APPSEC PHOENIX

VULNERABILITY MANAGEMENT AT SCALE AND THE POWER OF CONTEXT BASED PRIORITIZATION

CVE CVSS, CWE CWSS are not sufficient anymore. Prioritize vulnerabilities with contextual awareness and threat intelligence

info@appsecphoenix.com www.appsecphoenix.com +442031953879

CVSS, CVE And The Land Of Broken Dreams

Table Of Contents

[1. Executive Summary **3**
[1.1 Introduction to the Enterprise Digital Landscape 3
[1.2 The Complexity of Digital Transformation 3
[1.3 Risk Management: The Need For Contextual Visibility / Context is King 4

[2. Modern Enterprise Cybersecurity **5**
[2.1 The Operational Complexity Of Enterprise Cybersecurity 5
[2.2 Enterprise Cybersecurity Program Inputs 6
[2.2.i Cybersecurity Frameworks 7
[2.2.ii Threat Intelligence Information 7
[2.2.iii The Common Vulnerability Enumeration (CVE) System 8

[3. Enterprise Cybersecurity Risk Management **8**
[3.1 Calculating Risk Within An Enterprise Cybersecurity Program 8
[3.2.i The Fundamental Risk Equation 9
[3.2.ii Factor Analysis of Information Risk (FAIR) 9
[3.2.iii The Exploit Prediction Scoring System (EPSS) 9
[3.3 Residual Risk 10

[4. Putting It All Together: Context Is King **10**
[4.1 Inputs To Calculate A Better Contextual Risk 10
[4.1.i The severity of a vulnerability 11
[4.1.ii The probability of exploitation 11
[4.1. iii How important the asset is 11
[4.1.iv The locality of the asset 11
[4.2 Automating The Whole Process 12

[5. Scenarios **13**
[5.1 Scenario 1: Timeline Of Exploitation Impacts Contextual Risk 13
[5.2 Scenario 2: How Risk Depends On Locality For Two Vulnerabilities 16
[5.3 Scenario 3: How Risk Depends On Severity and Locality of System 17

[6. How To Automate Triaging And ACT Now On Prioritizing Vulnerabilities? **17**

[7. Conclusion **19**

[8. References **21**

[1. Executive Summary

[1.1 Introduction to the Enterprise Digital Landscape

Modern enterprises use IT technologies to improve business productivity and to provide innovative new products and features to customers [1]. However, digitization also exposes an organization to cyber risk that could result in significant financial and reputational damage, or even cause the demise of an organization. The costs of a medium size cyber-breach can amount to hundreds of thousands of dollars, while large incidents can cost millions to hundreds of millions in incurred damages [2]. According to IBM, the average cost of a large enterprise data breach was $4.35 million [3]. While large organizations may be able to weather such financial hardships, other research indicates that 60% of small businesses fail within six months of a cyber-attack [4].

Digital risks have not stopped the adoption of new information technologies; however in response to the increased risk, proactive enterprises of all sizes are implementing cybersecurity programs to protect themselves against cyber-attacks with security policies, controls, and cybersecurity-centric activities. A key component of an enterprise cybersecurity program - vulnerability management - proactively scans IT environments for vulnerabilities and remediates them in a timely manner. In contrast, other components include preparing back-ups and making recovery plans to respond if cyber-breaches do occur.

Building a cybersecurity program starts with a risk assessment and then prioritizes IT systems and information according to their calculated risk score. In theory, this approach is sound operationally however, it is challenging to scale and maintain. Cyber-risk management programs present significant challenges because an organization's IT infrastructure is complex and constantly evolving [5]. Aside from continuous change and technical complexity, the IT industry also suffers from a cybersecurity talent shortage [6].

Organizations can overcome these challenges and implement optimal risk management and cybersecurity programs by intelligently prioritizing cybersecurity activities. Strategically prioritizing cybersecurity activities intelligently according to an accurate contextual risk score, enterprises can overcome the challenge of an industry-wide skills gap and gain strong assurances of operational resilience.

[1.2 The Complexity of Digital Transformation

The benefits of technology-supported productivity come at the cost of digital complexity. IT infrastructure is operationally complex, which necessitates an equally complex approach to risk assessment. The traditional endpoint management strategy has expanded to include more cloud and off-premises computing solutions, more reliance on third-party applications, bring-your-own-device (BYOD) policies and IoT policies that invite more devices on the network, more social networking and business productivity applications, and a work-from-home model that requires more remote access services. This ever-increasing scope of what constitutes a corporate network has exponentially increased the attack surface.

On top of the technical complexity of IT infrastructure, other challenges that add additional complexity are also emerging within the IT industry, such as regulatory and industry compliance, sourcing qualified talent, and gaining competitive advantage. Organizations need to find solutions to risk management and cybersecurity that enable a high degree of assurance and efficiency.

[1.3 Risk Management: The Need For Contextual Visibility / Context is King

Cyber-risk assessment allows the prioritization of IT systems and information so appropriate policies, controls, and activities can govern their protection. The risk scores calculated during an assessment are weights of criticality that depend on asset-specific inputs, including business impact analysis (BIA), technical specification and locality, and cyber-threat intelligence (CTI) in order to be contextual. Without context, prioritization efforts are arbitrary and ad-hoc, leaving an organization haphazardly defended and at increased risk.

The most basic calculation of IT security risk combines the probability of exploitation with the potential impact on an organization should a breach occur. While this basic equation is rational, it must be expanded for practical application. Considering that enterprise IT infrastructure and the cyber-threat environment are constantly evolving ecosystems means that risk calculation must also be adjusted periodically.

Cyber-risk visibility - the ability to visualize an entire IT environment's business impact risk and cyber-threat-risk contextually - is evolving management science. This whitepaper aims to provide a perspective for calculating cyber-risk context across an organization’s IT infrastructure and present a logical system of inputs that allow a more accurate cyber-risk contextualization. The presented approach allows decision-makers to take better advantage of cyber-security resources while increasing the effectiveness of their cybersecurity efforts.

[2. Modern Enterprise Cybersecurity

Cybersecurity programs are multi-component, evolving, iterative processes and their ultimate goal is to protect the operational resilience of an organization. Their primary technical objectives are typically viewed through the lens of protecting the Confidentiality, Integrity, and Availability (CIA Triad) of information and information systems within an organization's infrastructure, and these primary technical objectives are accomplished by designing and implementing policies, controls, and processes that reduce the chances of compromise and allow a quick and effective response in the case of a security incident. In fact, a cybersecurity program is considered the only effective strategy for preventing attackers from penetrating private networks, stealing, encrypting, ransoming, or outright destroying information such that it is unrecoverable [7].

[2.1 The Operational Complexity Of Enterprise Cybersecurity

Enterprises big and small are responding to the increased risk presented by cyber-threats by implementing cybersecurity programs to mitigate the risk posed by digital transformation. However, modern enterprise cybersecurity is anything but static, simple, or predictable. On the contrary, it is dynamic, complex, and uncertain.

Digital transformation offers a competitive advantage [8], but as digital business operations and associated IT infrastructure become increasingly complex, cybersecurity programs also become prohibitively complex and can lose their structure and effectiveness. New vulnerabilities are disclosed on a daily basis, and a talent shortage within the cybersecurity profession places added pressure on IT security team members resulting in a high degree of burnout and personnel turnover. This balance means that addressing all vulnerabilities is operationally infeasible and the ability to accurately prioritize security activities has a big impact on an organization’s degree of protection.

Below is an example of many (but not all) potential components of an enterprise IT infrastructure that a cybersecurity program may be tasked with defending and a high-level topography of typical enterprise IT components is shown in Figure 1.

