Continuous Security Monitoring for DevOps

UpGuard

Table of Contents

Introduction 3

I. Understand Current Trends in Intrusions and Attacks 5

II. Identify Existing Vulnerabilities 8

III. Assess Current Defense Mechanisms 9

IV. Implement CM and Continuous Security Testing 10

Summary 11

Appendix 12

I. Introduction

Recent articles and books discussing IT security invariably begin by painting a dismal landscape rife with rising cyber threats increasing in both sophistication and volume. Interestingly, this is no different than sentiments echoed by literature from a decade ago; a decade from now, security will also still be a pressing issue, if not the focal point of enterprise concern. Fending off cyber attacks and maintaining security may be business as usual for enterprise IT, but vigilant organizations in recent years have been boosting their security measures in response to both increasing cyber crime and heightened control requirements from regulatory bodies. For enterprises content with yesterday's or even today's security mechanisms, tomorrow's intrusion methods will likely arrive unannounced and sooner than expected.

> *"Macro changes in attack targets and threats to the enterprise, as well as the IT delivery model, are shaping the risk and security landscape over the next decade."*

Source: Gartner, "Global Security Futures: Architectural Implications of Gartner's Security 2020 Scenario", December 17, 2013

> *"The threat to cybersecurity will grow as industries adopt new technologies, architectures and business methods, and as terrorists become more sophisticated."*

Source: Gartner, "Cyberterror Poses Growing Threat to Financial Services", October 1, 2002

The Expanding Attack Surface

Transformational technologies such as the cloud and mobile—while enabling enterprises to be highly agile and efficient— have given rise to IT infrastructures of unprecedented complexity and variance. Firms standing to benefit from the cloud's horizontal scalability and pay-per-use consumption model often neglect to gauge the impact these technologies have on existing systems. This is especially typical of enterprise workplace cloud applications: employees are quick to adopt new SaaS offerings, leaving IT staff trailing behind in their efforts to secure them. Furthermore, the predominance of enterprise SaaS applications and resulting decentralized data requires IT to completely rethink its data security strategy. RESTful cloud applications and web services make integration and extensibility trivial through safe, standardized methods of communication and data exchange; however, if not built carefully they can easily fall victim to unique REST API security issues like mashup-related vulnerabilities, among others—in addition to the traditional security flaws of standard web applications.

> ***"Traditional security models will be strained to the point that, by 2020, 60 percent of enterprise information security budgets will be allocated for rapid detection and response approaches, up from less than 10 percent in 2013."***

Source: Gartner Press Release, "Gartner Says the Nexus of Forces is Transforming Information Security", October 24, 2013

Today's IT infrastructures can simply no longer be designed with an on premise mindset. Enterprise security measures must transcend the notion of securing just the perimeter, as the perimeter is fast disappearing. For instance, hybrid technologies allow data centers to burst to the cloud when needed, effectively giving enterprises infinite scalability for their applications and systems. The security cost to these benefits are manifest in the unique challenges of securing data across multiple cloud service providers, protecting cloud-based systems and physical/virtual network endpoints, and securing mobile devices that access cloud resources.

