September 2023

IDENTIFYING ENTERPRISE RISK BASED ON BUSINESS CONTEXT WITH THREAT INTELLIGENCE

Randy Birdsall

John A. Foley

Chandra Mohan Babu Nadiminti

Girish Sivasubramanian

Dhruv H. Raithatha

IDENTIFYING ENTERPRISE RISK BASED ON BUSINESS CONTEXT WITH THREAT INTELLIGENCE

AUTHORS:
Randy Birdsall
John A Foley
Chandra Mohan Babu Nadiminti
Girish Sivasubramanian
Dhruv H. Raithatha

ABSTRACT

Presented herein are techniques that facilitate prioritizing risk mitigation efforts for business-critical services and transactions through the incorporation of a business context into threat intelligence scoring. Under aspects of the presented techniques, traditional threat intelligence tools may be employed to evaluate the risk that is associated with an enterprise asset; the results of such an evaluation may then be augmented with an enterprise-assigned business value for the asset to derive the asset's business risk; and such a business risk may be leveraged to prioritize risk mitigation efforts, may be combined with other business risks, etc. The above-described process may be referred to herein as Business Risk Management (BRM).

DETAILED DESCRIPTION

A traditional cyber security risk analysis typically relies on threat intelligence. Such threat intelligence may encompass, for example, a software bill of materials (SBOM) analysis, the results of network scanning, an analysis of log files, the results of an intrusion detection operation, etc. Within such a context, SBOM analysis, for instance, may be used to identify known vulnerabilities in the software that is employed by an enterprise.

While current threat intelligence functions can provide valuable information for managing potential risks at an enterprise level, such an enterprise will still struggle with prioritizing different risk mitigation activities.

The nature of such a struggle may be understood through an illustrative example wherein an enterprise relies on two online services. A first service provides real-time stock quotes and a second service is employed for the processing of payments. Under the instant example, both of the services are subject to the same vulnerability.

From a threat intelligence standpoint, mitigating against both of the potential risks would be of equal importance, as both of the risks arise from the same vulnerability. However, from a business standpoint the business context may be such that payment processing is far more important to the enterprise than the offering of stock quotes. Consequently, addressing the vulnerability with respect to the payment processing service may take precedence.

Techniques are presented herein that augment threat intelligence data with a business context to facilitate such a prioritization of risk management activities.

In connection with the presented techniques, a key observation may be made that an enterprise may assign a business value to each enterprise asset. Under the presented techniques, traditional threat intelligence tools may be employed to evaluate the potential risk that is associated with each of those assets. The results from such an evaluation may then be augmented with a business value to derive a business risk for an asset. The above-described process may be referred to herein as Business Risk Management (BRM).

For example, if an enterprise operates two services and both of those services are vulnerable to the OpenSSL 'Heartbleed' vulnerability (registered in the Common Vulnerabilities and Exposures (CVE) database as CVE-2014-0160), traditional threat tools may assign the same risk level to each of the services. But, as described in the previously-presented illustrative example, if one service is used for the processing of payments (collecting, during such processing, sensitive payment information from a customer) while the other service simply provides publicly-available data (in the form of stock quotes), then the enterprise may place a higher business value on the payment processing service.

According to the presented techniques, the BRM algorithm may augment the traditional threat score from the CVE-2014-0160 vulnerability to derive a new threat score for each asset. Under such an approach, and continuing with the above-described example, the payment processing system may receive a higher BRM score thus allowing the enterprise to prioritize the mitigation of the CVE-2014-0160 vulnerability within the payment processing service over the mitigation of the vulnerability within the stock quote service.

Aspects of the presented techniques may corelate a threat context and then apply a business context to calculate a business risk for an organization. Here, a business

transaction (BT) may be defined as the path that a request takes within an application (e.g., through its various services) to complete the intended request.

