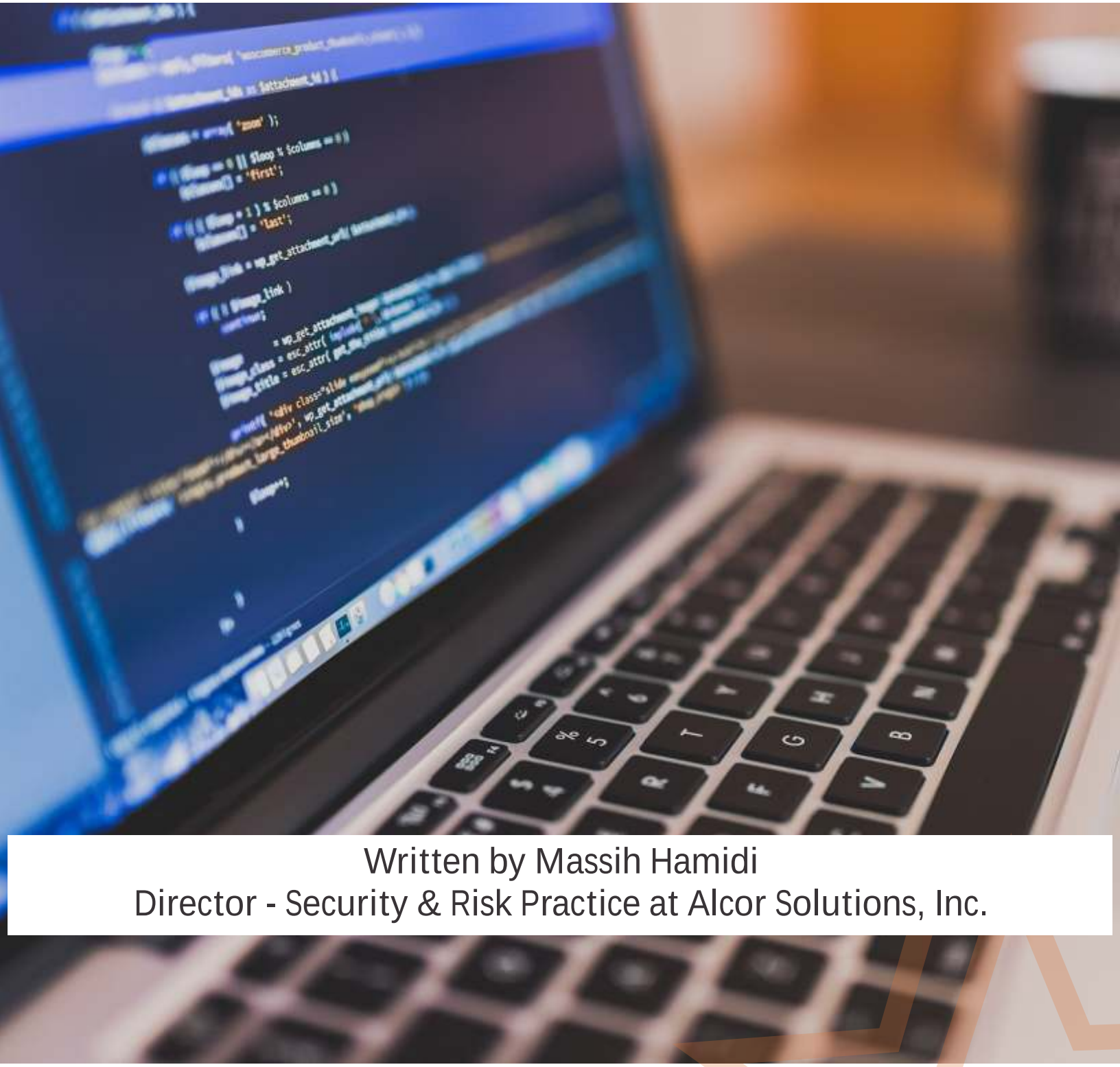
ALCOR
ENABLING CLOUD™

Article

ServiceNow® Vulnerability Response And Management



Written by Massih Hamidi
Director - Security & Risk Practice at Alcor Solutions, Inc.