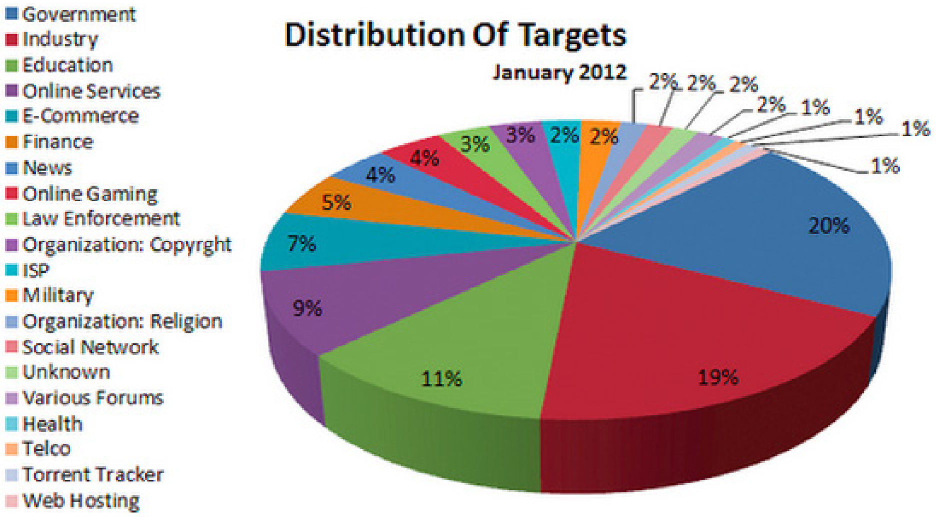
Ultimately, the combined negative impact of these transformational technologies is a rapidly expanding potential attack surface: the sum of all known and unknown vulnerabilities that could lead to an intrusion or compromise. New vulnerabilities and intrusion methods that render existing security measures ineffective comprise part of the attack surface. Enterprise adoption of the cloud, mobile devices/BYOD, and IoT (as well as other technologies on the horizon) also increase a firm's security risk exposure by potentially enlarging its attack surface. New mechanisms for mitigating risk are therefore continuously needed as the attack surface organically expands over time. Unfortunately, adapting enterprise security mechanisms accordingly to reduce the chances of a security compromise is an arduous and complicated affair for many enterprises.

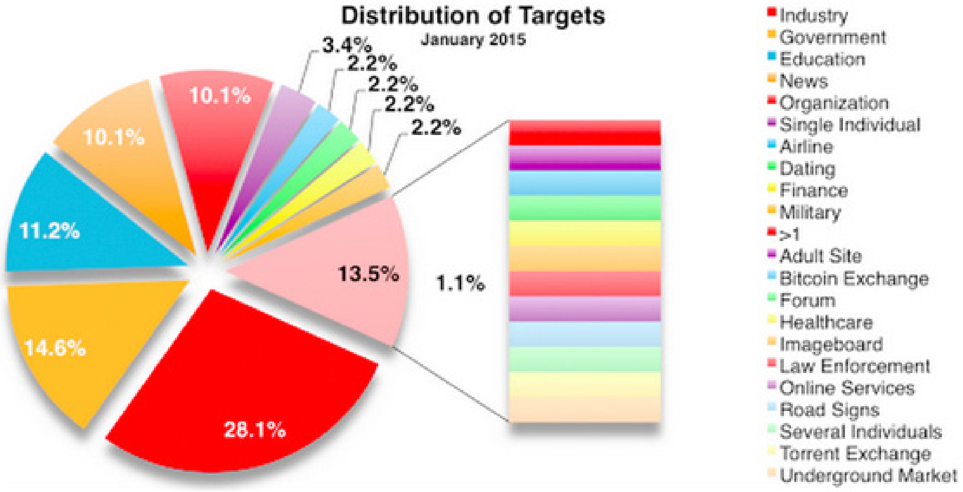
So how does one position their enterprise against a rapidly expanding attack surface? Implementing processes for continuous security monitoring is an effective and sustainable approach to combating security threats on an ongoing basis. To this end, the following 4 steps may provide enterprises some guidance in preparation for continuous security monitoring.

II. Understand Current Trends in Intrusions and Attacks

Analysis of patterns and trends in recently documented intrusions and attacks is instrumental to improving one's security posture against known and unknown threats This information in turn can provide guidance on how to bolster the firm's security mechanisms in anticipation of future threats. Luckily, there is no shortage of data for these purposes—the volume and frequency of attacks in recent years allows for a degree of predictive analysis in combatting future intrusion methods and attempts. A comprehensive enterprise security framework should include continual, detailed tracking of threat statistics to assess an organization's security strengths/weaknesses against the direction attack trends are heading. As an example, the following is a cursory overview of attack patterns and trends that shed some light on areas of concern.

