TEAM LEADER- PALLA BEAUTY GRACE

TEAM ID- LTVIP2023TMID03380

TOPIC- Network TRAFFIC ANALYSIS

NETWORK TRAFFIC ANALYSIS

- INTRODUCTION

Information gathering, or data collection, is a process where you follow a series of steps to conduct research and answer questions or resolve problems you have. Though information gathering isn't bound by cybersecurity, it is an essential skill to have in the field.

Regardless of where you are in your career, but even more so if you work in cybersecurity, you're likely to have attempted to gather data at some point.Usually, people conduct research to gather information to:

O Answer one or more questions they have

O Find a solution to a problem

O Reach a decision based on informed data and insights

O Uncover new angles to a problem

O Uncover a topic for debate or conversation

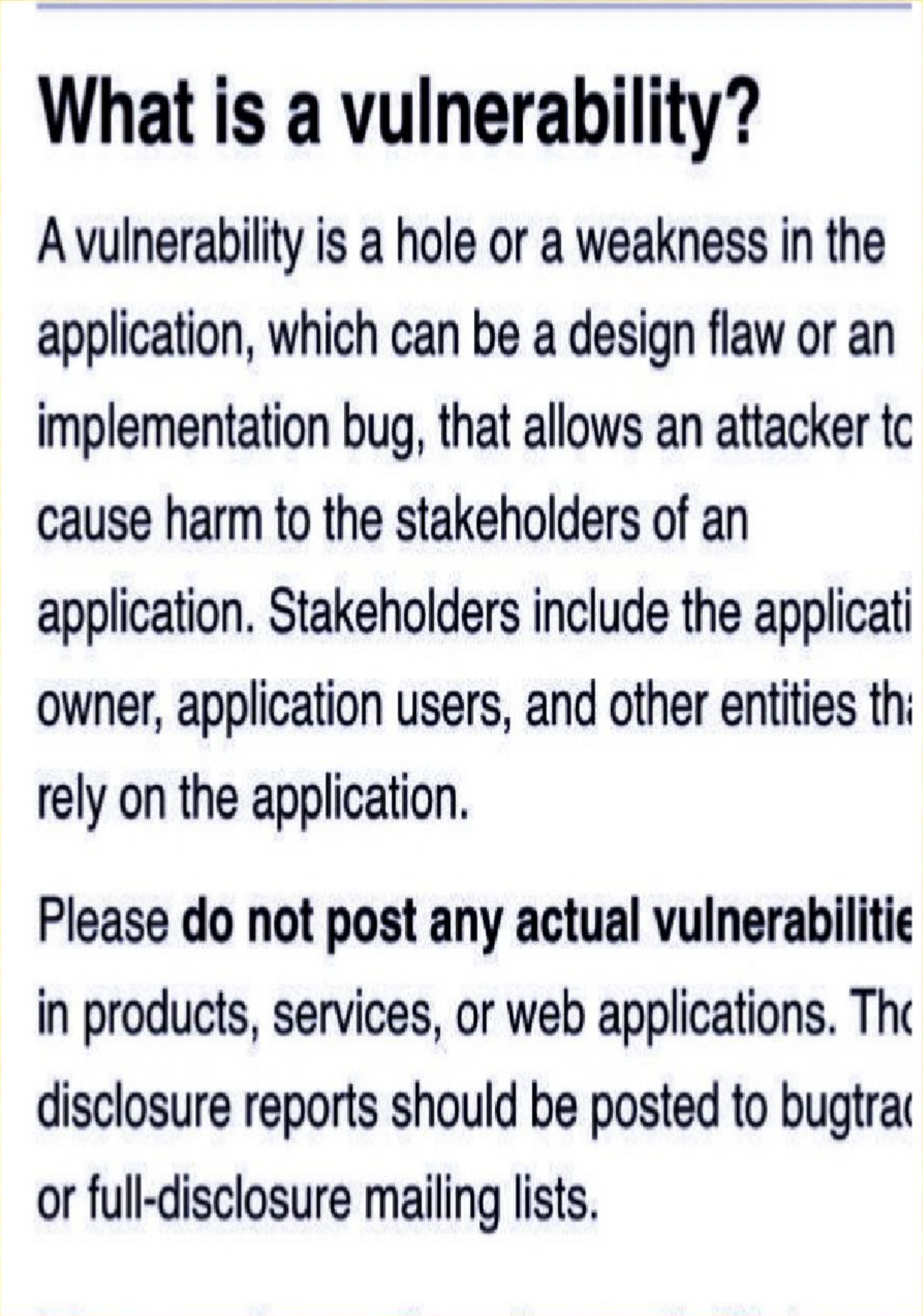
O Learn a specific skill or concept

O Find an online course

There are many other reasons why an individual would seek to gather data.In cybersecurity, the information gathering process is a crucial one because it helps you uncover information that may otherwise have been unknown to you.For example, by gathering and collecting data, you can learn more about securing business networks and reducing the potential of unauthorized access to your company's network.

- LITERATURE SURVEY

https://www.researchgate.net/publication/357393481_A_Systematic_Literature_Review_on_the_Cyber_Security



What is a vulnerability?

A vulnerability is a hole or a weakness in the application, which can be a design flaw or an implementation bug, that allows an attacker to cause harm to the stakeholders of an application. Stakeholders include the applicati owner, application users, and other entities tha rely on the application.

Please **do not post any actual vulnerabilitie** in products, services, or web applications. Tho disclosure reports should be posted to bugtrac or full-disclosure mailing lists.

VULNERABILITY IDENTIFICATION

https://owasp.org/www-community/vulnerabilities/

Examples of vulnerabilities

Lack of input validaion on user input

Lack of sufficient logging mechanism

Fail-open error handling

Not closing the database connection properly

