White Paper

Bitdefender®

Increasing Cybersecurity Resilience through Security Automation

The ever-evolving threat landscape, coupled with the increased number of cyberattacks aimed at businesses and organizations, has accelerated adoption of a growing number of security solutions. The malware-as-a-service industry has lowered the bar for cybercriminals -- not having the right technical skills is no longer a barrier for those who want an exploit kit, ransomware kit, or even a botnet.

Cyber risk is now among the top 5 risks affecting businesses, according to 65 percent of executives. At the same time, the risk of cyberattacks ranks the third most likely occurrence, right after natural disasters, according to the World Economic Forum's Global Risk Report for 2018. Cybercrime as an industry has also grown from $450 billion in 2016 and is estimated to reach a whopping $2 trillion by 2019, according to the same report.

We're in the midst of a paradigm shift: set-and-forget security solutions centered mainly on prevention are now being toppled by security solutions developed to detect threats, investigate cybersecurity incidents, and even respond to those incidents. This basically means organizations now focus more on detecting and responding to breaches as soon as possible, because they're starting from the premise that their organization will be breached in the foreseeable future.

In light of all this, security automation has become the main pillar and focus for organizations in terms of detection, response, and increasing their cybersecurity effectiveness against future attacks, regardless of their complexity and sophistication.

Recruiting cybersecurity experts is a big problem, and 66 percent of professionals around the world believe they have too few security professionals in their own departments. While the trend for this deficit is not encouraging, North America seems to be the one most affected, according to the 2017 Global Information Security Workforce Study by Frost & Sullivan. By 2022 the shortage of workers in the security industry will reach 1.8 million, suggesting organizations need to address the cybersecurity work gap before things get worse.

In 2018, 51 percent of IT and cybersecurity professionals agree they have a problematic shortage of cybersecurity skills, systematically increasing over the last four years by 28 percent. This has caused organizations to spend more in training internal staff or junior personnel on specific cybersecurity skills, but they face a growing problem revolving around staff spending more time dealing with daily security warning rather than planning or coming up with new security strategies.

Sub-optimal response processes and workflows are also the Achilles' heel of current security operations teams, as they have to manually and empirically filter out alerts, potentially spending too much time solving trivial security warnings and missing on potentially critical ones. This continuous and unfortunately scaling overburdening problem is turning cybersecurity experts into firemen who have to constantly put out fires rather than making decisions that actively develop and implement new security strategies and policies.

Cybersecurity teams that are also overwhelmed by alerts triggered by decentralized systems, each monitoring specific parts of the infrastructure, can lead to critical notifications being disregarded or buried under dozens or hundreds of irrelevant warnings. Some IT and security teams might even receive between 10,000 and 150,000 alerts per day, and not all of them during standard business hours. This alert fatigue can overburden security operations teams and ultimately lead to a scaling problem that cannot be addressed by throwing human resources at it -- not because staffing costs would skyrocket, but because of cybersecurity talent shortage.

An ESG study has revealed that, while 97 percent of IT and security decision makers agree that cybersecurity professionals need to keep up with their skills, 62 percent of organizations do not provide an adequate level of training, while 67 percent said they're having a hard time keeping up on cybersecurity skills because of increasing demands of their jobs.

The **ever-increasing attack surface** brought, in part, by these new technologies has been constantly increasing and allowing threat actors to exploit these blind spots to their advantage. Threat actors have become extremely successful at infiltrating organizations, particularly because of mobility, cloud operations, IoT devices, and even file-sharing platforms that not only increase the organizations' attack surface but also make it difficult for IT and security teams to manage them.

With SaaS accounting for 60% of all cloud-based workloads, some IT and security professionals have expressed

concerns over how to secure those infrastructures and, consequently, the data stored there. Mobility is also something that organizations have prepared for, with 42 percent stating they are actively executing a BYOD program, while 24 percent have successfully executed one. While some studies have shown that employee productivity increases as a direct result of a successfully implemented mobility plan, balancing security and BYOD is something that IT and security teams find difficult. The increased attack vector surface is something security experts fear most.