In 2012, industry firms were the main target of security compromises, accounting for 19% of attacks. Attacks on government systems came in second with 11% of attacks. In 2015, industries accounted for 28.1% of attacks, while government attacks accounted for 14.6%. Industry enterprises in particular should therefore be on hyper-alert for attacks and intrusion attempts.

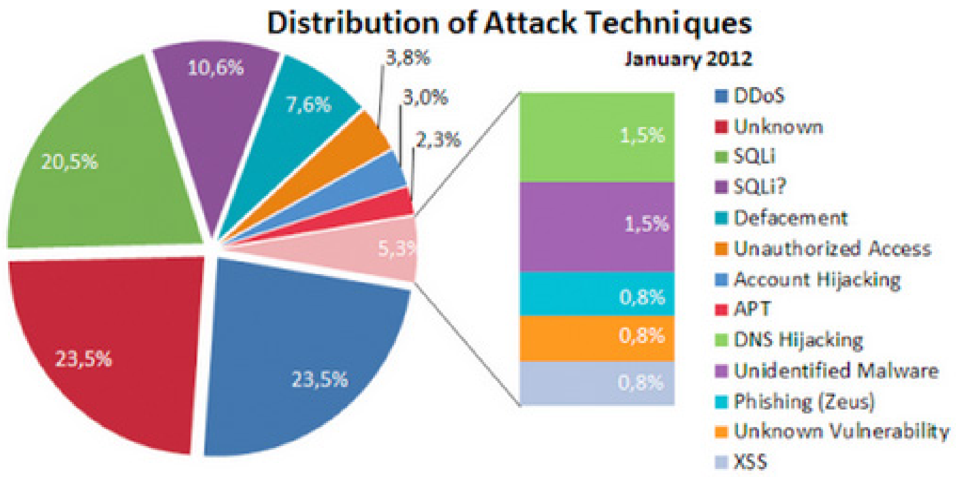


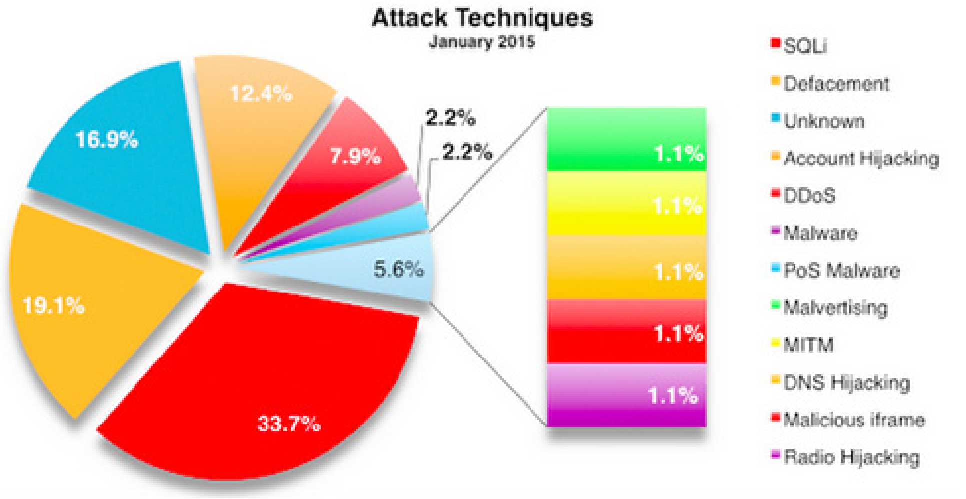


A. Prominent Targets
The following charts above the distribution of attack targets: the first represents data taken from January 2012, the second is from January 2015.

