NETBRAIN TECHNOLOGIES: CONTINUOUS SECURITY AUTOMATION

TABLE OF CONTENTS

APPLYING ADAPTIVE AUTOMATION FOR CONTINUOUS CYBER-SECURITY

You Can't Protect What You Can't See

The traditional approaches to security exhibit limitations that are of an alarming concern. Our entire culture of communication is based on protocols that were engineered without keeping security in mind. Applications with global accessibility are moving rapidly in a variety of different ways. Different application types live on premise or in the cloud potentially forming a variety of diverse traffic patterns. Although, we have modern technologies such as Software-defined networking (SDN), Network Function Virtualization (NFV) and Internet of Things (IoT) the rapid rush to the market unveils pockets for security flaws.

The new groundbreaking technologies are technically remarkable; however, they spawn troubleshooting challenges while navigating through the complexity. You can disregard the complexity but only until it calls for troubleshooting. The cyber threat landscape is evolving rapidly and we are treading towards a new era of both Terabyte and “low and slow” style distributed denial-of-service (DDoS) attacks. The low and slow are hard to detect and Terabyte attacks will bring the most important networks to their knees.

I.T departments are loaded with resource-constrained staff. This has resulted in a dearth of skills to combat DDoS attacks, thereby building a ‘perform storm’ for cyber criminals to conceal identity. Efficient DDoS detection is not limited to state of the art machine algorithms for detection and stateless mitigation technologies. These forms only part of the risk picture and there is a need for an enhanced shield to win the ever-losing battle.

The lack of automation to DDoS troubleshooting is not the righteous way to deal with the situation. Network automation for both the technical troubleshooting and workflow integration is the only way to combat the new era of DDoS. Network automation should comprise all security functions. A holistic approach must be applied to proactively prevent attacks by system hardening as well as arm us with better tools to respond quickly when faced with a threat, especially if it's a ‘day zero threat’ were we have limited knowledge of the correct mitigation technique to employ. Newly data-driven network documentation, automated security assessment and triggered troubleshooting with effective team and workflow collaboration are required.

Today, network automation enables security professionals to enhance agility within the security domain by introducing deterministic and predictable outcomes. This effectively stops DDoS at the network gates. When all troubleshooting events, including human behavior, become predictable, their outcomes enhance all operations of the security domain and corresponding workflows. Adaptive Automation is the missing piece of the DDoS puzzle. It allows teams to effectively troubleshoot attacks, disarm false positives and isolate parts of the network impacted.

The only way to combat today and tomorrow's DDoS is to automate as much as possible. The future of security offers a new stream of thought called Continuous Automation. Continuous Automation will

eventually guide security professionals to a point where networks automatically self-heal from any DDoS event without any human interaction.

THE DDOS LANDSCAPE

Over the last few years, the DDoS landscape has certainly transformed into a terrain that is more prone to attacks. The classic linear attack has transitioned to an attack that occurs from every part of the world, all at once. The attacks have intensified in terms of frequency, size and complexity.

Today's DDoS takes many different types of characteristics. More than likely, they are MultiVector with new additions of invasive low and slow called “snow shoeing” usually below the alarm threshold of detection systems. DDoS is not always about Terabyte volumetric attacks; that are loud and easy to detect. Security leaders are at the end of a shoestring with the ever-changing landscape of DDoS.

INTERNET OF THINGS (IOT) DIVERSE WORKLOADS

IoT brings in an array of normal day objects with the ability to communicate with each other. It will have a tremendous impact on how we live and most certainly upgrade the quality of everyday life in both; smart cities and cars.

The concern around IoT is the lack of standards leading to poorly connected devices with global accessibility. Now launching an attack is as easy as removing the spectacle from the nose. If you have the IP address of a device, you can attack it. This is the foundation and it’s not going to change anytime soon.

There are also concerns about the rising level of data that IoT will transport and how the existing network capacities cope with the surge of data. Another side of IoT that is often overlooked is the sear complexity workflows and the devices that may need to be traversed.

A less security-enabled device may lead to a more significant component. How would you troubleshoot and manage this level of complexity manually? You simply can’t.

THE CHALLENGES OF NEW TECHNOLOGIES

Escalated competition drives companies to adopt new technologies, potentially opening pockets of security holes. More than often, new technologies split opens the gateway for new vulnerabilities as security policies are often an afterthought.