ABSTRACT

Rigor, mathematics, process and integration are at the heart of security engineering and analysis. Vulnerability Management and Response is an important component of ServiceNow Security Operations and acutely and principally the center of thought surrounding an organization's technical assets (which include, people, infrastructure, systems, dynamics and information flows). This is part and parcel to the development, documentation and implementation of policies and processes to safeguard those particular assets. It is the core of security attacks, as 44-60 percent, based on data breach occurrences, such as the latest attack vectors of memory weaknesses known as "Meltdown" and "Spectre". This short article will focus on the general depictions of what Vulnerability Response and Management are in and initiate ServiceNow discussion in terms of their solution.

SUMMARY

Vulnerability Management is the consistent traversion of identifying, classifying, remediation, and mitigation of vulnerabilities found within a corporate network that affects everyone in the world, not just certain geographies. They are visible in software, but as Meltdown and Spectre has shown, vulnerabilities can happen within hardware, memory or within communication processes between HW and SW. Proper security strategy entails reverse engineering rigor, meaning, one has to assume that you currently have flaws inside and that you have active vulnerabilities at play in your environment. Finding out where these are, rather than assuming that you are currently safe. Vulnerabilities are located on PC's, Operating Systems, Firewalls, Processors/Chips, Firmware, Hardware, Software, Plug-ins, Middle-ware, Application Servers, Databases and anywhere else you might think of frankly, inside and outside a corporate entity.

Vulnerability Management construction and design is great, but crucial focus should be paid attention to Vulnerability Response. How are you going to respond to flaws, attacks, social attacks, is just as important as finding out what exposure you have and how you will manage the classification and identification. Correcting such vulnerabilities may surreptitiously involve patch installations, once they are distributed and tested by vendors, a change in particular policy from Network segments, reconfiguration of software and architecture and education of general users about social techniques hackers or bots use to circumvent these processes. Let's decrypt this rational in simple terms:

Significance:

- Vulnerabilities are constantly ranked as the most important priorities for security organizations today.
- Estimates of Vulnerabilities range in 2-3 million in totality, translation (You are exposed)!
- Most organizations manage, have monitoring systems, scan tens and thousands of assets daily, weekly and monthly. However, these assets belong to various teams and respond to various processes with separation of duty and authority.
- As an increasing amount of workload in companies move towards cloud providers, security and vulnerabilities will become more obfuscated and non-linear in nature.

ALCOR INPUT

Understanding of Vulnerabilities and how ServiceNow® SecOps response applications and modules enhance our customers security posture, vulnerability management and most importantly, give them an integrated way to have these various teams with differing applications and processes operate, communicate and respond in a streamlined coordinated fashion will provide benefits beyond contestation, for the customer and Alcor employee because understanding vulnerabilities is at the heart of security.

CONCLUSION

ServiceNow® Security Operations, in particular, Vulnerability Response, helps a corporation respond faster and with align information in accordance to their CMDB (data warehouse) of assets. This is not an abstraction, but rather, a correlation of assets to provide the security analyst a comprehensive way of assessing intelligence of the assets in relation to the given vulnerability at play. Time compression and complete ticket intelligence is provided, along with calculation or risks of the vulnerability in terms of severity, business impact, vulnerability scoring, complexity of attack and the old CVSS system of Confidentiality, Integrity and Availability. This is the first application of ServiceNow® Security Operations, more detail to come regarding Security Incident Response and Threat Intelligence applications of the ServiceNow® response solution.

Alcor is a technology implementation company focusing on Enterprise and Government technology needs in ITSM, systems integration, web development and mobility space. We provide a strategic ITSM implementation approach to our clients and focus on solving business problems by leveraging an integrated business process design and technology implementation capability.