DDoS attacks comprised 23.5% of attacks for January 2012, with another 23.5% of attacks using unknown techniques. In January 2015, however, SQLi attacks made up the majority of attacks. Taking advantage of SQLi-based vulnerabilities is a popular web application intrusion method; the rise in its popularity among cyber criminals can be correlated to the general increase in popularity of SaaS applications and ubiquitous open source CMS packages like Drupal and WordPress—the latter of which powers 23.7% of all websites.

In fact, both of these CMS offerings have fallen victim to SQLi exploits in recent years. Enterprises deploying database-driven web/cloud applications should therefore take heed: hackers are now increasingly targeting the application stack for low-hanging intrusions, along with the typical intrusion methods focusing on underlying systems and network layers.





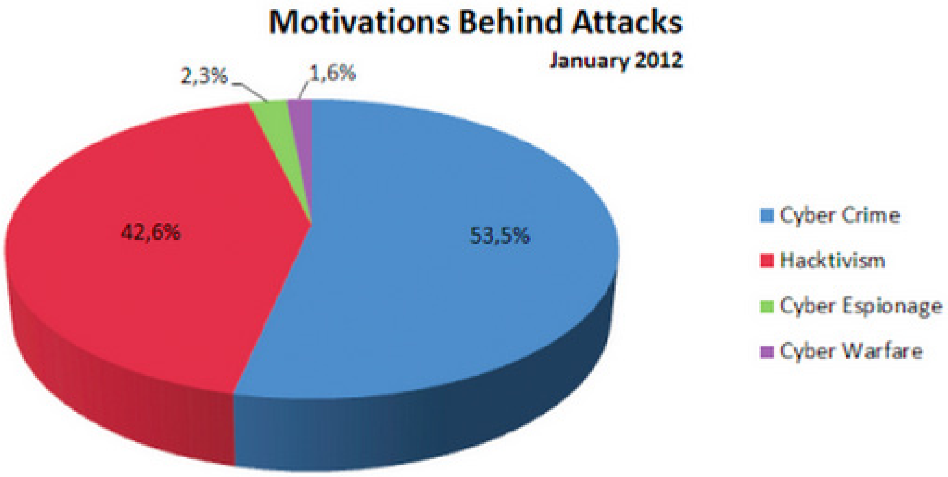
B. Attack Techniques
The following chart on the right depicts the distribution of attack techniques: the first is for January 2012, the second is for January 2015

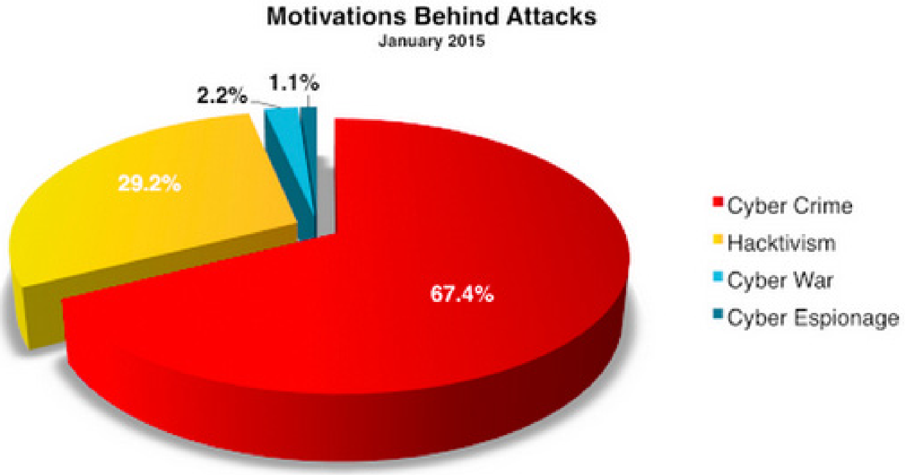
The vast majority of attacks are for criminal purposes like credit card, identity, and intellectual property theft. Enterprises should determine the extent to which their systems store sensitive data (e.g., customer/ employee information, credit card data) and to what extent those systems are vulnerable.