For a great overview, check out the OWASP Top Ten Project. You can read about the top vulnerabilities and download a paper that covers them in detail. Many organizations and agencies use the Top Ten as a way of creating awareness about application security.NOTE: Before you add a vulnerability, please search and make sure there isn't an equivalent one already. You may want to consider creating a redirect if the topic is the same. Every vulnerability article has a defined structure.

COMMON WEAKNESS ENUMERATION

Are you wondering about CWE? We explain CWE (Common Weakness Enumeration) and why this community-based initiative is essential in cybersecuritycybersecurity

Common Weakness Enumeration (CWE) is a system to categorize software and hardware security flaws—implementation defects that can lead to vulnerabilities. It is a community project to understand security weaknesses or errors in code and vulnerabilities and create tools to help prevent them.

The MITRE Corporation operates CWE, and the National Cyber Security Division and US-CERT support it. CWE has over 600 categories detailing different types of vulnerabilities and bugs.

CWE strives to stop vulnerabilities and bugs by educating developers on building better products that aren't susceptible to exploitation. Programmers can use CWE as a resource while writing code to prevent vulnerabilities during the development process. Security Orchestration, Automation, and Response (SOAR) tools use CWEs to build policies and workflows to automate remediation.

The 2022 CWE Top 25 includes:

CWE-787 - out-of-bounds writing. Severity score: 64.20

CWE-79 - improperly neutralizing input when generating web pages (cross-site scripting). Severity score: 45.97.

CWE-89 - improperly neutralizing special elements in SQL commands (SQL injection). Severity score: 22.11

CWE-20 - improperly validating input. Severity score: 20.63.

CWE-125 - out-of-bounds reading. Severity score: 17.67.

CWE-78 - improperly neutralizing special elements in operating system commands (OS command injection). Severity score: 17.53.

CWE-416 - using after free. Severity score: 15.50.

CWE-22 - improperly limiting pathnames to restricted directories (path traversal). Severity score: 14.08.