Network Context Security (LAN / WAN) ● Network design, performance, and compliance ● Segmentation ● Wireless networks ● Remote access services ● IoT & peripherals services ● Backup and recovery planning Vulnerability Management: ● Application security ● DevSecOps ● 3rd party vendors ● Vulnerability scanning ● Penetration testing ● Change management Regulatory and Industry Compliance ● Reporting requirements ● User privacy requirements	Infrastructure Security ● Operating systems ● Application whitelisting / blacklisting ● Ingressing email communications ● 3rd party vendor reliance Application Security ● Code security ● Runtime vulnerabilities ● Open-source vulnerabilities ● CI/CD vulnerabilities ● 3rd party vendor requirements ● CWE Top Ten ● OWASP Top Ten Website Security ● CMS web application framework vulnerabilities ● Website vulnerabilities ● Plug-in vulnerabilities

Container complexity • Chassy and hosting complexity • Tenancy separation and isolation of containers • Container security • 3rd party software library security API Security • Identity and access management • JWT and similar • OWASP API Top Ten	• OWASP Top Ten Added Complexity • Cloud Workload • Cloud IAM and identities • Cloud Data and misconfiguration

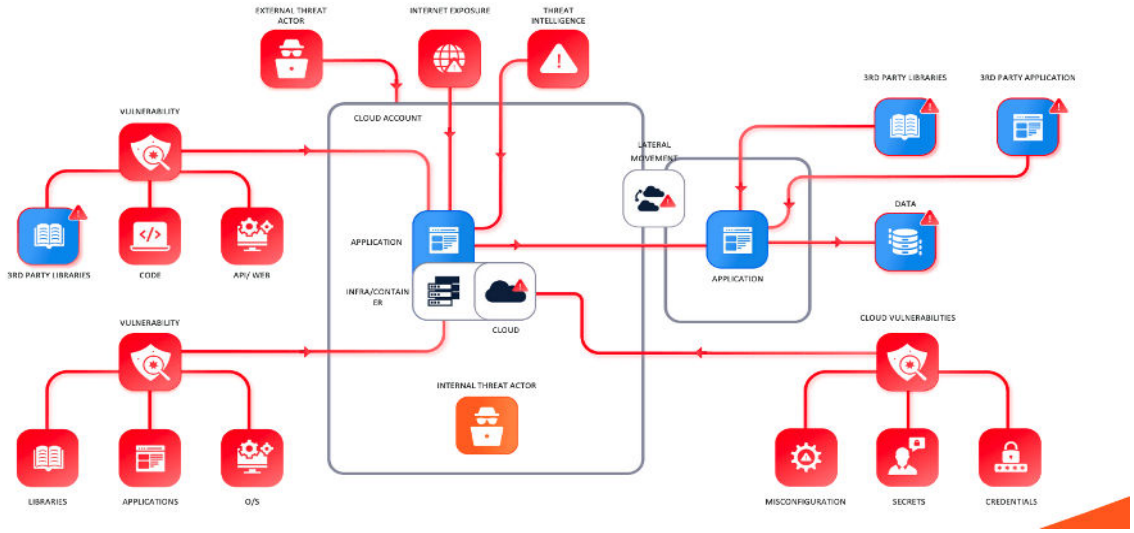


Figure 1: A topography of IT components in a typical enterprise

A cybersecurity program includes activities such as - but not limited to:

- Administrative policies, controls, and standard operating procedures (SOP)
- Technical policies, controls, and SOP
- Physical policies, controls, and SOP
- Mandatory training programs to increase user awareness
- Vulnerability management programs
- Continuous monitoring of network and endpoint activity to detect any indicators of compromise (IOC)
- Incident Response Plans (IRP) and Disaster Recovery Plans (DRP)

[2.2 Enterprise Cybersecurity Program Inputs

An organization's cybersecurity program depends on various inputs during the course of its design and lifecycle. These inputs all serve different purposes, but in general, the most critical inputs are (1) IT industry standard frameworks and advisories to ensure that peer-reviewed best practices are being followed and (2) Cyber-threat intelligence such as vulnerability scoring systems, adversarial behaviour analysis, and malware signatures for adjusting protection profiles in real-time.

[2.2.i Cybersecurity Frameworks

Following recognized industry standards and best practices is important for building a comprehensive approach when developing and maintaining an enterprise cybersecurity program. Industry-leading IT security frameworks and advisories formalize reliable peer-reviewed information, providing a solid base for the design and implementation of security policies, controls, and procedures. IT security frameworks also relay best practices for specific asset types such as application security, cloud security, and critical infrastructure. Tried and tested approaches provided by well-known and respected frameworks also help to provide a solid foundational starting point and prevent a cybersecurity program from being arbitrary or ad-hoc.

The major IT security frameworks are:

- NIST CSF [9]
- ISO 27001 [10]
- COBIT-5 [11]
- CERT-RMM [12]
- CIS-CSC [13]

[2.2.ii Threat Intelligence Information

Cyber-threat intelligence (CTI) data provides insight into adversarial behaviors such as tactics, techniques, and procedures (TTP), attack patterns, threat actors' motives, and detection information such as malware signatures and indicators of compromise [14]. CTI enables better, evidence-supported security decisions and proactive defensive strategy by responding to what is currently evolving in the threat landscape.

CTI can come from a variety of sources including publicly available systems and repositories, internal sources such as host and network IDS/IPS, SIEM data, or honeypot, private sources such as specialized CTI platform feeds and security product feeds from malware scanners, EDR/XDR products, and vulnerability scanners.

Some most commonly used sources of Cyber Threat Intelligence (CTI) include:

- **Common Vulnerability Enumeration (CVE) System** [15] the IT industry's de-facto source of new and historical vulnerability information which also includes the Common Vulnerability Scoring System (CVSS) and Common Platform Enumeration (CPE) system
- **Common Weakness Enumeration (CWE) System** [16] is a library of hardware and software design weaknesses for software developers and system architects to be aware of and protect against
- **The Exploit Prediction Scoring System (EPSS)** [17] - an enriched assessment of a CVE's CVSS score that better estimates the probability that a vulnerability will be exploited in the wild
- **Official reports and advisories -** this includes official software vendor responses to vulnerability disclosures that affect their products, and advisories from government agencies such as CISA [18] and large IT institutions such as NIST [19] and SANS [20]
- **Chatter -** social media chatter and other internet activity such as blogs or dark-web communication
- **Publically available exploits -** sources of publicly available exploit code such as Metasploit, ExploitDB, and GitHub that host proof-of-concept (PoC) exploit code produced by cybersecurity research analysts and penetration testers

- **CTI metadata** - malware signatures and indicators of compromise (IOC) markup language descriptions such as YARA rules [21] and feeds from malware scanners, EDR/XDR products, and vulnerability scanners

[2.2.iii The Common Vulnerability Enumeration (CVE) System

The MITRE CVE database is considered the de-facto source of publicly available vulnerability information. CVEs are a library of publicly disclosed computer security flaws and include information about the vulnerability's severity and context. This context includes one or more Common Platform Enumeration (CPE) [22] codes that indicate which software applications and versions are affected and a CVSS score [23] accompanied by a vector string that provides additional exploitability context such as whether remote or local access is required, the degree of expertise required to exploit the vulnerability, whether the vulnerability allows an attacker to gain access to higher permissions, whether user interaction is required, and which aspects of the CIA Triad are impacted.

The number of CVEs issued has increased by 10X year on year, flooding decision-makers with reliable but incomplete information. This has made the job of IT security teams difficult at best and unmanageable in some cases. While CVSS scores provide a diverse set of contextual information about a particular vulnerability, the context that can be extracted is quite minimal, and needs to be manually enriched with additional CTI data in order to provide valuable context [24]. Also, while a CVSS vector provides easily accessible insight into the potential impact of a vulnerability, the real and full contextual severity to an organization cannot be extracted from a CVSS vector [25].

For example, the existence and accessibility of exploit code are critical to determining the probability of the vulnerability being attacked. While the CVSS "Exploit Code Maturity" temporal score metric relays whether PoC exploits code exists, it only relays its degree of maturity on a scale of 1-4. While moderately revealing, Exploit Code Maturity provides a less than desirable amount of information for prioritization and the same is true for other CVSS components.