Cybersecurity policies address risks of all areas of I.T. Their policies and procedures must adapt and support changes in new technologies. These changes must be streamlined and automated as much as possible.

New technologies introduce a loss of network visibility. We now have an array of SDN, NFV, containers and virtual machines. Tracking activity and troubleshooting these technologies require new methodologies that are generally in the minds of the engineer.

DIVERSE TRAFFIC FLOWS

Traffic flows are now skating in every possible direction. There has been a transition from the monolithic single application per server to a tier application approach with a diverse traffic pattern. Most of the traffic for the new style of application is predominantly a mesh of east to west. Traditional troubleshooting methods are used to superintend north to south traffic flows.

So, what are some of the validated architectures that put you in the best position to protect your network against all these changes?

GUIDELINES FOR EFFECTIVE SECURITY

Until recently, there was a scantiness of appropriate guidelines for the masterful security. However, after extensive research and experience, here are a set of guidelines that would empower you to layout well organized network designs and implement improvements to protect the network more adequately; putting security professionals in a better position to combat a DDoS event.

From an implementation point of view key areas such as Secure Shell (SSH) or Telnet, Exec Timeouts, Password encryption are recommended as security yardstick. From a design perspective architects should decentralize Internet connectivity by engaging a layered approach to Internet connectivity. Instead of retaining Internet access solely in a central hub it should be decentralized to individual branch sites.

Others may choose to have secondary Domain Name System (DNS) servers on a redundant Content Delivery Network (CDN) Anycast network. However, decentralization and outsourcing to CDN Provider changes the traditional security paradigm which may be met with hesitation. They come at a high cost, coupled with long lead times both from the design and new Internet link connectivity perspective.

Recommended designs offer validated architectures and implementation of golden rules render best practices to guide the administrator but unfortunately, they don't solve the unsolved challenges to effectively stop a DDoS on its track.

UNSOLVED CHALLENGES TO STOP DDOS

The following unsolved challenges for effective DDoS troubleshooting are prevalent at all stages - Before, During and After a DDoS event.

LACK OF REAL-TIME NETWORK VISIBILITY

GROWING TRAFFIC VOLUMES

The amount of network traffic is mushrooming multifold and will continue to mount at an unprecedented level due to the introduction of billions of IoT devices ranging from light bulbs to smart cars. However, while the level of network traffic soars, the level of visibility into network traffic is decreasing because of the presentation of new styles of applications and technologies.

Having adequate network visibility is the most important tool to understand network behaviour in order to be acutely aware of how traffic is flowing. There is a common saying that the most important aspect of security is to *“know thy traffic.”*

The granularity of network visibility depends on how much and the type of data you collect additionally, followed by how this is aggregated and visually presented to the user. It's not just limited to the application of traffic profiling. The administrator must have adequate visibility into the network topology and should have the ability to drill down to infinite detail on any device and at any site within seconds. Essentially, network visibility provides accurate information about the present state of the network from both the traffic and diagrammatic point of view. This leads to better business decisions for faster DDoS troubleshooting.

Today's visibility is primarily achieved through the command line interface (CLI). Networking is not just about connecting two devices anymore. Network complexity has grown to multiple devices including a variety of traffic types. The CLI has a very deep field of view but it is too narrow to support the complexity of today's networks. The box-by-box mentality limits the ability to visualize anything end-to-end and restricts the administrator’s view to one particular area of the network.

Traditional methods for network visibility don’t work anymore. Effective DDoS troubleshooting requires end-to-end “real-time” detailed network visualization. You can't protect what you can't see, so if it's not end-to-end, you are severely limiting the success of troubleshooting.

VISIBILITY & DOCUMENTATION IS CRITICAL TO COMBAT DDOS

Visibility and documentation plays an essential role in combating DDoS attacks. You will not be able to safeguard your network unless you notice an attack rocketing towards your network. Similarly, documentation acts as an effective architect for the engineers since it summarizes the DDoS. NetBrain provides precise visibility into areas of the network that are under attack. This type of visibility leads to better troubleshooting, equipping you with stronger risk management while undergoing a DDoS event.

WHAT DOES END-TO-END VISIBILITY LOOK LIKE?