CWE-352 - cross-site request forgery (CSRF). Severity score: 11.53.

CWE-434 - unrestricted uploading of files with dangerous type. Severity score: 9.56.

CWE-476 - NULL pointer dereferencing. Severity score: 7.15.

CWE-502 - deserializing untrusted data. Severity score: 6.68.

CWE-190 - integer overflow or wraparound. Severity score: 6.53.

CWE-287 - improper authentication. Severity score: 6.35.

CWE-798 - using hard-coded credentials. Severity score: 5.66.

CWE-862 - missing authorization. Severity score: 5.53.

CWE-77 - improperly neutralizing special elements in commands (command injection). Severity score: 5.42.

CWE-306 - missing authentication for critical functions. Severity score: 5.15.

CWE-119 - improperly restricting operations in memory buffers. Severity score: 4.85.

CWE-276 - incorrect default permissions. Severity score: 4.84

CWE-918 - server-side request forgery (SSRF). Severity score: 4.27.

CWE-362 - concurrent execution with shared resources and improper synchronization (race condition). Severity score: 3.57.

CWE-400 - uncontrolled resource consumption. Severity score: 3.56.

CWE-611 - improperly restricting XML external entity references. Severity score: 3.38.

CWE-94 - improper control of code generation (code injection). Severity score: 3.32.