[3. Enterprise Cybersecurity Risk Management

Risk cannot be completely avoided. Organizations need to choose where to apply efforts to reduce risk. Cybersecurity risk management (RM) helps an enterprise decide what systems and information to prioritize or tolerate. Ultimately, the RM strategy's goal is to ensure that critical systems are prioritized and that assurances are in place which guarantee business operations can be maintained indefinitely. Cybersecurity RM must ensure that appropriate policies, controls, and processes are in place and resources are allocated according to priority [26]. Without this balancing act, efforts to develop a cybersecurity program would be arbitrary, ad-hoc, and inefficient, providing incomplete protection and poor visibility into the location and severity of security gaps.

Corporate cybersecurity budgets have increased in response to the increased risk of the cyber-attack [27], but a talent shortage has limited the development of cybersecurity activities for many organizations. In the current environment where highly skilled cybersecurity talent is hard to find and the number of attacks and cost of a breach is constantly increasing, organizations need to focus their efforts and optimize their ability to identify and prioritize the most critical risks. Decision makers need to have quantitative insight into the context of their IT infrastructure risk and the global cybersecurity threat environment.

[3.1 Calculating Risk Within An Enterprise Cybersecurity Program

Risks are interpreted as mathematical principles, and calculated risk metrics are a final weighted score that executive-level managers use to prioritize IT systems and information. As a digital environment and business operations become more complex, a more complex approach to risk

quantification is also required. It is therefore important to visualize risk as both a high-level concept with basic elements, and as a more complex set of inputs to generate a practical risk assessment.

[3.2.i The Fundamental Risk Equation

The most basic risk equation is useful to gain a high-level understanding of risk, but it is not very useful for practical risk calculation. Expressed as an equation risk can be calculated as such:

$$Risk = Severity * Probability * Impact$$

The impacts of a particular asset being breached include potential lost revenue due to downtime, the costs of lost data, the cost of replacement or recovery to operational baseline, possible regulatory penalties, and sometimes increased cyber-insurance costs. The probability of an asset being compromised depends on a number of factors including its location within the network and the probability of it being attacked in the first place

If evaluated on its simplicity this equation receives high marks, but it offers very little towards a practical assessment of risk. These initial input variables are fine but are obviously confronted with a reality that is much more complex.

[3.2.ii Factor Analysis of Information Risk (FAIR)

For large enterprises, a detailed approach to risk quantification is required. For these cases, Factor Analysis of Information Risk (FAIR) [28] exemplifies a group of risk calculation tools, including an extended risk equation where Impact is derived from asset value and the direct vs indirect damage an attack can pose to the business value of the asset (annualized, per month or hour depending what the reference value is).

[3.2.iii The Exploit Prediction Scoring System (EPSS)

The Exploit Prediction Scoring System (EPSS) [17] is a data-driven method of calculating the probability that a software vulnerability will be exploited, allowing better prioritization of remediation efforts.

The EPSS model uses current threat data from MITRE CVE and other sources of CTI, including

- CVSS v3 score and keyword tags extracted from a published CVE
- CVE metadata, including the number of days a CVE has been published and the number of references listed in the CVE
- CPE metadata such as software application, vendor and version number
- Other forms of information about the vulnerability such as social media chatter, security research, and blog posts
- Online sources of exploit code: Metasploit, ExploitDB, or Github
- Security product data-feeds such as malware scanners or vulnerability scanners
- Number of in-the-wild exploitation observations

The EPSS model specifically evaluates the probability that a particular vulnerability will be exploited in the wild within 12 months of its disclosure, producing a probability score between 0 and 100%. EPSS predicts the probability (threat) of a specific vulnerability being exploited, but it can also be scaled to estimate the threat for multiple vulnerabilities on a server, a subnet, a mobile device, or at an enterprise wide scope. This is possible because of a statistical property about the independence of events and requires simply computing the probability of at least one event occurring.

[3.3 Residual Risk

Residual risk refers to the risk that remains after security controls, process improvements, and mitigations have been applied. Residual risk also includes the risk that has been formally accepted by an organization when they choose to take no action. Many factors can impact how much residual risk remains after a Cybersecurity Program has been designed and implemented. One factor that affects residual risk are the determinations made when calculating risk scores, so it is important that the method for assigning risk scores is well thought out and includes consideration for contextual risk.

[4. Putting It All Together: Context Is King

By enriching asset and vulnerability context, increased visibility is gained, allowing IT security decision-makers the information needed to prioritize security activities while maintaining strong assurances. Without risk context, any approach is a sledgehammer one; an arbitrary and ad-hoc security strategy is not a strategy, and this type of approach increases risk. On the other hand, data-driven decision-making can provide quantified risk scores that are actionable, allowing a company to use a more surgical style approach; calculate contextual risk, prioritize activities, apply resources strategically based on business impact and data-driven probabilities, reduce anxiety and prevent an overwhelmed feeling of unmanageable issues while also providing high-degree security assurance.

Although the number of CVEs published each year has been climbing, placing a burden on analysts to determine the severity and recalculate risk to IT infrastructure, enriching a CVE's context offers an opportunity to increase IT security team efficiency. For example, in 2021, there were 28,695 vulnerabilities disclosed, but only roughly 4,100 were exploitable meaning that only 10-15% presented an immediate potential risk. Having this degree of insight offers clear leverage, but how can this degree of insight be gained?

[4.1 Inputs To Calculate A Better Contextual Risk

When we revisit the most basic method of calculating risk, we see that it combines impact and probability. Although this makes sense, it is only a high-level perspective and useless in practical situations. The business impact, operational criticality, inherent value, and technical locality of all IT systems and information needs to be combined with CTI data that describes the state of the current threat environment. More detailed and better-quality inputs accomplish a more accurate contextual risk score from the perspective of a particular asset or a particular CVE vulnerability. These inputs are discussed below and shown in Diagram 1. Diagram 2 visualizes the combined inputs to show a final suggested priority position.

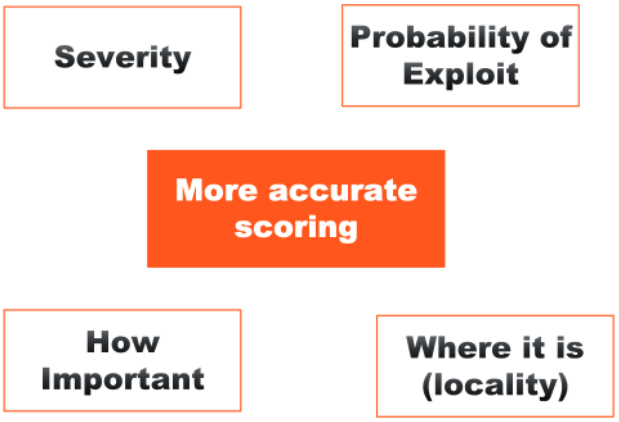


Diagram 1: Context inputs for calculating a risk score

[4.1.i The severity of a vulnerability

Severity measures how much damage can be done to a target system. Regarding prioritization, a vulnerability that allows remote code execution (RCE) without user interaction at admin level system privileges is a very high-severity. However, if the system containing this vulnerability does not contain highly sensitive data and is on a segmented network without a public attack surface, the vulnerability is contextually less severe. If, on the other hand, the vulnerability affects a public-facing system that contains private customer user data, it should be prioritized with a higher score.

[4.1.ii The probability of exploitation

Exploitability measures how much opportunity a vulnerability offers an attacker. Probability depends on the exploitability of a particular vulnerability and is directly impacted by several main factors including, but not limited to, the level of skill required to conduct an attack (known as the complexity of an attack), the availability of PoC code or fully mature malicious exploit code for a particular vulnerability, and whether the vendor of the vulnerable software has issued a security update to fix the security gap. Exploitability can also be enriched with CTI from social media sources and even dark-web reconnaissance. All of these factors impact the greater context of risk.

If fully mature malicious exploit code is available to the general public and can be executed by a low-skilled attacker, the probability of exploitation in the wild increases significantly. On the other hand, if a security patch has been made available by the vendor and remediation can be done quickly, the priority of the vulnerability can be elevated because there is a high degree of protection offered by a simple procedure.

