National Institute of Standards and Technology
[redacted]
cyberframework@nist.gov

Re: Request for Comment on the public draft of the NIST Cybersecurity Framework (CSF or Framework) 2.0

Dear NIST CSF Team,

Introduction

In response to the National Institute of Standards and Technology's ("NIST") public draft of the NIST Cybersecurity Framework (CSF or Framework) 2.0, Black Kite offers the following views.

Black Kite's approach is from the standpoint of having the ability to identify vulnerabilities that are commonly used by threat actors by labeling these organizations/entities that have vulnerable products on any related asset. The data set is of benefit to network and security professionals in Departments and Agencies attempting to determine their cyber vulnerabilities across 20 different technical categories. The data set is essential to protect vendor supply chains, at-scale, with highly curated data mapped to industry frameworks such as MITRE and NIST standards.

With the largest cyber threat intelligence data lake in the marketplace, USG agencies rely on our product's unique capabilities. Currently, Black Kite is monitoring 80,000 companies for CISA, including government agencies, distributed across all 16 critical infrastructure sectors. That includes automating CISA's Known Exploited Vulnerabilities (KEV) tracking and reporting process, DDoS resiliency reports for federal agencies and reverse IP enrichment. Black Kite also provides vulnerability mitigation through the NSA's Cybersecurity Collaboration Center, for over 1,000 Defense Industrial Base companies serving DoD.

Comments

Under Category: Cybersecurity Supply Chain Risk Management (GV.SC), **add a Subcategory**

GV.SC-11: Cybersecurity supply chain risk management plans include automation for scalability and speed that covers a massive attack surface and gives insight into cyber threats
Implementation Examples
Ex1: Identify which suppliers within their ecosystem have access to their data, process their data, have access to systems that have their data, or even have access to their systems in general.
Ex2: Establish an automated and non-invasive process of identifying critical vulnerabilities and continuously monitor cyber risk across thousands of suppliers.
Ex2: Integrate a visualized defensible intelligence dashboard that is digestible to senior stakeholders as a tool to prevent or reduce supply chain risk
Ex3: Escalate a supplier and/or its third-party relationships' likelihood of a ransomware attack to the organization
Ex4: Develop a response plan by cross-correlating findings to determine the effective course of action for remediation using a strategy report that prioritizes and itemizes steps
Ex5: Automate the gap analysis and use of industry-standard compliance frameworks to map each supplier and/or its third-party relationships as part of planning and due diligence

Conclusion

We appreciate NIST's efforts to provide tools/frameworks to organizations in emphasizing cybersecurity supply chain risk management.

However, these tools still require humans to curate the data, use questionnaire management for policy documents/feedback from customers, and lack the ability to remediate vulnerabilities. That approach doesn't scale, requires significant manual effort, lacks accuracy, and results in ineffective point-in-time evens assessments. Black Kite automates all those functions, using industry-leading frameworks to provide data that is not only accurate, trustworthy, and verifiable, but timely and accurate to make decisions actionable at scale. Black Kite combines important features of business intelligence with threat intelligence collection to break through the wall of operationalizing risk intelligence to allow organizations to decide whether to accept, transfer, or mitigate their risk.

Supply chain risk management is an all-of-government mandate for continuous monitoring of U.S. Government vendor supply chains (See E.O. 14017, *America's Supply Chains*). Black Kite automates and synchronizes federal agencies when it comes to continuously monitoring suppliers to the nth party to protect digital assets, information, critical infrastructure, and systems from unauthorized access, cyberattacks, data breaches, and state-sponsored threats. Black Kite provides an automated, exportable, remediation plan for each one of your vendors. In our Strategy Report, we highlight the vendor's current posture and outline a set of prescriptive steps that are designed to advise them on increasing cyber resiliency and reducing financial risk.

Black Kite is the ONLY security ratings service that provides a multidimensional View of Third Party Risk using a standards-based methodology (MITRE, FAIR, NIST).

Contact

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Tony Monell
V.P. Public Sector
[redacted]

Black Kite was recently added to CISA's Continuous Monitoring Diagnostics Program Approved Products List. The CDM Program delivers cybersecurity tools, integration services, and dashboards that help participating agencies improve their security posture.