From: vapplica group
Sent: Thursday, January 18, 2018 12:44 PM
To: cyberframework <cyberframework@nist.gov>
Subject: Re: Update to Cybersecurity Framework

Good Morning,

We are Cybersecurity and Biometric firm like to submit comments for draft 2 of Cybersecurity Framework version 1.1 and the draft Roadmap due to NIST by 11:59PM on Friday, January 19, 2018.

Attached is the document. Please let me know if you need anything else.

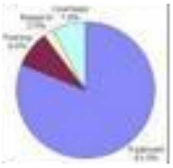
Thank you.
Best Regards,
Sandeep Singh
vapplica group llc.

[***Attachment copied below***]

icloudcyber Security Management

product of vapplica llc.

Proposal to provide Professional Services



Public Comment Period Public comments for draft 2 of Cybersecurity Framework version 1.1 and the draft Roadmap are due to NIST by 11:59PM on Friday, January 19, 2018 via cyberframework@nist.gov. NIST anticipates finalizing Cybersecurity Framework version 1.1 in the Spring of 2018.

The proposed comments below for the Cybersecurity frameworks mainly includes some add-on to the Framework Core and Framework profile section. The framework core section proposal objective includes machine learning, penetration testing system and usage open source community. In framework profile section propose about subcategorization. Also in general proposal to give provision for some emerging technology in security field.

For Framework Core the proposed. Include the following

Machine Learning In Cybersecurity

The emerging machine learning algorithms in cyber security can help to better analyze threats and respond to attacks and security incidents. It could also help to automate more menial tasks previously carried out by stretched and sometimes under-skilled security teams. Introduction of technology like machine learning (ML), deep learning (DL) and artificial intelligence (AI) to the core framework. Use of these methodology in framework core section such as detect and identify and use the outcome for protect. At its simplest level, machine learning is “the ability (for computers) to learn without being explicitly programmed.” Using mathematical techniques across huge datasets, machine learning algorithms essentially build models of behaviors and use those models as a basis for making future predictions based on newly input data.

Penetration testing

Proposing to include the penetration testing tools and system in core framework. Penetration testing tools simulate real-world attack scenarios to discover and exploit security gaps that could lead to stolen records, compromised credentials, intellectual property, personally identifiable information (PII), cardholder data, personal, protected health information, data ransom, or other harmful business outcomes. By exploiting security vulnerabilities, penetration testing helps you determine how to best mitigate and protect your vital business data from future cybersecurity attacks. Once penetration testing has exposed the gaps in security, the testers can make recommendations on how to close them.

We would like to propose to give the provision for the penetration test conducted by machine learned smart machine.

Open Source

Proposing to use the advantage of open source software community on framework Core section. The global communities united around improving these solutions introduce new concepts and capabilities faster, better, and more effectively than internal teams working on proprietary solutions.

Framework profile

Proposing different profile for Business organization, academic organization

and government organization under framework profile. And each of these subcategorized organization can select appropriate profile. The same categorization can be done in framework core section.

Flexibility to add emerging technology.

The general increase in information and data over the year the framework should capable including the emerging technologies. The general increase in information indicate artificial security intelligence is necessary. Adaptive skills will be key for the next phase of cybersecurity. Provision for Machine learning, artificial intelligence, deep learning algorithms could be helpful for greater flexibility in future.

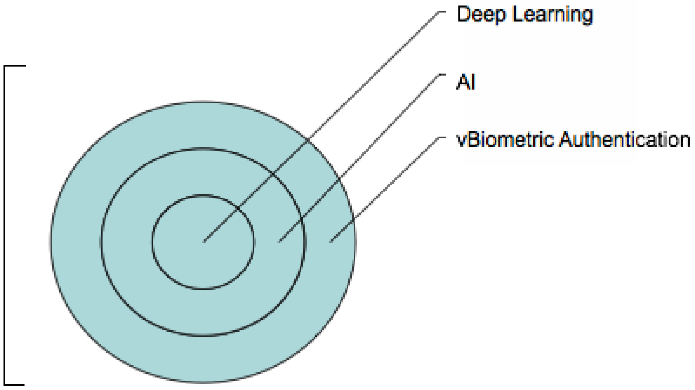
Framework to take the consideration for the following;

1. *vBiometric Authentication*: The framework may take consideration the hardware authentication which can be particularly important for the Internet of Things (IoT) where a network wants to ensure that the thing trying to gain access to it is something that should have access to it. One method is to bake biometric Face authentication into a user's hardware. vBiometric Face Recognition product uses facial recognition authentication system. Recognized as one of the fastest and most accurate technology in the world. Involving, artificially intelligent and mobile ready capabilities. Algorithms that are active and current with latest testings of National Institute of Standards and Technology. These innovative solutions is designed to meet requirements of law enforcement, security agencies, hospitality industry, residential apartment buildings, retail sector and multitude of security vertical markets. It can combine a variety of hardware-enhanced factors at the same time to validate a user's identity.

2. *Artificial Intelligence and User-behavior analytics*: The technology uses big data analytics to identify anomalous behavior by a user. The defender is challenged with enhancing their visibility and insights into their own organizations' systems, in order to regain the advantage and inform critical, timely decision-making. Tueri Cyber intelligence is central to this challenge, providing total visibility and tailored, real-time insights into emerging anomalies – as opposed to feeds of old news about previous threats. The breach of the network perimeter is now assumed as inevitable by today's security professional.

3. *Deep Machine learning*: Deep learning encompasses a number of technologies, such as artificial intelligence and machine learning. With situational awareness of the entirety of an organization's activity, new technologies can be leveraged to analyze it, and form a constantly-evolving picture of normality. Fundamental advances in probabilistic mathematics and machine learning have made this approach possible, delivered by technology that learns what is normal and abnormal within a particular organizational environment on a continual basis, and surfaces probabilistically anomalous events in real time.

Usage of these technology for security purposes for enhancing the security, Like- user behavior analytics, deep learning focuses on anomalous behavior.



4. *Cloud:* The cloud is going to have a transformative impact on the security technology industry. True cyber intelligence is not about identifying past threats and attack vectors, therefore, but is focused on understanding exactly what is happening within the organizations, to a level of granularity that will expose even very subtle and quiet actions. Clever intelligence is about analyzing this detailed, real-time information in such a way as to correlate multiple weak indicators and form a picture of understanding from that data. icloudcyber Security management platform is an ideal example that uses amalgamation of Private and Public cloud concept to provide Cyber-as-a-Service following NIST framework guidelines at the core of its concepts.

5. Privileged Account Management

Privileged accounts represent the largest security vulnerability an organization faces today for all sectors. Privileged Account Management (PAM) is a domain within Identity and Access Management (IdAM) that focuses on monitoring and controlling the use of privileged accounts.Privileged accounts include local and domain administrative accounts, emergency accounts, application management, and service accounts. vPrivilage is an example that uses advanced authentication mechanism and is designed from the ground up for security.

This complete enterprise-ready Privileged Account Security Solution is tamper-resistant, scalable and built for complex distributed environments to provide the utmost protection from advanced external and insider threats.
vPrivilege Vault centrally secures and controls access to privileged credentials based on privileged account security policies.
vPrivilege Record This complete enterprise-ready Linux based Privileged Account Security Solution is tamper-resistant, scalable and built for complex distributed environments to provide the utmost protection from advanced external and insider threats.