0	2	2



Appendix A: Finding Severity Definitions

The severities listed below are specific to GuidePoint's network penetration testing activities performed by the Threat & Attack Simulation team. While these severities may coincidently align with other sources, GuidePoint uses our understanding of the findings, the context of the affected hosts, and the tactical ability to perform exploitation to determine each severity level. Any variation in the items mentioned would impact the specific finding's severity. Because of this real-world analysis, our assessment's severities may differ greatly from non-exploitation-based assessments such as risk assessments and vulnerability scans.

Severity	Defining Characteristics
High	• GuidePoint directly leveraged this finding to achieve user, system, or sensitive information compromise • The finding indicates systemic deficiencies in critical and fundamental security functions
Medium	• Exploitation did not lead to user, system, or sensitive information compromise • Exploitation required the presence of additional vulnerabilities or specific circumstances for success • Exploitation will lead to a loss of service or system availability but requires significant resources
Low	• Exploitation resulted in the minor exposure of non-sensitive assets or information • Exploitation of the finding was possible but extremely unlikely given the conditions needed • Could be used by a persistent attacker to improve the efficacy of social engineering attacks

Note: While a finding may meet multiple of these criteria, one match in the highest category is sufficient to rate the finding that severity.