Even if you have the up-to-date documentation for every site in your network, that only gives you basic topology references. Visibility is not just about basic topology information. Security professionals require application flow, design, performance and historic information.

Visibility must be end-to-end, from one network point to the other i.e. from attack entry to the unfortunate victim. Administrators cannot adequately manage a DDoS unless they have access to full end-to-end visibility. This type of network detail facilitates quick identification of security threats.

The ability to drill down into specific areas of the network with infinite details enables security professionals to monitor security threats proactively and take informed decisions at the time of the attack.

GENERATIONS OF NETWORK VISIBILITY

Traditionally, Generation 1 visibility is carried out using simple network discovery with SNMP (Simple Network Management Protocol) that is useful for Asset and Inventory reports. SNMP furnishes the same accuracy and detailed information that it fetched the last time when it was polled.

If the documentation is not up to date you will not have adequate network visibility. An alarming 95% of enterprises still rely on this type of static diagrammatic form for visibility. Although, it is not very efficient for DDoS troubleshooting, arriving at all angles and directions.

INADEQUACIES TO NETWORK DOCUMENTATION

Creating and maintaining accurate network documentation is the key for efficient troubleshooting. It may sound like a simple task but most network documentation is stagnant and out of date. Traditional network diagramming is manual and time-consuming. It is broken down into two phases: data collection and drawing that are not tightly coupled and automated.

The current mechanism is not just about pulling data with SNMP. There is a great deal of ephemeral and static information inside a device that SNMP alone cannot extract. The ideal method gathers data inside the devices such as real-time routes, MAC address, ACL etc. Generation 3 provides a real-time, up-to-date, adaptive and dynamic solution by simulating an engineer using CLI commands to extract required data instantly from thousands of devices in an automated fashion.

Networking is dynamic with traffic flowing in all directions. The documentation of the network should also be robust with the ability to instantly map asymmetric flows. Documentation should adequately represent the network from the architectural point of view and should also include Layer 1 to Layer 7 details in a single pane of glass that is easy to view in order to make informed decisions between multiple teams.

LIMITATIONS TO NETWORK AUTOMATION

Most of the traditional network automation is based on custom scripts. Custom scripts are useful for one off temporary workaround jobs but questionable for both manageability and trackability. They lack portability and do not correspond well with the human intervention to write as well as run and manage.

A more advanced type of automation is required; a kind of automation that is data-driven, dynamically created, simplified and adaptive to current and future conditions. We need a better solution than the homegrown scripts to support the Art of Networking.

THE ART OF NETWORKING

You will never see two identical networks. Even if they provide the same service, every network will have unique designs, product vendors and configuration templates. The products offered by vendors are merely the building blocks for smart engineers to develop the design of a network. The decision for formulating a design that is in the mind of the engineer, results in millions of unique snowflakes, causing an array of troubleshooting steps.

INADEQUATE TROUBLESHOOTING

THE ART OF TROUBLESHOOTING

Troubleshooting is an individual specific art consisting of techniques that are personalized and developed over time due to the on-the-job experience. Traditionally, troubleshooting is carried out with the command-line user interface (CLI). There is no structure to the text returned from the CLI command and it's difficult to extract when you want to correlate the errors from the neighboring devices. Troubleshooting a DDoS solely with CLI is an uphill struggle and an automated approach is needed to effectively enhance the before, during and after stages of a DDoS event.

THE NEED FOR A SCIENCE

Without automation, the troubleshooting behavior of humans is unpredictable. Troubleshooting a DDoS should not be left to an individual's preference, especially when the security professionals are leaving companies at an alarming rate. The science of troubleshooting and knowledge gained from the former engineers should be centralized and updated with the lessons learned. It is only with this type of collaboration that one can devise the most efficient troubleshooting steps to stop a DDoS on time. Pre-rehearsed automated approach to DDoS plan eradicates the panic button.

SHORTAGE OF SKILLED SECURITY STAFF

There is a dearth of skilled security staff available to cope with the latest security concerns. The ISACA cybersecurity report states that over 85% of business leaders feel that we are in a labor crisis of skilled cybersecurity workers. Therefore, we ought to empower the more junior workforce with the knowledge from the more senior and limited workforce.

THE STRUGGLE FOR EFFECTIVE TEAM COLLABORATION

The majority of teams combating a DDoS attack should more than likely be distributed. You could have different detection and mitigation suppliers or managerial parts of the network outsourced to 3rd Party.