The facts stemming from the previous data can be interpreted as follows: (a) web application exploits are on the rise, and (b) are primarily targeting industry enterprises (c) for criminal purposes like theft and fraud. While this may not be especially enlightening, the example serves to illustrate how enterprises can build and assess their security profiles using current trends in intrusions and attacks. More granular attack data and trends are readily available for firms wishing to further refine their security posture against existing and unknown threats/vulnerabilities.

> ***"Your medical information is worth 10 times more than your credit card number on the black market."***

Source: Reuters





C. Motivational Trends

The following chart on the right depicts motivations for attacks: the first is for January 2012, the second is for January 2015. In both cases, cyber crime accounted for roughly over half of all attacks.

II. Identify Existing Vulnerabilities

Equipped with insight into the range of threats the enterprise is potentially facing, one can assess which critical vulnerabilities are present in the firm's infrastructure. Though methods for going about this vary (a myriad tools and solutions exist for achieving this end), a database or repository containing the latest threats and intrusions is required for testing systems against current attack patterns and identifying potentially vulnerable configurations.

The Open Vulnerability and Assessment Language (OVAL)

A popular reference point for current vulnerability data is Mitre's Open Vulnerability and Assessment Language (OVAL). Though the acronym refers to Mitre's XML-based language for creating security tests, the eponymously-named open source project and standard serves as a preeminent resource for security and vulnerability data. Integral to OVAL is its comprehensive open source repository of OVAL definitions: machine-readable tests that enable standardized testing procedures to check for software vulnerabilities, configuration issues, programs, and patches. With OVAL definitions, one can determine which systems are prone to or possess a given vulnerability.

UpGuard and OVAL

UpGuard has integrated OVAL into its platform to provide full vulnerability scanning and assessment. Augmented by OVAL's up-to-date repository of vulnerability definitions, UpGuard enables users to easily test systems for the presence of critical exposures and misconfigurations. Furthermore, once vulnerabilities are detected, users can automate the proper course of action towards remediation with features such as alerts, task assignments based on event triggers, and more. By combining the latest data regarding current vulnerabilities and threat patterns with powerful discovery, configuration management (CM) and monitoring capabilities, UpGuard delivers a comprehensive solution that ensures enterprise systems are protected against present and future threats.

III. Assess Current Defense Mechanisms

The mechanisms implemented for enterprise security are just as prone to vulnerabilities as the resources and systems they are protecting. Typically, firewalls and IDS/IDPS solutions stand as the first and second line of defense against external breaches. But what of threats originating internally? Acts of a disgruntled employee or the effects of a Trojan can be difficult to trace and remediate, especially if security controls are designed to protect against threats from external environments. IDS/IDPS solutions using both signature and anomaly-based threat detection can be effective in identifying internal threats, but carry the negative side effect of generating many false positives. To make matters worse, resulting exposures often go undetected for some time when these types of security devices have been compromised. Potential systemic security failures can ensue, wreaking havoc throughout the entire enterprise environment.

Firewalls and Diminishing Returns

Firewalls for years have provided effective perimeter-based security, but as mentioned previously—the concept of the perimeter network is slowly dissipating with the growing preponderance of virtual servers and cloud infrastructures. Clearly, an on premise network firewall provides very little if any protection for IaaS and PaaS enterprise customers. According to Gartner's estimates, roughly 75% of all servers in 2014 are virtual, with a steady increase in adoption expected over the next several years. The current popularity of hybrid cloud deployment models is indicative of the steady adoption of cloud technologies for mission-critical, highly secure applications—a transition that just a few years ago was cause for great security concern among enterprises.

To address this increasing presence of new infrastructure paradigms like the hybrid cloud, vendors are providing their own configurable firewall solutions for securing servers and applications within the service offering's cloud. For example, AWS offers EC2 security groups as a virtual firewall to protect server instances and applications hosted in Amazon's cloud. These virtual firewalls essentially function the same as their on premise counterparts and are subject to the same limitations. For example, customers are left with little recourse in the event that an unauthorized virtual firewall port is opened—either accidentally or by an intruder or bot.

