METHOD OF AUTOMATED CYBER RISK ASSESSMENT, INSURANCE UNDERWRITING, AND REMEDIATION

An IP.com Prior Art Database Technical Disclosure

Authors et. al.: Omar Santos
Pavan Reddy
Robert Waitman
Jeffrey Tumpowsky
Andrew Morris

IP.com Number: IPCOM000250702D
IP.com Electronic Publication Date: August 23, 2017

METHOD OF AUTOMATED CYBER RISK ASSESSMENT, INSURANCE UNDERWRITING, AND REMEDIATION

AUTHORS:
Omar Santos
Pavan Reddy
Robert Waitman
Jeffrey Tumpowsky
Andrew Morris

CISCO SYSTEMS, INC.

ABSTRACT

An end-to-end solution is provided for correlating and analyzing cyber security threat intelligence, security vulnerability information, geopolitical news and events, and historical information about cyber losses using machine learning to provide an automated threat score, "insurability" score, and automated security vulnerability remediation. A layered use of artificial intelligence learns which vulnerabilities, mitigations and remediations should be prioritized, along with automated fix/mitigation validation.

DETAILED DESCRIPTION

While cyber insurance offers a mechanism to transfer some of the potential losses from cyber risk, manual processes and the inability to adequately assess cyber risk is limiting the growth and effectiveness of cyber insurance. Existing cyber risk assessment capabilities are not sufficiently comprehensive, and gaps exist in knowledge, methodology, and tools. Major insurance companies recognize this gap and are looking to leverage other cyber security intelligence to calculate risks for their clients. There are many different/disparate ways to collect cyber security telemetry and other contextual information to be able to calculate a threat score. However, all those solutions are very fragmented and do not provide a solution that is scalable, may be automated, and may be used to automate the prioritization of security gaps and remediation (for both risk of threats and vulnerabilities).

An end-to-end solution is provided for correlating and analyzing cyber security threat intelligence, security vulnerability information, geo-political news and events, and historical information about cyber losses using machine learning to provide an automated

threat score, "insurability" score, and automated security vulnerability remediation. An embodiment addresses automated blended risk assessment and security mitigation and remediation across logical systems, information technology (IT) applications, databases, and physical systems from a multi-system cloud service. Further, an embodiment provides capability and functionality for providing visual risk, continuous cyber threat and vulnerability monitoring, alerting, mitigation using application programming interfaces (APIs) and streaming services for end users and cyber insurance companies including underwriters, re-insurers, as well as brokers.

Figure 1 below illustrates an end customer (e.g., small, medium, or large enterprise; self-employed individual; government institution; service provider; etc.), a cyber insurance company (e.g., underwriter, re-insurer, broker, etc.), and the cloud service solution described herein.