[4.1. iii How important the asset is

Importance measures the potential costs to an organization should an asset be breached and how valuable an attacker may see an asset. Value is directly correlated to the level of risk assurances required for an asset to be considered secure and, therefore, it's level of priority in security planning.

Systems and information may be critical to an organization if they are directly related to revenue-generating activities or host sensitive data protected by national or regional legal regulations such as GDPR or HIPPA or an industry standard such as PCI-DSS. Assets may also be considered especially important if they are significantly costly to replace or refresh to an operational state.

[4.1.iv The locality of the asset

Locality is a measure of an asset’s technical specification and placement in the network topography. A system and the information it contains may be within a local area network (LAN) or wide-area-network (WAN), on external infrastructure (IaaS) that is fully or partially controlled by an organization, on a segmented VLAN network, behind a firewall, network intrusion and detection system (NIDS), or other security appliance, and may be a virtual machine with a type 1 or 2 hypervisor, or use containerization to host one or multiple operating systems and software applications. The type of attacks that an asset is susceptible to and which vulnerabilities impact it depends on its locality.

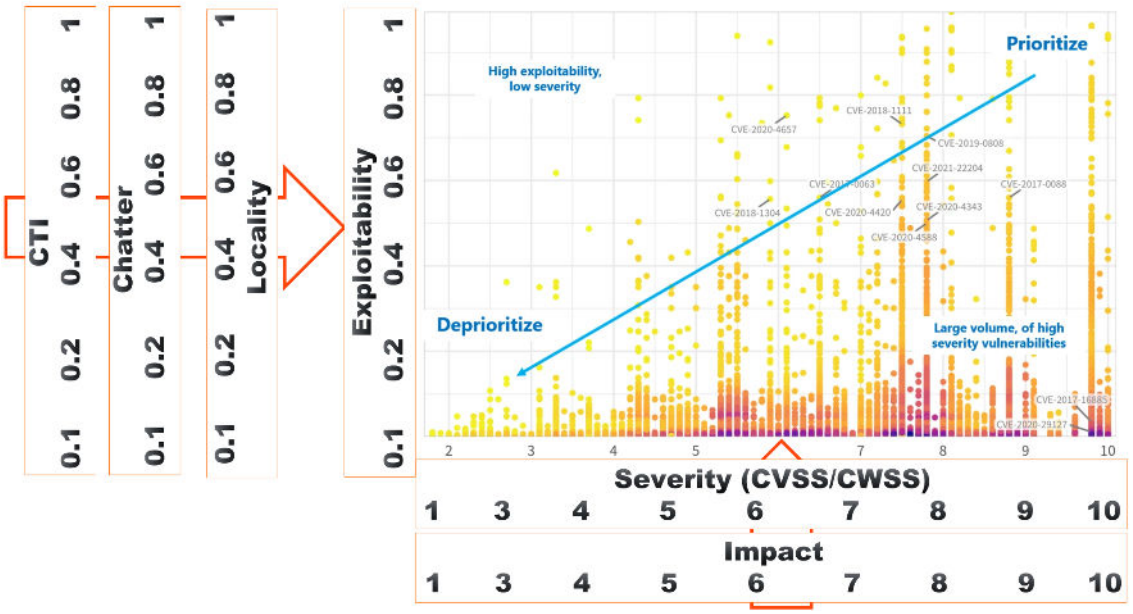


Figure 2: Combining inputs to visualize a final priority position

[4.2 Automating The Whole Process

While operational efficiencies can be gained through the accurate contextualisation of cyber-risk to more effectively prioritize vulnerabilities, operational efficiencies can also be gained by automating the process of collecting related data and calculating a set of contextual risk scores for a particular system, sub-group of systems, or IT infrastructure across an entire enterprise.

Enriching CVE data is prohibitively time-consuming and complex so delegating this task to an IT security team detracts from actual remediation activities. Instead, by presenting human analysts and IT security administrators with an easily accessible list of security priorities by risk score, they can focus on the triage processes such as remediation, responding, developing adjusting controls and policies, or developing training programs.

Figure 5 shows a detailed diagram of the mature triage process and a high-level overview of the steps, including

1. Aggregation - collect the required inputs for calculating a contextual risk score
2. Contextualization - process the collected inputs into a contextualized assessment
3. Quantification - combine the aggregated inputs into a quantified risk score
4. Prioritization - generate a final prioritization score that allows sorting of security vulnerabilities