How Can Security Automation Help?

The hero that's supposed to save the security industry and, implicitly, save security operations a lot of valuable time, is machine learning. These algorithms have the unique ability to be trained to cope with a wide range of security scenarios while improving response capabilities.

A pragmatic view of machine learning and how it can be applied to solve today's problems is its use as a tool rather than a one-size-fits-all approach. For example, while machine learning's capabilities significantly differ from what Hollywood would have us believe, we can still look at it as an Iron Man suit that significantly augments the capabilities of security experts.

Security automation tools are not designed to be fully autonomous, but rather simply enhance the response time, experience, and knowledge of cybersecurity professionals, while reducing their effort in dealing with repetitive tasks.

"Security professionals can use the building blocks of pragmatic AI today to: 1) predict and adapt to future threats; 2) identify, prioritize, and remediate existing vulnerabilities; and 3) detect and stop cyberattacks in progress — at a scale and speed that is simply not possible with human analysis and manual processes," according to Forester.

Improving efficiencies in IT operations, mitigating security risks, improving data analytics, improving business automation, and gaining better customer insights are only a handful of the areas where machine learning can prove more than just a powerful cybersecurity ally, but also an effective business tool.

Applying security automation in cybersecurity

Of course, deploying security automation and orchestration tools should not be an all-at-once endeavor -- organizations should take a rather agile approach to it. Gradual implementation of automation principles to security problems will bring faster and better results than an all-in-one security automation project. Understanding where exactly organizations should start to deploy automation tools is vital, and it's often recommended to start with security processes that result in the easiest wins by saving the most time for cybersecurity teams.

When adhering to an agile methodology for applying security automation within infrastructures it's important to start small, but start nonetheless. This basically means accepting that you need security automation within your infrastructure and be prepared to start planning for long term strategy that's subject to constantly change based on the organization's needs.

Analyzing the organization's environment before actually building an automation strategy should be next on the list, as it helps them understand what are the most frequent security incidents they face and whether they are critical to their security posture. This can help organizations automate specific processes and patterns based on that detailed analysis of their environment, and at the same time figure out how much time IT and security teams could gain by offloading these tasks to automated security systems.

Since time is the most valuable commodity for security teams, this analysis and implementation process needs to be reiterated over and over, as the entire agile approach towards security automation involves fine-tuning processes until a satisfactory objective is met and IT can balance security with the cybersecurity workforce gap.

Best Use Cases for Security Automation Today

As threat actors actively exploit both known and unknown vulnerabilities in data breaches, organizations still struggle to timely deploy patches and fix affected software. A look at the number of reported vulnerabilities each year shows a clear growing trend. For instance, by mid-year there had already been more than 10,000 reported vulnerabilities in 2018, while in 2017 there were just a little over 14,000 throughout the entire year.

Security automation can easily be applied to various areas of enterprise security, but endpoints are usually the most targeted by cybercriminals, which is why organizations should start by focusing on them. Since endpoints can be anything from services to workstations and mobile devices, the fact that they harbor sensitive data turns them into valuable targets and makes security automation all the more challenging for companies.

When trying to determine how to best implement the right security automation tools, it's also vital to understand what the attack kill chain is, how advanced threats operate, and what the actual phases of an attack are.

For example, most attacks start with reconnaissance, attempting to identify vulnerabilities within a targeted infrastructure, followed by weaponization, when threat actors actually prepare the malware best suited for infiltration. The delivery, exploitation and installation phases of an attack are usually tied together tightly, as they involve actually landing the payload on the victim's computer, exploiting a found vulnerability, then installing the actual malware that could enable remote control for the threat actor.

The last phases of the attack kill chain usually involve remote connection to the attacker-controlled command and control (C&C) server to retrieve instructions, followed by the intruder achieving his goals and exfiltrating data, destroying his footprint, or even downloading additional malware either for lateral movement across the infrastructure or to increase his foothold.