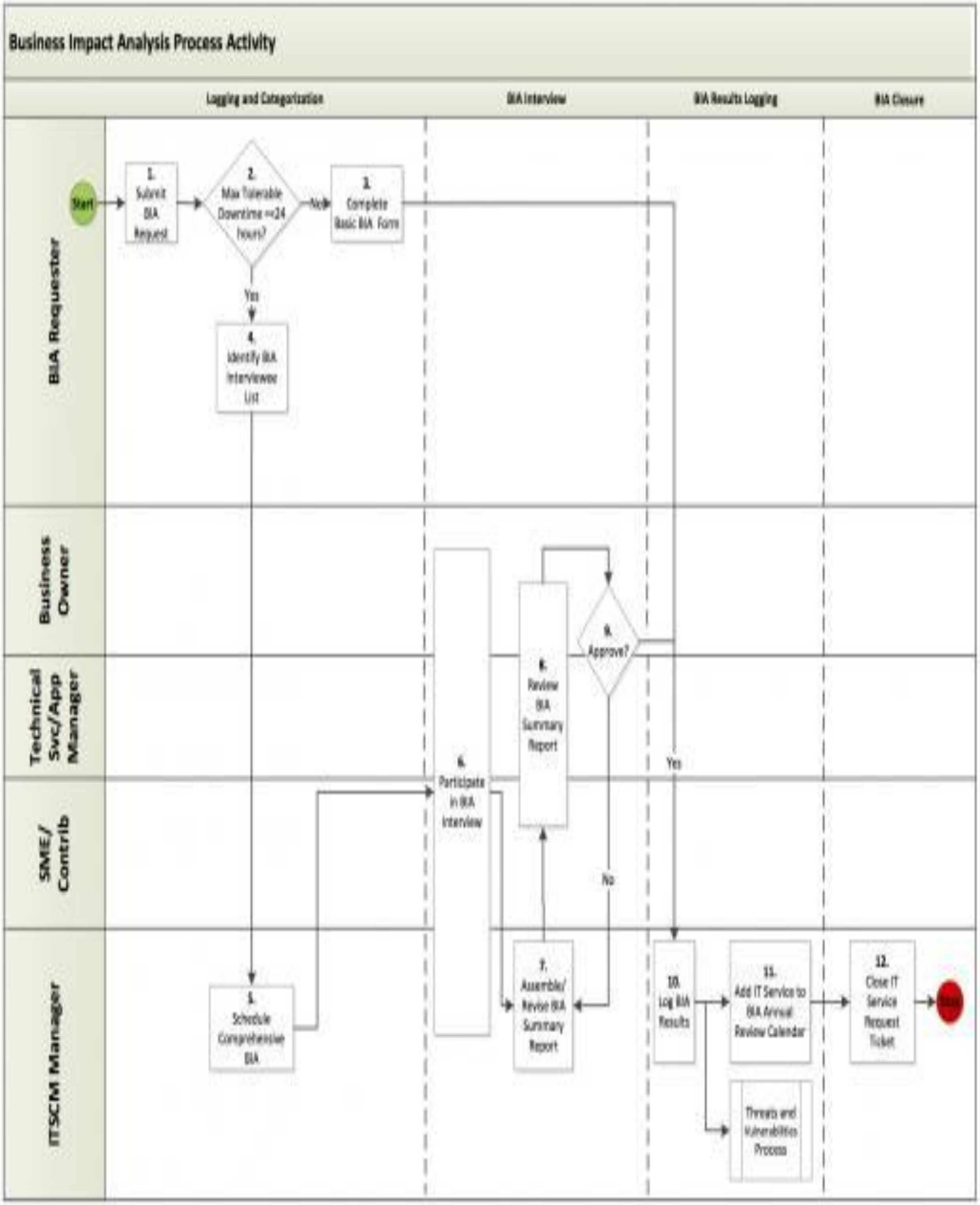
BUSINESS IMPACT ASSESSMENT

- A business impact analysis (BIA) is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency. A BIA is an essential component of an organization's business continuity plan (BCP).

- Business Impact Analysis (BIA)
- The UCSF Business Impact Analysis (BIA) process identifies and evaluates the potential effects (financial, life/safety, regulatory, legal/contractual, reputational and so forth) of natural and man-made events or disasters on business operations. The information is quantified and analyzed and reported to executives to meet regulatory diligence, compliance requirements, and as an input to

disaster recovery solution planning. This is a broad brush approach to seeing the risk at a high level.

-


Business Impact Analysis Process Activity
Logging and Categorization
BIA Interview
BIA Results Logging
BIA Closure
BIA Requester
Business Owner
Technical Svc/App Manager
SME/ Contrib
ITSCM Manager
Start
1. Submit BIA Request
2. Max Tolerable Downtime <=24 hours?
No
Yes
3. Complete Basic BIA Form
4. Identify BIA Interviewee List
5. Schedule Comprehensive BIA
6. Participate in BIA Interview
7. Assemble/ Revise BIA Summary Report
8. Review BIA Summary Report
9. Approve?
Yes
No
10. Log BIA Results
11. Add IT Service to BIA Annual Review Calendar
Threats and Vulnerabilities Process
12. Close IT Service Request Ticket
End

Business Impact Analysis (BIA)

The UCSF Business Impact Analysis (BIA) process identifies and evaluates the potential effects (financial, life/safety, regulatory, legal/contractual, reputational and so forth) of natural and man-made events or disasters on business operations. The information is quantified and analyzed and reported to executives to meet regulatory diligence, compliance requirements, and as an input to disaster recovery solution planning. This is a broad brush approach to seeing the risk at a high level.

Business Impact Analysis Process

Frequently Asked Questions (FAQs):

What is a BIA?

BIA versus Risk Assessment

How do I know if a Business Impact Analysis (BIA) is required?

What should I expect during the BIA Process?

Who should attend the BIA interview?

What are the types of BIA?

What type of BIA will I need?

What are the BIA Interview questions?

What is the information in the BIA used for?

What are the application Tiers?

When will I see the BIA results?

How do I access my BIA Summary Report?

How often will BIAs be reviewed?

What is a BIA?