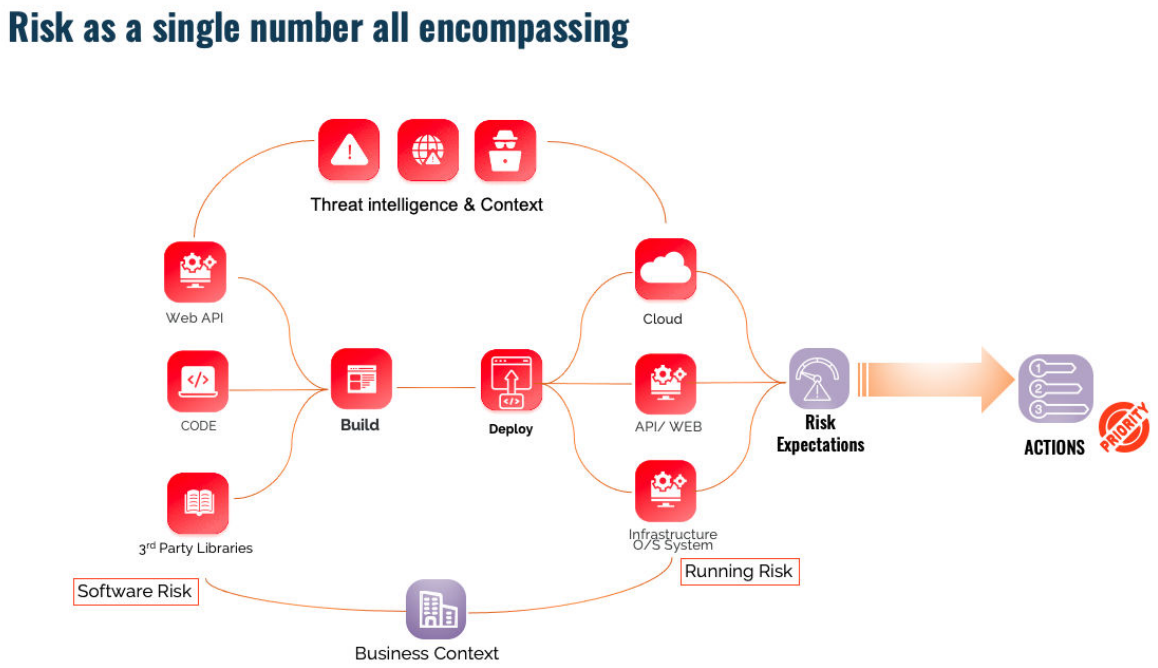


Figure 5: The automated process of prioritizing cybersecurity activities

[5. Scenarios

[5.1 Scenario 1: Timeline Of Exploitation Impacts Contextual Risk

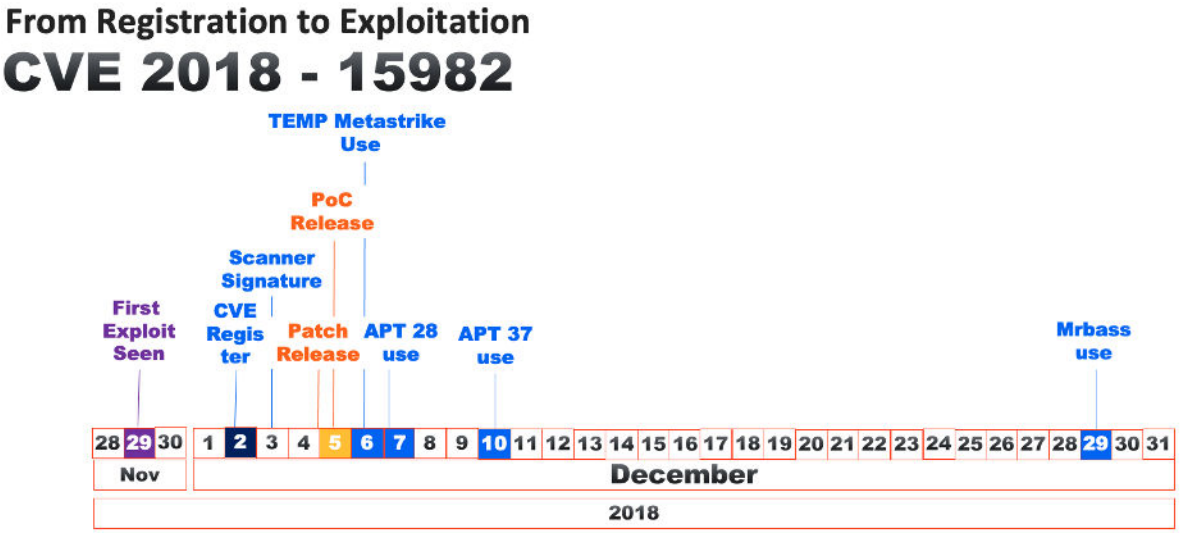


Figure 3: A timeline of events for CVE-2018-15982

CVE-2018-15982 affected Adobe Flash Player versions 31.0.0.108 and earlier, a Mozilla Firefox compatible web browser plug-in. The vulnerability was a use-after-free vulnerability that could give an attacker arbitrary code execution. The CVSS base score was 9.8 and labeled as “Critical”. A timeline of events related to CVE-2018-15982 is shown above in Figure 2. For simplicity, we will only consider how the probability of exploitation impacts contextual risk.

To calculate the probability of exploitation for CVE-2018-15982, we need to combine several CTI inputs including

- Which attacker groups are actively exploiting the vulnerability
- Whether or not an official patch has been released by the vendor
- Whether a publicly available PoC exists
- Whether fully mature malicious exploit code is available
- Is the vulnerability observed to be actively exploited in the wild

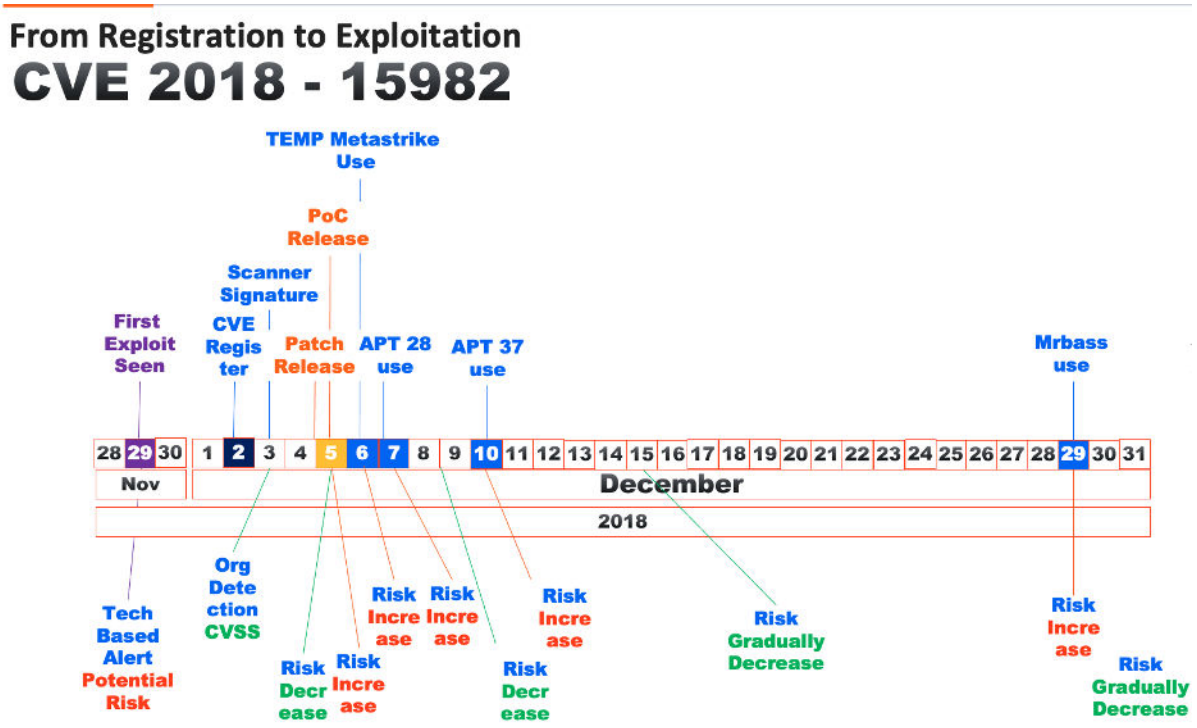


Figure 4: Timeline for CVE-2018-15982 with relative risk assessment

Figure 4 shows the same vulnerability timeline for CVE-2018-15982 with a relative risk assessment below the timeline. Analysis of the vulnerability for a mature triage includes the following significant events:

- November 29, 2018 - the vulnerability is first seen in the wild before the vendor officially acknowledges its existence. This scenario is a “zero-day” vulnerability. It implies that organizations are not prepared to detect it because traditional security products such as malware scanners have no prior knowledge of its existence. The vulnerability in Flash Player can be categorized as “potentially exploitable”.
- December 2, 2018 - CVE is officially issued for the vulnerability and assessed with a CVSS score of 9.8 - critical severity.
- December 3, 2018 - A malware signature is available. The impact on the risk of exploitability is highly contextual depending on the malware signature’s availability to each organization. The contextual risk is reduced if their installed malware scanner has added the signature and scanning applications have been fully updated.
- December 4-5, 2018 - In quick succession, PoC source code and an official security patch from the software vendor are released. The impact on the contextual risk of exploitability quickly diverges. If an organization can quickly deploy the security update, its risk is reduced. Otherwise, the overall risk of exploitation is increased because PoC is available, meaning that attackers now have easy access to source code that can be weaponized.

- December 5-29, 2018 - Increased interest on the web, Twitter chatter, and security researchers are publishing blog articles describing how the vulnerability works, but more importantly, advanced persistent threat (APT) groups are exploiting CVE-2018-15982 scale, and mature malicious exploit code is being shared on dark web forums. The contextual risk for this vulnerability increases dramatically for organizations.

Only using the CVSS score to plan a defensive strategy indicates that this is a critical vulnerability and demands attention. However, when the exploitability factor is enriched with CTI, the contextual risk score changes over time. Also, an opportunity to dramatically save valuable IT security team efforts becomes available through a platform that can automate the aggregation and contextualization of CTI.

To optimize prioritization, security team members could have been automatically notified immediately after the CVE-2018-15982 was published, allowing human analysts to deploy temporary workarounds such as disabling Adobe Flash Player or blocking websites that contain Adobe Flash content. Furthermore, remediation efforts could be optimized by prioritizing CVE-2018-15982 immediately after the official security patch is released. For a human-only team of threat, analysts to optimize prioritization in this way would require a significant number of manhours to monitor and communicate the situation.

Today CVE-2018-15982 has a 50% exploitability, low attack surface (Adobe flash being decommissioned), and almost 0 activity in the wild from most threat actors, the risk level is medium to low. Nonetheless, a CVSS of 9.8. Figure 5 below shows the contextual exploitability risk score evolution over time. In a practical setting, the full set of risk inputs described in Section 4 should be applied, including severity, importance to business operations, and locality, which may further impact the contextual risk score.