IV. Implement CM and Continuous Security Testing

In the same sense that rising demand and increased consumption of widely accessible, scalable IT resources gave rise to the cloud, rapidly expanding and ever-evolving threats have given rise to continuous security testing. With this approach, the challenges of IT security can managed like contemporary software: with agility, continuously tested/monitored, and responsive to constant changes. Because the threat of the unknown casts such a looming shadow over enterprise security solutions, it's important that firms employ solutions that are agile, scalable, and highly responsive to new and evolving attack methods.

Using CM tools like UpGuard to establish a proper, secure starting point for maintaining confidence in enterprise system integrity is critical for ongoing security testing and monitoring. Such tools can provide crucial verification and risk assessment of proposed changes to a system. For example, configuration items (CI) can be tested against approved secure configuration baselines to ensure that they are up to par. Resulting information can then in turn provide the requisite information for identifying breaches in policies and procedures, as well as intrusions and security compromises.

> ***"The Only Thing That Is Constant Is Change"***
>
> \- Heraclitus

Summary

Enterprise IT security initiatives must take a multi-tiered approach these days to provide effective, comprehensive protection. Different lines of defense are necessary to protect today and tomorrow's enterprise networks, with various solutions interacting and complementing each other—even discovering vulnerabilities/openings in the other solution's respective line of defense. The 4 steps outlined previously provide pragmatic initial steps towards gearing up one's enterprise for continuous security monitoring:

1. Understand Current Trends in Intrusions and Attacks
2. Identify Existing Vulnerabilities
3. Assess Current Defense Mechanisms
4. Implement CM and Continuous Security Testing

In short, the sheer evolution and advancement of recent technologies makes it necessary to constantly test, assess, and re-evaluate tools currently being used for combating cyber attacks. Moore's Law is intent-agnostic and applies to technological advances created for both noble and nefarious purposes. Without the latest security tools and methodologies, enterprises fall victim to technology in the truest sense: at the mercy of hackers, intruders, or anyone with the technological wherewithal to gain access to their systems. As the goal of attaining effective enterprise security is a moving target, firms must adopt a multi-tiered approach to protecting their infrastructures to include continuous security monitoring. This involves both addressing new malware, vulnerabilities, and intrusion methods as they surface, as well as securing systems against future unknown threats. ■

Appendix

References

http://blogs.gartner.com/adam-hils/2015-8-network-security-trends-that-wont-gain-t-raction/

http://www.forbes.com/sites/sungardas/2015/01/02/cyber-security-professionals-predict-their-biggest-concerns-for-2015/

http://people.cis.ksu.edu/~xou/publications/tr_homer_0809.pdf

http://www.infoworld.com/article/2616316/security/the-5-cyber-attacks-you-re-most-likely-to-face.html

http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-attack.html

http://www.cio.com/article/2908134/cloud-computing-brings-changes-for-it-security-workers.html

https://technet.microsoft.com/en-us/library/cc959354.aspx

http://www.personal.psu.edu/users/j/m/jms6423/Engproj/Types%20of%20Attacks.xhtml

http://searchsecurity.techtarget.com/video/Rethink-network-design-with-next-gen-network-security-architecture

http://www.sanog.org/resources/sanog14/sanog14-apnic-Security-21072009.pdf

http://www.symantec.com/connect/articles/security-11-part-3-various-types-network-attacks

http://www.networkworld.com/article/2163059/cloud-computing/hybrid-clouds-pose-new-security-challenges.html

http://www.csoonline.com/article/2124905/identity-management/why-rest-security-doesn-t-exist--and-what-to-do-about-it-.html

https://securityledger.com/2013/10/gartner_traditional_it-security_dead_by_end_of_decade/

http://hackmageddon.com/2015/02/05/january-2015-cyber-attacks-statistics/

*All charts are from hackmageddon.com