A business impact analysis (BIA) is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency. A BIA is an essential component of an organization's business continuance plan; it includes an exploratory component to reveal any vulnerabilities and a planning component to

develop strategies for minimizing risk. The result is a business impact analysis report, which describes the potential risks specific to the organization studied. One of the basic assumptions behind BIA is that every component of the organization is reliant upon the continued functioning of every other component, but that some are more crucial than others and require a greater allocation of funds in the wake of a disaster. For example, UCSF may be able to continue more or less normally if one of the cafes on campus has to close, but would come to a complete halt if the information systems crash.

As part of a disaster recovery plan, a BIA is likely to identify costs linked to failures, such as loss of cash flow, replacement of equipment, salaries paid to catch up with a backlog of work, loss of profits, staff and data, and so on. A BIA report quantifies the importance of business components and may suggest appropriate fund allocation for measures to protect them. The possibilities of failures are likely to be assessed in terms of their impacts in areas such as safety, finances, marketing, business reputation, legal compliance and quality assurance and in this case IT resiliency. Where possible, impact is expressed monetarily for purposes of comparison. For example, UCSF may spend three times as much on recruiting potential students, faculty and staff in the wake of a disaster to rebuild customer confidence. The BIA should assess a disaster's impact over time and help to establish recovery strategies, priorities, and requirements for resources and time.

BIA versus Risk Assessment

Business impact analysis and risk assessment are two important steps in a business continuity plan. A BIA often takes place prior to a risk assessment. In particular UC San Francisco's IT Business Continuity Team will focus its BIA efforts on the effects or consequences of the interruption to critical IT business functions and attempts to quantify the financial and non-financial costs associated with a disaster. The business impact assessment looks at the parts of the organization that are most crucial. A BIA can serve as a starting point for a disaster recovery strategy and examine recovery time objectives (RTOs) and recovery point objectives (RPOs), and resources and materials needed for business continuance.

A risk assessment identifies potential hazards such as a hurricane, earthquake, fire, supplier failure, utility outage, IT or network availability or cyber-attack and evaluates areas of vulnerability should the hazard occurs. Assets put at risk include people, property, supply chain, information technology, business reputation and contract obligations. Points of weakness that make an asset more prone to harm are reviewed. A mitigation strategy may be developed to reduce the probability that a hazard will have a significant impact.

During the risk assessment phase, the BIA findings may be examined against various hazard scenarios, and potential disruptions may be prioritized based on the hazard's probability and the likelihood of adverse impact to business operations. A BIA may be used to justify investments in prevention and mitigation, as well as disaster recovery strategies.

UCSF has a department that manages continuity for the campus (Office of Emergency Management – OEM) who are conducting separate BIAs and risk assessments for the business side of our campus. You may be in contact with OEM regarding the UCReady project or wish to contact OEM for more information. The IT Business Continuity Team specializes in IT resiliency and thus a BIA conducted by IT Business Continuity will focus on IT assets owned or managed by the interviewee.

How do I know if a Business Impact Analysis (BIA) is required?

To determine if a BIA is required, please complete the Business Impact Analysis Request Form (must have MyAccess Account):

Go to URL: http://Help.ucsf.edu

Select 'Request Specific Services'

Select 'Consulting & Development'

Login with your MyAccess Account

Select 'Business Impact Analysis Request' form

Complete all necessary fields and click the 'Submit' button

What is should I expect during the BIA process?

A BIA is generally a multi-phase process that includes the following steps (with possible follow-up interviews):

- Gathering information via both survey and in-person interviews
- Evaluating the collected information
- Preparing a report to document the findings
- Presenting the results to the interviewee
- Potentially saving the information in UCSF's BIA repository, BC Catalyst

The information gathered may include participation by the functional owner of the data or system/application, subject matter experts and technical IT managers. A description of the principle activities that the business units perform, subjective rankings of the importance of specific processes, names or organizations that depend on the processes for normal operations, estimates of the quantitative impact associated with a specific business function and the non-financial impact of the loss of the function, critical information systems and their users, the staff members needed to recover important systems, and the time and steps required for a business unit to recover to a normal working state may be parts of the information gathered during an IT BIA.