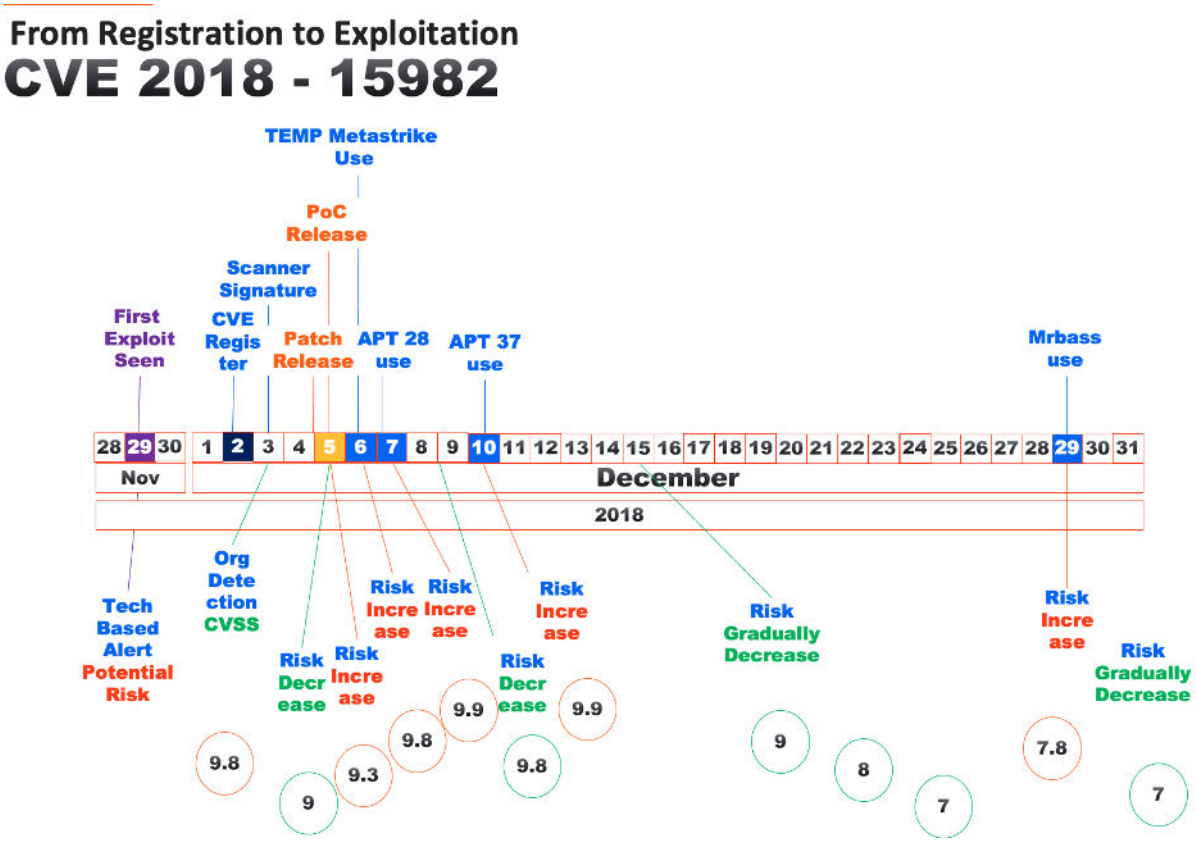


Figure 5: Contextual exploitability risk score evolution for CVE-2018-15982

[5.2 Scenario 2: How Risk Depends On Locality For Two Vulnerabilities

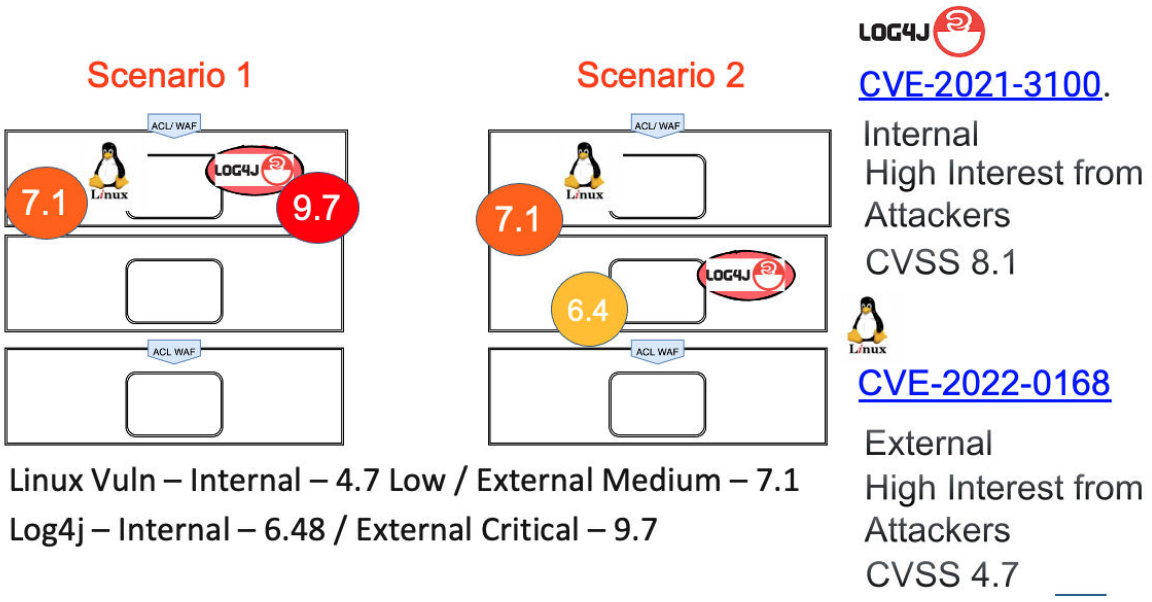


Figure 6: Diagram showing the locality topography for a network that contains both CVE-2021-3100 and CVE-2022-0168

For this case we will compare CVE-2021-3100 (known as Log4J) and CVE-2022-0168 to show how locality of a vulnerability impacts its relative risk. For example, two vulnerabilities result in different final prioritization scores depending on whether they are contained in an internal or external facing system.

Log4J is a remote code execution (RCE) vulnerability that affects Apache Log4j2 versions from 2.0-beta7 to 2.17. 0 on any OS (Windows, Linux, macOS) and can allow a remote attacker to execute arbitrary code on the target server. The exploitability of Log4J depends on having a vulnerable version installed and using it to log unsanitized input that comes from an external source such as a username, HTTP headers, or other incoming data. Log4J has a CVSS severity score of 8.1. CVE-2021-3100 is a denial of service (DOS) vulnerability that affects Linux-based systems. It allows an attacker to disable an affected system resulting in downtime, and has a CVSS score of 4.7.

Considering the locality context of the vulnerabilities as they exist on a network (shown in Figure 6), we see that in Diagram 6 scenario 1 on the left, the Log4J CVSS severity score is increased to a relative contextual risk score of 9.7 and the Linux DOS vulnerability increased to 6.1. Both vulnerabilities have increased their overall risk score because they are publicly exposed.

Diagram 6 Scenario 2 on the right shows a modified network environment where the Log4J vulnerability is no longer on a public-facing system. The Log4J vulnerability is only used for an enterprise's internal application. The locality context reduces the relative severity of Log4J because it does not accept data from a public source that could be crafted to exploit the vulnerability. Because the Linux DOS vulnerability is still on a public-facing system, the two vulnerabilities are not of comparable priority.

[5.3 Scenario 3: How Risk Depends On Severity and Locality of System

For this case, we will again evaluate CVE-2021-3100 (known as Log4J) and compare the contextual risk scores of two independent systems with different levels of business criticality. In Figure 7 below

you can see that the asset represented on the left has a lower importance to the business than the aset on the right which contains personally identifiable information (PII), but they are both impacted by Log4J.

The input factors for calculating how important an asset include:

- Incoming revenue that depends on the asset
- Potential long term impact on the brand (reputational damage) if the asset were compromised
- Number of users affected by a downtime (brand and customer impact)
- Potential regulatory fines, contractual fines, or other compliance consequences as a result of downtime or a data breach

Since the systems have different degrees of business criticality, an evaluation of Log4J's ultimate risk score across the two systems results in a different weighted adjustment of the base CVSS severity score of 8.1. In Diagram 7 (Scenario 1) on the left, the Log4J CVSS severity score is decreased to a relative contextual risk score of 6.48 and further reduced due to the non-criticality of the system to a 5.1. However, on the system that contains PII, the CVSS severity score is increased to 9.7 critical.