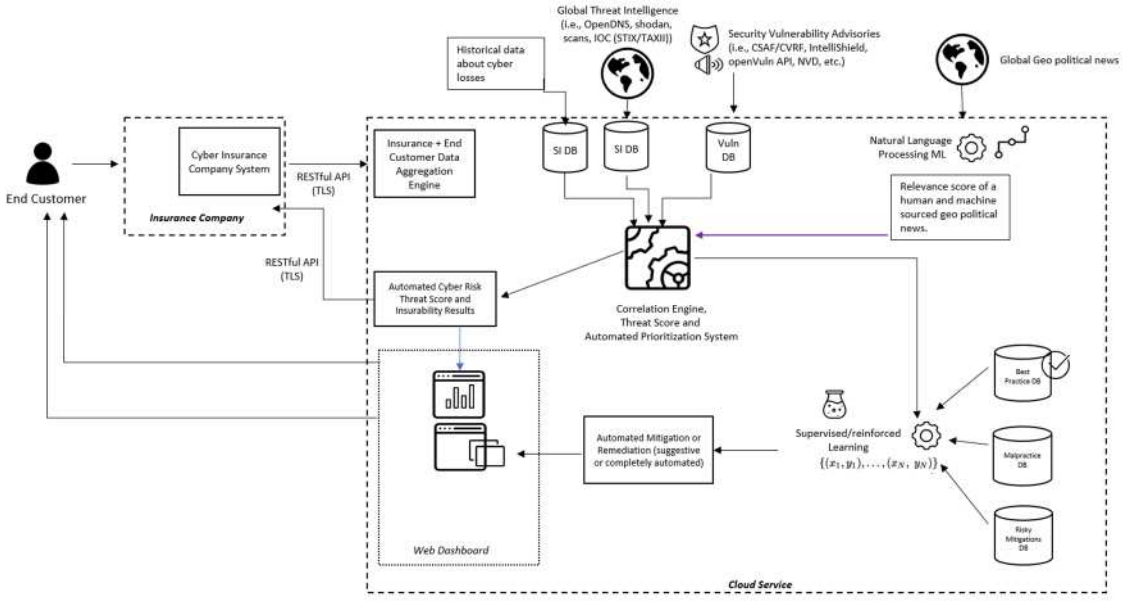

Figure 1

The following describes the process shown in Figure 1:

1. The end customer engages with the cyber insurance company to obtain insurance coverage.

2. The insurance company communicates with the cloud service via representational state transfer (REST)-ful API(s) over an encrypted channel (e.g., Transport Layer Security (TLS)), using a streaming service, etc.).

3. The cloud service receives and aggregates the end customer data and potentially other pertinent insurance information from the insurance company.

4. The cloud service also subscribes, stores, and processes the following types of data:

- Historical cyber security incident losses data and case study information.
- Global cyber security threat intelligence including but not limited to:
    - Domain Name Server (DNS) threat intelligence
    - Active and passive scan information
    - Dark web threat intelligence
    - Indicators of compromise (IoC) and any other observable (this may be represented in Structured Threat Information eXpression (STIX) and transported via a Trusted Automated eXchange of Indicator Information (TAXII) service).
- Security vulnerability information (this may be represented and processed using the Common Security Advisory Framework (CSAF) / Common Vulnerability Reporting Framework (CVRF) from software and hardware vendors, APIs such as the Cisco Product Security Incident Response Team (PSIRT) openVuln API, and/or the National Vulnerability Database (NVD)).
- Global geo-political news and events

5. The historical cyber security incident losses data, cyber threat intelligence and vulnerability information are stored in respective databases for further processing.

6. The global geo-political news and events include large unstructured text used to create training sets in order for machine learning to distinguish signal from noise. These data sets can include news articles, social media posts, and other related data. Geopolitical events that may have an impact to the overall risk of a company are learned by the system. A relevance score is produced and correlated with cyber threat intelligence and security vulnerability information. These events (along with the relevance score) may include a configurable or “learned” expiration date.

7. The main correlation engine combines and correlates the cyber threat intelligence, security vulnerability data, and geopolitical event information and relevance score and provides the following outputs:

- An automated cyber risk threat score along with an insurability score. The results may be delivered to the cyber insurance company via APIs, streaming services, and a web dashboard. Similarly, the results may be shown to the end customer via customized dashboards including analytics about the cyber threat information, security vulnerabilities, exposures, communications to high-risk third party systems or cloud providers, and other pertinent information.
- The correlation engine may also prioritize security vulnerabilities that need to be fixed or mitigated based on the Common Vulnerability Scoring System (CVSS) base and temporal score for each vulnerability, along with any related IoC, related exploits, and geopolitical data. The prioritized security vulnerability data is then provided to a remediation engine.

8. The remediation engine uses supervised and reinforced learning to suggest or automatically implement a remediation or mitigation for such security vulnerability.

9. The remediation engine uses information from a security best practice database, a security malpractice database (for reinforced learning), and data about types of mitigation and remediations that could be risky (e.g., a mitigation could potentially introduce a denial of service condition if not applied correctly or a fix/remediation could introduce side effects to the overall affected system).

10. The result of the remediation engine is displayed in a web dashboard and may also be applied to certain systems in the end customer site.

Figure 2 below illustrates similar concepts implemented without a cyber insurance company.