To align a high performing team to efficiently troubleshoot a DDoS attack usually consists of different technical skills, multiple locations, time zones and cultures. There will be a variety of people involved to troubleshoot and solve a problem in a short period. Every individual's efforts must be coordinated efficiently while under extreme pressure from financial loss and negative branding of Loss of Service.

DDoS is a complicated collaboration effort that consists of emerging tools and practices along with cross-cultural leadership. Operating within a global team environment may increase the complexity that acts as a barrier for efficient DDoS protection.

INADEQUATE NETWORK HARDENING/SECURITY CHECKLISTS

Reacting quickly is one thing but being proactive with network hardening and security checklist is just as important. How secure is your network? The most accurate way to find out is to simulate an attack but not all attacks can be simulated and the future threat patterns are unknown.

The prime objective is to understand the entire network’s exposure. For this, the security professionals must run an assessment since it offers a level of understanding of how the network is positioned in terms of hardening.

A good assessment is not a once off task. It must be adopted and refined over time to form a complete testing model. It must be updated with the lessons learned and improved efficiency over time. This type of hardening provides network integrity by ensuring that the configuration and design adhere to the “golden rules” of security. However, there is so much effort involved in network hardening, multiple devices, configuration parameters and design reviews.

The problem is that there is a lot of bulk scanning and network reconnaissance that is hard to execute the manual way. It's not just about finding vulnerabilities in ports and message types; it's a complex operation that NetBrain can automate systematically. More than often the manual approach is too time-consuming and resource intensive. Engineers often get stuck in the weeds and the necessary steps are missed.

“NETBRAIN: KNOW THY TRAFFIC”

Security professionals must examine all aspects of security, all at once and view results in one place. To combat today's DDoS attacks requires a holistic view of the entire security operation.

There is limited privilege-having a skilled task force if there is poor team collaboration. Similarly, the advantage is restricted if you have the most efficient network design but the network documentation does not match with what's actually on the network.

To resolve and combine all the unsolved elements into a comprehensive and effective DDoS solution, one must incorporate network automation with both the technical and workflow perspective. There are different types of automation for different activities. Some use automation just for the configuration management without any integration with the other aspects of I.T operations.

NetBrain offers a solution to automation that fills the security gaps and combats the-unsolved DDoS protection mysteries. It's only when you look at these elements holistically can you adequately protect yourself from the today and the unknown threats of tomorrow.

APPLYING AUTOMATION TO SECURITY WORKFLOW

Network automation is essentially about carrying out activities swiftly and efficiently. The activity depends on the type of automation you are undertaking. It's not just about CLI automation since there are different levels of automation depending on the organization’s maturity level.

Automation is not merely restricted to a singular set of technical tasks compiled together. It is multilevel and touches many elements and workflows within an I.T department. You can automate network hardening, compliance checks, documentation and triggered troubleshooting.

It is an integral part for business agility and should be engrained in culture from day 1. Network automation does not remove humans from network operations; it just removes their direct control, thereby improving the overall efficiency. Network devices have a tremendous amount of information stored in

them. But unless the efficient data collection methods are combined with automation, much of this static and ephemeral data remains locked inside, which is more or less unproductive for the engineer. Retrieving data quickly from network devices in an automated way is more practical than a manual approach to troubleshooting a DDoS attack.

Once you have real-time device data, you don't need to carry out any manual parsing with complicated regular expressions. This saves time and obviously money when you are going through network downtime. Network automation provides deterministic outcomes and procedures to troubleshoot any type of DDoS attack effectively.

NETBRAIN ADAPTIVE AUTOMATION PLATFORM

INTEGRATE WITH EXISTING SECURITY WORKFLOWS: PROTECT, ISOLATE AND MITIGATE

NetBrains ambition is to integrate into a team's existing workflow during the Protect, Isolate, and Mitigate stages of a DDoS attack. The initial workflow is to Protect and in the event of an attack to Isolate and Mitigate.

Firstly, the data mapping techniques can map the network in the blink of an eye and through various Application Programming Interface (API) integration points visualize any data on that Map within a single pane of glass. Secondly, the data on the map helps the teams in collaborating more seamlessly with one Map Uniform Resource Locator (URL). Teams can be either internal or external as everything is collaborated and tracked at one location.