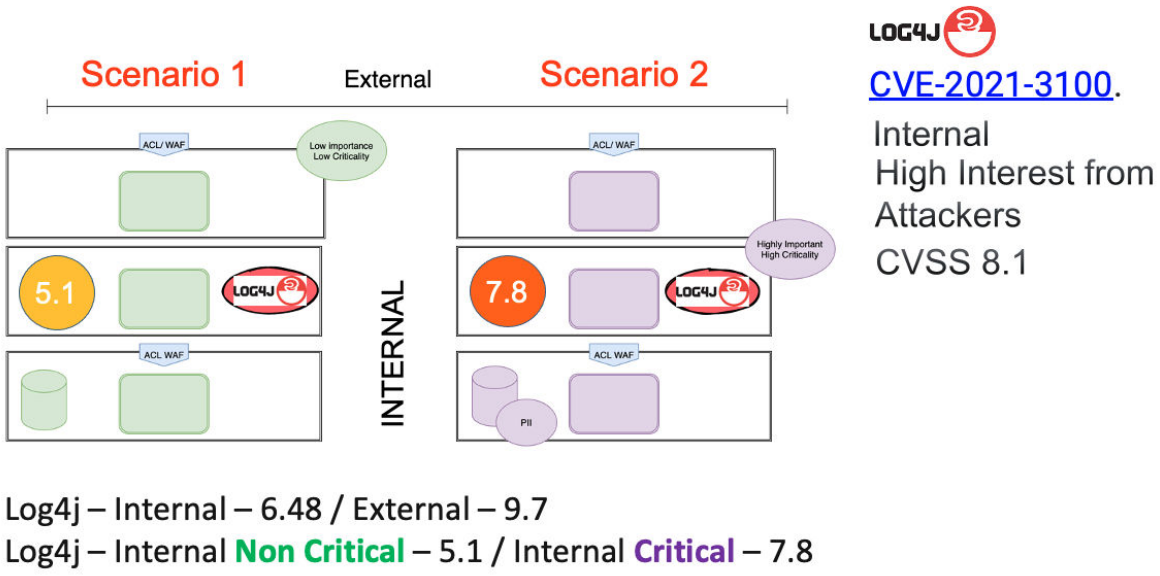
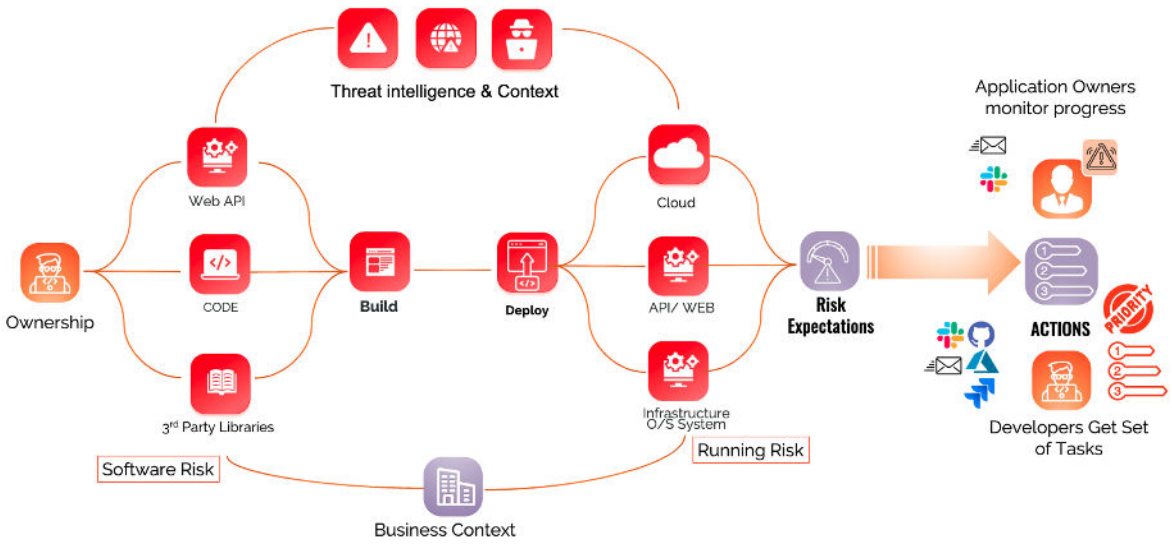


Figure 7: Diagram showing the locality topography for a network that contains both CVE-2021-3100 and CVE-2022-0168

[6. How To Automate Triaging And ACT Now On Prioritizing Vulnerabilities?

For medium and large enterprises, strategically prioritizing assets is key. Addressing all aspects of vulnerability management, application security, cloud security, critical infrastructure, and considerations for legal and regulatory compliance can be daunting and could lead any security professional to be overwhelmed with tasks and information. Security and development teams face significant burdens with a large number of vulnerabilities and triaging and prioritizing vulnerabilities

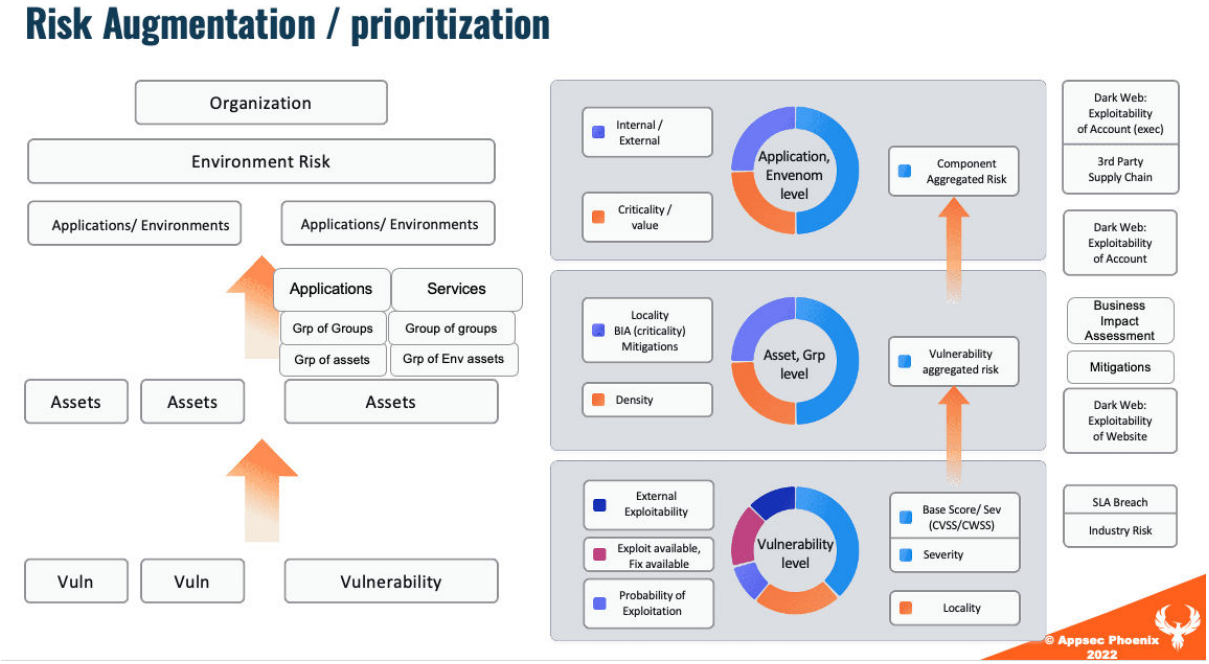
manually is a complex process that can lead to inconsistent decisions and impact the resulting degree of IT security assurance. The consequences of ineffectively implementing a Vuln Management program can be dire to an organization's operational resilience.