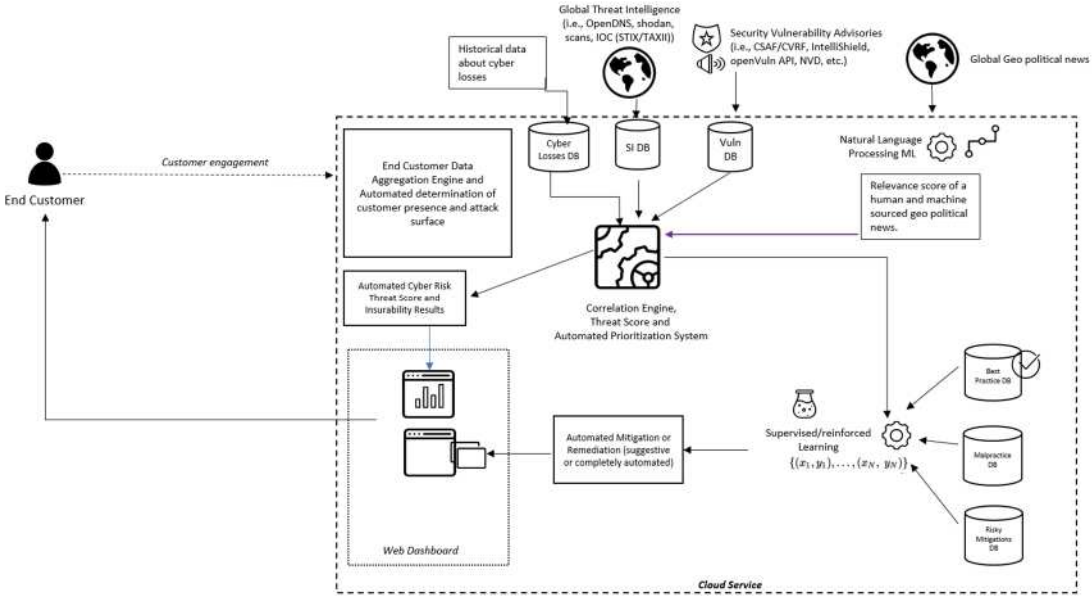

Figure 2

Figure 3 below illustrates details regarding the use of automated vulnerability prioritization, machine learning and automated fix and/or mitigation validation and testing.

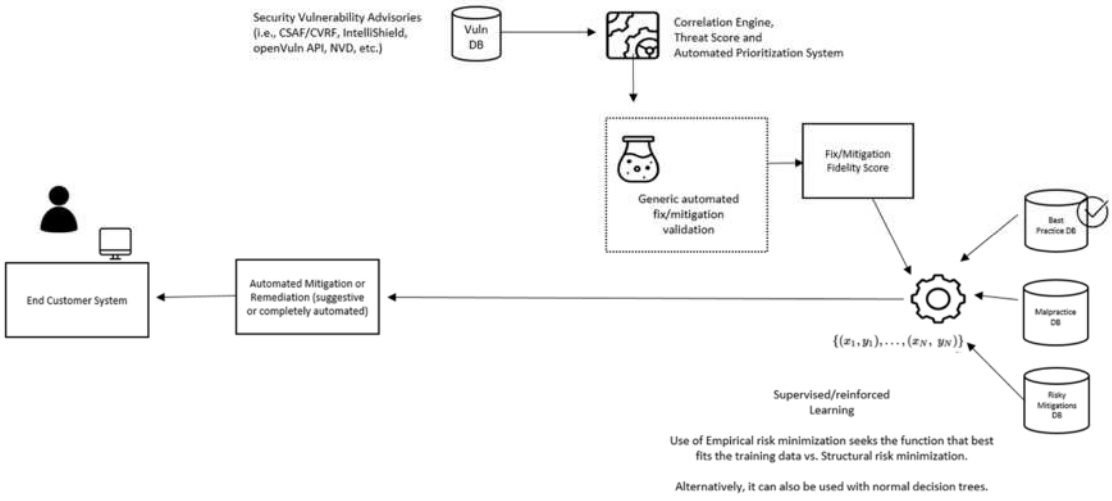

Figure 3

As shown, the correlation engine provides an overall threat score and automated prioritization of which security vulnerabilities need to be fixed or mitigated. This may be because there is an active threat actor that could be exploiting a given vulnerability in the wild and a geopolitical event that could have an impact and introduce a higher risk for such vulnerability to be exploited. After the correlation engine identifies the vulnerability that should be prioritized, it may send the vulnerability information, along with the fix or mitigation information to an automated fix/mitigation validation system.

