PICUS

BLUE REPORT 2024

The State of Threat Exposure Management

40% of Environments are Vulnerable to Full Take Over

EXECUTIVE SUMMARY

Introduction

Now in its second year, the Blue Report 2024 aims to provide key findings and practical recommendations for cybersecurity professionals by evaluating the effectiveness of current cybersecurity detection and prevention practices. Conducted by Picus Labs and Picus Data Science teams, this annual study uses over 136 million attack simulations on the Picus platform to assess the real-world performance of security products. These simulations cover a diverse variety of attack vectors, threat groups, ransomware attacks, vulnerabilities, and more - highlighting both progress and ongoing challenges in threat detection and prevention.

This year's edition introduces results from the Attack Path Validation (APV) and Detection Rule Validation (DRV) products on the Picus platform, offering deeper observations into organizational preparedness against automated penetration tests and the effectiveness of detection rules in SIEM systems.

The Blue Report 2024 serves as a crucial resource for cybersecurity professionals and decision-makers. It provides perspective into the current state of cybersecurity and recommends Continuous Threat Exposure Management (CTEM) for those working to adopt a holistic approach. By addressing the outlined defensive gaps and optimizing detection and prevention strategies, organizations can enhance their resilience against even the most advanced cyber threats.

Executive Summary

The Blue Report 2024 provides an in-depth examination of the current state of cybersecurity across organizations, conducted by Picus Labs. Utilizing over 136 million attack simulations on the Picus platform, the study evaluates the real-world efficacy of security products, bringing to light critical insights and ongoing challenges in threat detection and prevention.

This year's report emphasizes the need for a holistic approach to Continuous Threat Exposure Management (CTEM) to strengthen defenses against cyber threats. While significant advancements have occurred, several critical vulnerabilities persist, underscoring the necessity for continuous optimization.

Automated penetration tests conducted by the Picus APV revealed that 40% of tested environments had paths leading to domain administrator access, posing severe risks of total network control.

The analysis of attack simulations performed by the Picus SCV revealed notable variability in the real-world performance of cybersecurity products. Even top performers in controlled evaluations like MITRE ATT&CK showed diverse effectiveness in operational environments, underscoring the importance of continuous validation and fine-tuning of security controls.

Additionally, organizations exhibited significant improvement in prevention effectiveness, with scores rising from 59% in 2023 to 69% in 2024. However, detection effectiveness presented mixed results with log scores improving from 37% to 54%, but alert scores declining from 16% to 12%. This signals a pressing need to enhance visibility and alert mechanisms in SIEMs and EDRs. A deeper dive into SIEM system detection rules with the Picus DRV revealed that most issues are related to log collection (38%) and performance (33%).

Key recommendations from the report focus on enhancing exposure management through comprehensive validation and continuous fine-tuning of security measures. Organizations are urged to adopt a "proactive security" mindset and manage their exposure to cyber threats. By adopting these strategies, organizations can better protect against evolving cyber threats and enhance their overall security posture.

Key Findings

The Blue Report 2024 provides a comprehensive examination of the current state of threat exposure management across various organizations. This year's findings reveal several critical vulnerabilities and underscore cybersecurity teams' challenges in maintaining robust defenses against evolving cyber threats. Below are some of the most significant insights from the report:

- **High-Risk Attack Paths**
  The report reveals a significant vulnerability across 40% of tested environments, where attack paths could lead to domain administrator access. Such access gives attackers control over user accounts, security settings, and overall network management, analogous to having a master key to the network.

- **Prevention vs. Detection Effectiveness**
  Despite achieving a higher Log Score, which rose from 37% to 54%, indicating better data capture and monitoring, the Alert Score fell to 12% from 16% in 2023. This reduction suggests that increased logging did not translate to improved visibility and timely threat detection. The disparity points to a need for optimization across the entire detection engineering pipeline.

- **Variability in Cybersecurity Product Performance**
  There is notable variability between the performance of cybersecurity products in controlled environments versus real-world settings. Products that score 100% in evaluations like MITRE ATT&CK can exhibit significant effectiveness variability once deployed in diverse operational environments. This underscores the necessity for continuous validation and ongoing fine-tuning to maintain robust defenses.

- **Detection Rule Challenges in SIEM Systems**
  The majority of issues identified in the detection rules of SIEM systems are related to log collection (38%) and performance (33%). Improper log source consolidation affects 23% of cases, while unavailable (10%) and broken log sources (5%) further deepen detection challenges.

- **Endpoint Security Gaps**
  macOS endpoints are significantly more likely to be misconfigured or operate without Endpoint Detection and Response (EDR) tools. As a result, they prevent only 23% of simulated attacks, compared to 62% and 65% for Windows and Linux endpoints, respectively. This underscores a substantial gap in IT and security teams' skill sets and strategies for securing macOS environments.

Key Findings

- **Ransomware Defense Challenges**
  BlackByte is the most challenging ransomware to defend against, with only 17% of organizations successfully preventing it. BabLock and Hive followed, with prevention rates of 20% and 30% respectively, indicating the need for enhanced ransomware defense strategies.

- **Easy to Crack Passwords**
  In 25% of environments, attackers can successfully crack at least one dumped password hash, converting it into a cleartext password.

Key Recommendations

The Blue Report 2024 highlights several critical areas that require attention to enhance cybersecurity defenses. Based on the in-depth analysis and findings, we propose the following key recommendations for organizations to strengthen their threat exposure management:

✔ Adopt a Proactive Security Mindset

Shift from a reactive to a proactive and continuous approach in cybersecurity. This involves continuously identifying and mitigating potential threats and vulnerabilities before they can be exploited.

✔ Implement Continuous Threat Exposure Management (CTEM)

Establish a comprehensive CTEM program to continually identify, prioritize, and validate and fix exposures. This helps in maintaining a robust security posture even as the threat landscape evolves.

✔ Enhance Detection and Prevention Mechanisms

Improve detection capabilities by optimizing the entire detection engineering pipeline, including log collection, performance, and alert mechanisms in SIEM and EDR systems. Regularly review and update detection rules to ensure they are effective against the latest threats.

✔ Strengthen Ransomware Defenses

Implement robust backup and recovery solutions and ensure that all endpoints have up-to-date security controls. Conduct regular simulations of ransomware attacks to test and improve the effectiveness of your response strategies.

✔ Improve Endpoint Security Configuration

Ensure that security controls on all endpoints, particularly macOS systems, are properly configured and that appropriate EDR tools are in place. Conduct regular audits and assessments of endpoint security configurations to identify and fix any misconfigurations.

✔ Enhance Log Management and Analysis

Address common issues in log collection and performance to improve the effectiveness of detection rules in SIEM systems. Ensure proper log source consolidation and availability.

✔ Prioritize Password Security

Implement strong password policies and ensure that password hashing methods are robust to prevent easy cracking of password hashes. Regularly audit and enforce compliance with password security best practices across the organization.

BLUE REPORT 2024

picussecurity

picussecurity.com

PICUS