Organizations aiming to protect their endpoints have to break the attack kill chain before the attacker accomplishes his objectives, and doing so involves deploying as many layers of defense as possible that can anticipate, prevent, detect and respond, investigate, and even remediate any security issues found. Unlike the attack chain, these security layers are not singular in the sense that, if one is bypassed, the entire security posture of the organization will be compromised. On the contrary, if one security layer fails to detect a specific threat at a step during the attack chain, the other security layers could spot the threat during the same phase of the attack chain. This means security layers continuously augment each other's capabilities and constantly interact with each other to validate whether a security issue is indeed part of an advanced threat.

Traditionally, endpoint protection platforms (EPP) mostly focused on detecting threats during reconnaissance, weaponization, delivery and exploitation. While this is great from an automation perspective, prevention is usually based on automated set-and-forget technologies that can normally cope with the majority of attacks. For instance, Bitdefender prevention technologies can prevent more than 99% of generic and advanced attacks, without system administrators manually intervening during the process.

Key Bitdefender Automation Technologies

However, these are not the only security layers that can be automated for endpoints. Security patching automation is one area where organizations can offload time constraints from security and operations teams by automatically deploying the latest security patches across their entire install base. Whether it's operating systems or applications, security patching automation can help organizations prevent a potential data breach by denying attacks from exploiting known vulnerabilities, and it can also help with compliance.

The importance of patching becomes even more dramatic if we remember the Equifax incident that led to the exposure of personal data of 143 million users, because of an unpatched Apache Struts vulnerability. Failure to maintain software up to date can have more than just financial repercussions, but also reputational consequences that organizations may not be able to recover from.

Bitdefender has a Patch Management Module as part of its enterprise security solution, GravityZone, that can automate the software patching process for both Windows-based operating systems as well as popular applications.

Another vital part of security automation is the ability to deploy machine learning algorithms within an infrastructure that have been specifically trained to detect advanced and sophisticated threats. This hyperdetect security module should be able to be fine-tuned based on the organization's needs, allowing aggressive and normal settings that impact how thorough and "paranoid" the algorithms should be concerning security events.

Hyperdetect is one of Bitdefender's technologies based on machine learning and trained to detected anomalies and sophisticated attacks and malware. It can prove invaluable for organizations that constantly face threats but also have a predictable workflow in terms of software installed on endpoints and employees accessing online resources.

With 97 percent of data breaches caused as a direct result of a spearphishing email, according to 2018 Verizon Data Breach Investigations Report, defenses against this particular attack vector can also be part of a security automation strategy. For example, having employee email attachments detonated within a sandboxed environment built to simulate the users' machine while also containing threat analysis tools, can help organizations detect and prevent threats from reaching the endpoint. This sandbox analyzer can be a powerful tool during the threat analysis process, as IT and security teams can use the threat intelligence collected during the contained execution process and not just increase their security posture by patching identified vulnerabilities, but also proactively design new security procedures and practices meant to address similar problems in the future.

Bitdefender's Sandbox Analyzer is built around these principles, and it's not integrated with the endpoint security agent, but also automatically submits suspicious files for detonation within a sandbox. This security automation tool can be highly effective at identifying fileless threats based on scripts and even advanced persistent threats that try to evade traditional endpoint-deployed security layers.

However, the true pinnacle of security automation is detection and threat response automation. While it's not usually a single technology, but rather a bulk of behavior and anomaly detection technologies and tools, it can help protect against never-before-seen threats during the on-execution stage. Everything from obfuscated malware to targeted attacks, script-based attacks, exploits and even ransomware can be quickly and automatically identified based on a "zero-trust" model by analyzing everything going on within the operating system, both in user mode and kernel mode.

Of course, any truly effective automated detection and response tool should also be able to maintain a trail of changes made by malicious processes and roll back those chances in case of malicious actions.

The ultimate goal when using any automated detection and response is to limit the number of security warnings and offload incidents response times from IT and security teams to the automated solution. Having a solution that can only focus on truly important security warnings and not cause alert fatigue to security operations teams is the true measure of an automated security tool.v

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers. More information is available at http://www.bitdefender.com/.

BD-Business-Oct.30.2019-TK#: 70585