Questions to explore during the discovery phase include interdependencies between systems, business processes and departments, the significance of the risk of points of failure, responsibilities associated with service-level agreements, staff and space that may be required at a recovery site, special supplies or communication equipment needed, and cash management and liquidity necessary for recovery.

A BIA for information technology might start with the identification of applications supporting essential business functions, interdependencies between existing systems, possible failure points, and costs associated with the system failure. The analysis phase examines the risks and prioritizes uptime requirements and RTO and RPO.

When information gathering is complete, the review phase begins in consultation with business leaders who can validate the findings. UC San Francisco has implemented a utility, BC Catalyst, that will store the information gathered in the BIA and will be used to track changes to the systems and applications that were identified as time-sensitive/critical. An annual review of the BIA in Catalyst ensures that the information is kept up to date and changes to the BIA can be tracked and made available for senior management and planning purposes.

The goals of the BIA analysis (and by storing in Catalyst) are to determine the most crucial business functions and systems, the staff and technology resources needed for operations to run optimally, and the time frame within which the functions need to be recovered for the organization to restore operations as close as possible to a normal working state.

VULNERABILITY PATH AND PARAMETER IDENTIFICATION

- Vulnerability identification is an integral part of vulnerability assessments, helping you understand the risks to your systems, assets, data and people, whether that is compromised credentials or unpatched applications.
- A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.

- Imperva
- Login
- Why Imperva
- Products
- Solutions
- Support
- Partners
- Customers
- Resources
- Company
-
- Vulnerability Assessment
- 124.2k views
- App Security
- Essentials
- What is vulnerability assessment
- A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.
-
- Examples of threats that can be prevented by vulnerability assessment include:
-
- SQL injection, XSS and other code injection attacks.
- Escalation of privileges due to faulty authentication mechanisms.
- Insecure defaults – software that ships with insecure settings, such as a guessable admin passwords.
- There are several types of vulnerability assessments. These include:
-

- Host assessment – The assessment of critical servers, which may be vulnerable to attacks if not adequately tested or not generated from a tested machine image.
- Network and wireless assessment – The assessment of policies and practices to prevent unauthorized access to private or public networks and network-accessible resources.
- Database assessment – The assessment of databases or big data systems for vulnerabilities and misconfigurations, identifying rogue databases or insecure dev/test environments, and classifying sensitive data across an organization's infrastructure.
- Application scans – The identifying of security vulnerabilities in web applications and their source code by automated scans on the front-end or static/dynamic analysis of source code.
- This is part of an extensive series of guides about [data security]
-
- Vulnerability assessment: Security scanning process
- The security scanning process consists of four steps: testing, analysis, assessment and remediation.
-
- The vulnerability assessment process: analysis, risk assessment, remediation
-
- *1. Vulnerability identification (testing)*
- The objective of this step is to draft a comprehensive list of an application's vulnerabilities. Security analysts test the security health of applications, servers or other systems by scanning them with automated tools, or testing and evaluating them manually. Analysts also rely on vulnerability databases, vendor vulnerability announcements, asset management systems and threat intelligence feeds to identify security weaknesses.
-
- *2. Vulnerability analysis*

- The objective of this step is to identify the source and root cause of the vulnerabilities identified in step one.
-
- It involves the identification of system components responsible for each vulnerability, and the root cause of the vulnerability. For example, the root cause of a vulnerability could be an old version of an open source library. This provides a clear path for remediation – upgrading the library.
-
- *3. Risk assessment*
- The objective of this step is the prioritizing of vulnerabilities. It involves security analysts assigning a rank or severity score to each vulnerability, based on such factors as:
-
- Which systems are affected.
- What data is at risk.
- Which business functions are at risk.
- Ease of attack or compromise.
- Severity of an attack.
- Potential damage as a result of the vulnerability.
- *4. Remediation*
- The objective of this step is the closing of security gaps. It's typically a joint effort by security staff, development and operations teams, who determine the most effective path for remediation or mitigation of each vulnerability.
-
- Specific remediation steps might include:
-
- Introduction of new security procedures, measures or tools.
- The updating of operational or configuration changes.
- Development and implementation of a vulnerability patch.
- Vulnerability assessment cannot be a one-off activity. To be effective, organizations must operationalize this process and repeat it at regular

intervals. It is also critical to foster cooperation between security, operation and development teams – a process known as