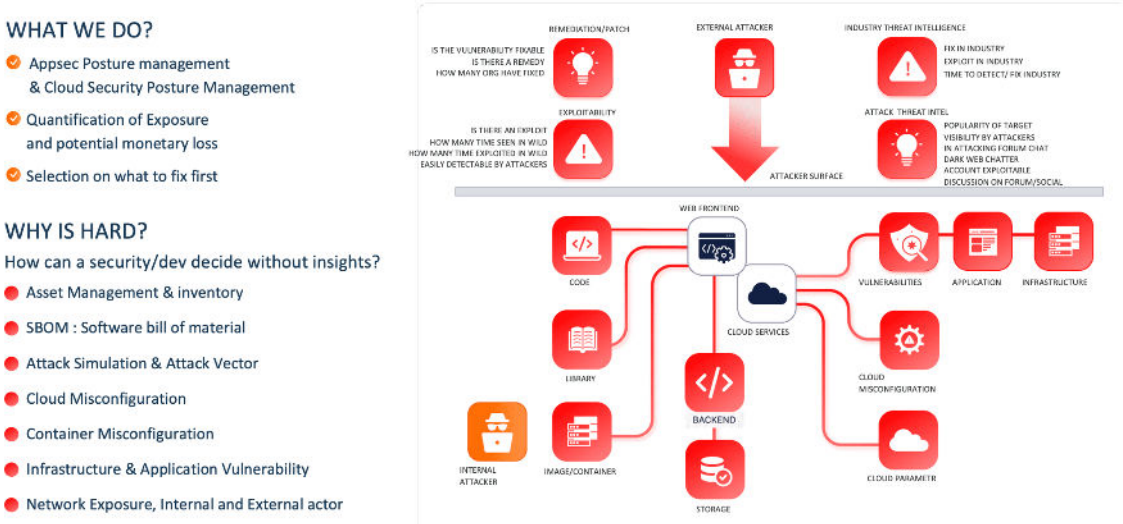
Appsec Phoenix is on a mission to help organizations and security teams move from addressing individual vulnerabilities into consolidated and actionable risk reduction. AppSec Phoenix is a next-generation Security Orchestration and correlation (ASOC) and Risk View System allowing organizations to manage IT security operations in a data-driven/risk-based way.

Appsec Phoenix supports Vuln Management program execution with technology that provides both high-level overview and low-level insights on what to focus on and aids security professionals to set appropriate and achievable priorities. Our solution properly coordinates vulnerability scanning activities with threat intelligence and synthesizes data into a structured information system, ensuring that a Vuln Management program is accountable and stays on track.

The Phoenix system provides Application & Cloud Security Posture Management (ASPM), Application Tooling Orchestration (ASTO), and prioritization at scale leveraging up to 15 data sources.



Any good Vuln Management program needs to have executive sponsorship and a consistent feedback loop to enable executive risk/data-based decision-making that are in line with the risk management goals of the organization.



ACT now on vulnerability get a demo at
https://appsecphoenix.com/request-a-demo/

[7. Conclusion

While companies engage in digital transformation for competitive advantage, it comes with the cost of increased risk. The number and costs of cyber-breaches are on the rise, and a talent shortage is putting pressure on organizations to optimize the efficiency of their cybersecurity operations while maintaining bulletproof assurances.

Both the enterprise IT infrastructure and cyber-threat environment are complex and highly dynamic, making continuous assessments of new vulnerabilities a high-stakes game with potentially devastating consequences. A system that supports visibility across an enterprise by intelligently contextualizing risk on the fly across an organization is a big benefit for vulnerability prioritization. An automated platform offers advantages by offloading the most arduous tasks of enriching CTI and applying it contextually to an organization’s infrastructure of systems and information to prioritize vulnerabilities strategically with risk scores adjusted to real-time.

Risk Calculating real-time contextual insight above and beyond traditional risk management allows the optimized data-driven decision-making and strategic prioritization that can account for relationships between complex business operations, IT infrastructure, and the cyber-threat landscape. Contextual risk scores are calculated using a set of inputs that include the vulnerability's severity, how important the asset is to business operations, the assets locality, and the probability of exploitation, providing a holistic risk assessment for prioritization and optimal application of resources and allowing human IT security personnel to spend less time enriching vulnerability metadata to determine potential risk and more time on remediation activities that increase overall network security.

AppSec Phoenix provides a robust data-driven scalable platform that manages the aggregation, contextualization, and quantification and ultimately allows the strategic prioritization critical to modern vulnerability management and, ultimately risk remediation and high-degree assurances.

[8. References

[1] McKinsey Digital - Managing tech transformations
https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/managing%20tech%20transformations/managing-tech-transformations.pdf

[2] CISA - COST OF A CYBER INCIDENT: SYSTEMATIC REVIEW AND CROSS-VALIDATION
https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf

[3] IBM - How much does a data breach cost in 2022?
https://www.ibm.com/security/data-breach

[4] INC.com 60 Percent of Companies Fail in 6 Months Because of This (It's Not What You Think)
https://www.inc.com/thomas-koulopoulos/the-biggest-risk-to-your-business-cant-be-eliminated-heres-how-you-can-survive-i.html

[5] SANS - Understanding the (True) Cost of Endpoint Management
https://www.sans.org/media/analyst-program/Custom-Survey-Understanding-the-True-Cost-of-Endpoint-Management.pdf

[6] Fortinet - 2022 Cybersecurity Skills Gap: Global Research Report
https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf

[7] Gartner - Improve IT Security with Vulnerability Management, Gartner ID Number: G00127481, May 2005

[8] - Capgemini Consulting & MIT Sload - The Digital Advantage: How digital leaders outperform their peers in every industry
https://www.capgemini.com/wp-content/uploads/2017/07/The_Digital_Advantage__How_Digital_Leaders_Outperform_their_Peers_in_Every_Industry.pdf

[9] NIST - Cybersecurity Framework
https://www.nist.gov/cyberframework

[10] International Standards Organization - ISO/IEC 27000:2018 Information technology security techniques
https://www.iso.org/standard/73906.html

[11] ISACA - COBIT 5 Framework
https://www.isaca.org/resources/cobit/cobit-5

[12] CERT Resilience Management Model (CERT-RMM) Version 1.2
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084

[13] Center for Internet Security Critical Security Controls
https://www.cisecurity.org/controls

[14] ENISA - Cyber Threat Intelligence Overview
www.enisa.europa.eu/publications/cyberthreat-intelligence-overview/at_download/fullReport

[15] MITRE - Common Vulnerability Enumeration System
https://cve.mitre.org/

[16] MITRE - Common Weakness Enumeration System
https://cwe.mitre.org/

[17] The EPSS Model
https://www.first.org/epss/model

[18] CISA - Cybersecurity Infrastructure Security Agency
https://www.cisa.gov/

[19] National Institute of Science and Technology
https://www.nist.gov/

[20] SANS (System Administration, Networking, and Security)
https://www.sans.org/

[21] Veronis - YARA Rules Guide: Learning this Malware Research Tool
https://www.varonis.com/blog/yara-rules

[22] MITRE - Common Platform Enumeration System
https://cpe.mitre.org/specification/

[23] First - Common Vulnerability Scoring System
https://www.first.org/cvss/

[24] FIRST - EPSS User-Guide
https://www.first.org/epss/user-guide

[25] Association for Computing Machinery - Exploit Prediction Scoring System (EPSS)
https://dl.acm.org/doi/fullHtml/10.1145/3436242

[26] McKinsey & Company - Perspectives on transforming cybersecurity
https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx

[27] Deloitte - Reshaping the cybersecurity landscape
https://www2.deloitte.com/content/dam/Deloitte/pt/Documents/risk/Cybersecurity.pdf

[28] FAIR Institute - FAIR Risk Management
https://www.fairinstitute.org/fair-risk-management

APPSEC PHOENIX

ACT today on vulnerabilities
ACT today on RISK

ACT today with AppSec Phoenix

info@appsecphoenix.com
www.appsecphoenix.com
+442031953879