A generic automated validation may be performed using containers to test the mitigation or the fix. After this validation is performed, a fix/mitigation fidelity (or confidence) score may be produced. This may also be used as input to a system that uses supervised or reinforced machine learning leveraging either empirical risk minimization or decision trees, and may also use data from the security best practice, malpractice, and risky mitigation databases (knowledge base). The goal is to learn what will be the best course of action for mitigation and remediation in an automated way.

Figure 4 below illustrates that this may also be accomplished without the threat correlation engine and using vulnerability data directly from the security vulnerability database.

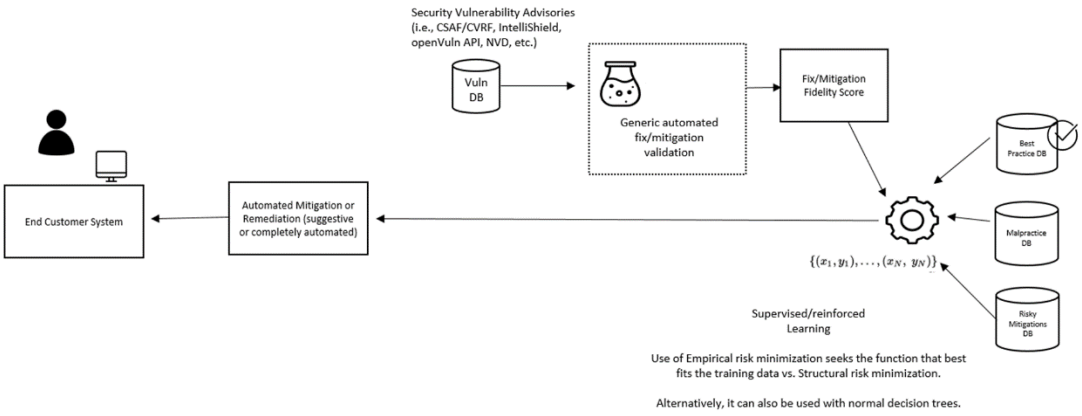

Figure 4

Figure 5 below illustrates that, alternatively, the automated fix and mitigation validation process may be skipped and the data from the security vulnerability database may be applied directly to the system.

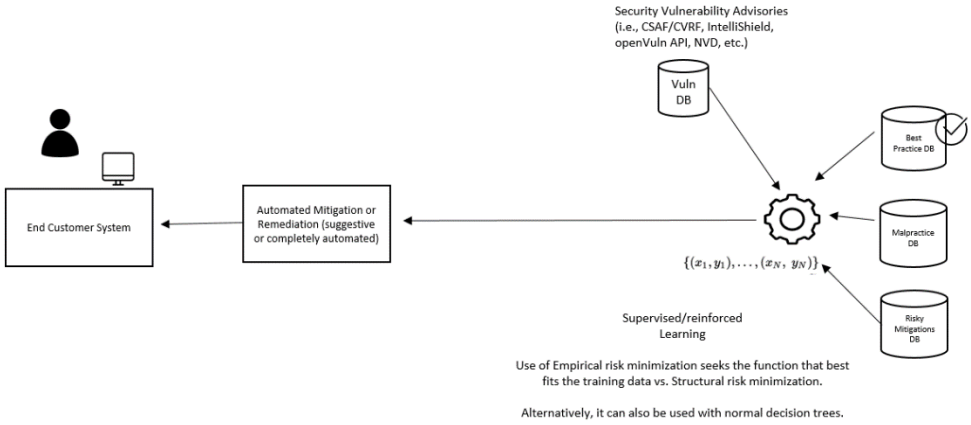

Figure 5

These techniques may be implemented in a product or a cloud service.

In summary, an end-to-end solution is provided for correlating and analyzing cyber security threat intelligence, security vulnerability information, geopolitical news and events, and historical information about cyber losses using machine learning to provide an automated threat score, "insurability" score, and automated security vulnerability remediation. A layered use of artificial intelligence learns which vulnerabilities, mitigations and remediations should be prioritized, along with automated fix/mitigation validation.