RESULT

Network traffic analysis can attribute the malicious behavior to a specific IP and also perform forensic analysis to determine how the threat has moved laterally within the organization--and allow you to see what other devices might be infected. This leads to faster response in order to prevent any business impact.

ADVANTAGES

The importance of network traffic analysis and monitoring in your cybersecurity process

What is Network Traffic Analysis (NTA)?

Network traffic analysis (NTA) is a method of monitoring network availability and activity to identify anomalies, including security and operational issues. Common use cases for NTA include:

Collecting a real-time and historical record of what’s happening on your network

Detecting malware such as ransomware activity

Detecting the use of vulnerable protocols and ciphers

Troubleshooting a slow network

Improving internal visibility and eliminating blind spots

Implementing a solution that can continuously monitor network traffic gives you the insight you need to optimize network performance, minimize your attack surface, enhance security.

Benefits of NTA include:

Improved visibility into devices connecting to your network (e.g. IoT devices, healthcare visitors)

Meet compliance requirements

Troubleshoot operational and security issues

Respond to investigations faster with rich detail and additional network context

A key step of setting up NTA is ensuring you’re collecting data from the right sources. Flow data is great if you are looking for traffic volumes and mapping the journey of a network packet from its origin to its destination. This level of information can help detect unauthorized WAN traffic and utilize network resources and

performance, but it can lack rich detail and context to dig into cybersecurity issues.

Packet data extracted from network packets can help network managers understand how users are implementing/operating applications, track usage on WAN links, and monitor for suspicious malware or other security incidents. Deep packet inspection (DPI) tools provide 100% visibility over the network by transforming the raw metadata into a readable format and enabling network and security managers to drill down to the minutest detail.

DISADVANTAGES

Data volume and complexity

One of the biggest challenges of NTA is dealing with the large and complex amount of data that needs to be collected and processed. Depending on the size and architecture of the network, NTA may require terabytes or even petabytes of storage and computing resorces.

APPLICATIONS OF NETWORK TRAFFIC ANALYSIS

Once an NTA solution determines what normal behavior on your network looks like, it can alert your organization when anomalous behavior occurs. By alerting your security team to suspicious activity early on--whether the threat is coming from outside or inside your network--NTA solutions can provide the extended visibility you need to mitigate the security incident.

Network traffic analysis can attribute the malicious behavior to a specific IP and also perform forensic analysis to determine how the threat has moved laterally within the organization--and allow you to see what other devices might be infected. This leads to faster response in order to prevent any business impact.

CONCLUSION

Network traffic analysis is an essential way to monitor network availability and activity to identify anomalies, maximize performance, and keep an eye out for attacks. Alongside log aggregation, UEBA, and endpoint data, network traffic is a core piece of the comprehensive visibility and security analysis to discover threats early and extinguish them fast.

When choosing a NTA solution, consider the current blind spots on your network, the data sources you need information from, and the critical points on the network where they converge for efficient monitoring. With NTA added as a layer to your security information and event management (SIEM) solution, you'll gain visibility into even more of your environment and your users.

FUTURE SCOPE FOR NETWORK TRAFFIC ANALYSIS

People also ask

What is the scope of network traffic analysis?

Network traffic analysis (NTA) is a method of monitoring network availability and activity to identify anomalies, including security and operational issues. Common use cases for NTA include: Collecting a real-time and historical record of what's happening on your network. Detecting malware such as ransomware activity