The factors that may influence the threat score that is tied to a BT or service may include any number of one or more of the following – whether a service or BT processes sensitive data; whether a third-party application programming interface (API) is used; the performance load that is experienced by the services that make up an application; whether a service or BT is public facing or internal facing; a manually-specified priority that is assigned to a BT or service; whether a vulnerability increases the possibility of access to a data store (such as a database, a cache, a cloud-based facility, etc.) as such an exploit could have a greater impact; if the risk involves a known malicious Internet Protocol (IP) address; if the service or BT travels through vulnerable third-party code to handle a request; and if the service or BT risk increases when the detected vulnerabilities are exploited in the wild.

Figure 1, below, presents elements of an exemplary process flow that is possible according to the techniques presented herein and which is reflective of the above discussion.

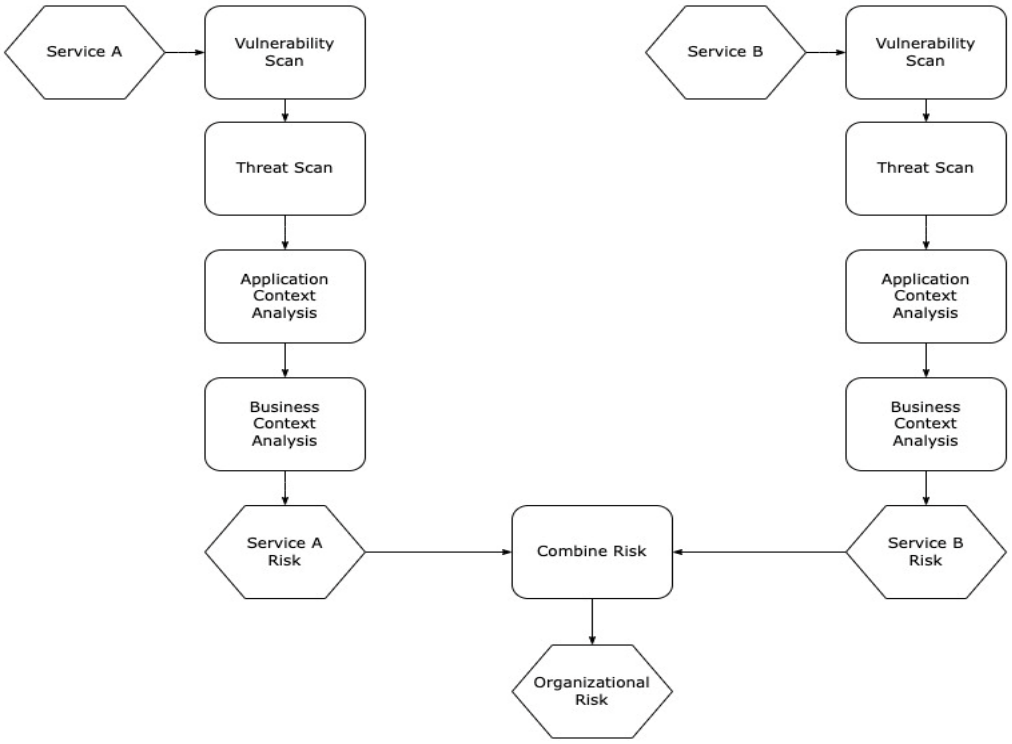

Figure 1: Exemplary Process Flow

As depicted in Figure 1, above, and continuing with the theme of the illustrative example that was presented above, for each of two services (Service A and Service B) a series of activities may be independently completed. Those activities may include a vulnerability scan, a threat scan, an application context analysis, and a business context analysis. The outcome of the above-described activities may be a risk value for each of the two services – i.e., a Service A risk value and a Service B risk value. The two separate risk values may then be combined (through aspects of the presented techniques as described above) to develop an overall organizational risk value.

In summary, techniques have been presented herein that support prioritizing risk mitigation efforts for business-critical services and transactions through the incorporation of a business context into threat intelligence scoring. Under aspects of the presented techniques, traditional threat intelligence tools may be employed to evaluate the risk that is associated with an enterprise asset; the results of such an evaluation may then be augmented with an enterprise-assigned business value for the asset to derive the asset's business risk; and such a business risk may be leveraged to prioritize risk mitigation efforts, may be combined with other business risks, etc. The above-described process may be referred to herein as BRM.