NetBrain has the ability for external events to trigger map creation, enabling the perfect use case to combat any type of DDoS automatically with minimal human intervention. Executable Runbooks make any workflow and task executable. They enable a new standard of security by codifying knowledge and the ability automates the security checklists. Runbooks enable consistent network hardening and security checklists to the highest possible level.

NetBrain solution fills the critical gaps of visibility, collaboration and automation. Through various API integration points, it protects the network at every angle from the latest security threats lurking on the DDoS landscape. The power of automation manifests with every second count.

COMBINING HUMAN AND EVENT DRIVEN ACTIVITIES

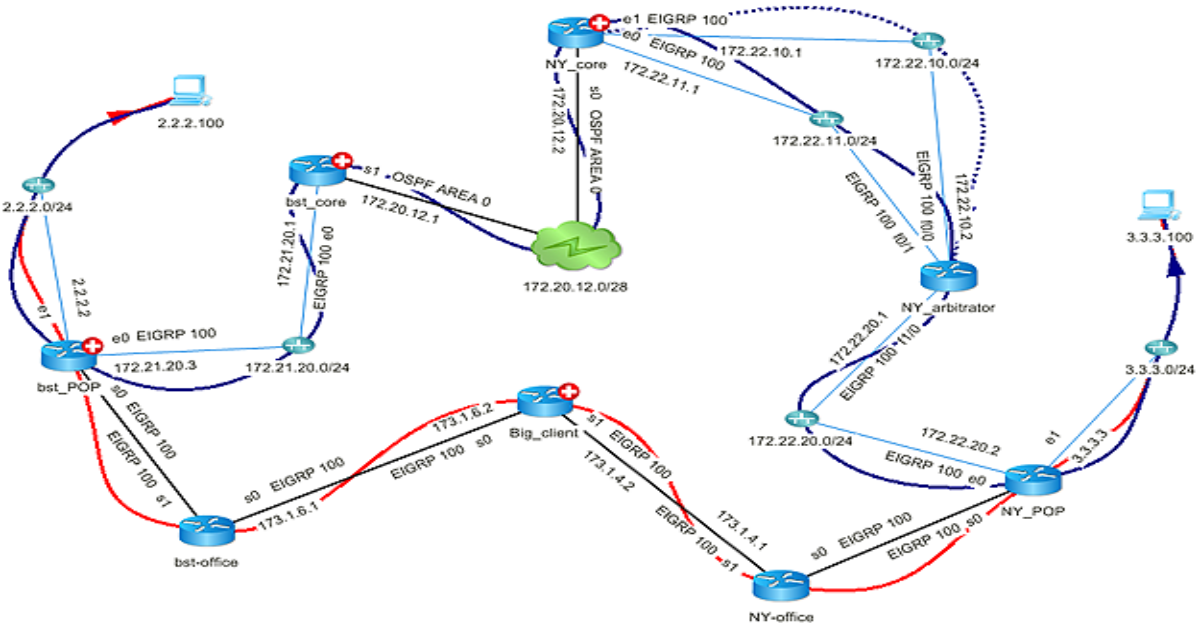
Within the management of information security controls, there are human and event driven parts. For example, security team members drive the human-driven activities while an Intrusion Detection System (IDS) or Firewall appliance triggers the event driven activity. Challenges surface combining both these elements when you want to get data to and from the network accurately, efficiently and promptly. NetBrain's adaptive solution is the canny brain of the entire network security operations that sits between both; the human and event-driven components.

ADAPTIVE NETWORK AUTOMATION FRAMEWORK

Cyber criminals are hurling an endless array of new threats at the gates of networks. Some of the latest cybercriminal events are breaching the most respected networks, taking critical services offline.

The DDoS landscape is constantly evolving, resulting in the requirement for an adaptive DDoS solution to evolve at the same pace as the newly arriving threats. However, a static DDoS solution will only stop yesterday's threats and has no chance of preventing unknown future events. We don't know what's coming tomorrow; therefore, security professionals require a flexible and adaptable solution. NetBrain's Adaptive Network Automation framework is updated with lessons learned to keep pace with the new threats and the up-to-the-minute cyber criminal's knowledge.

Now with NetBrain, automation is highly customizable by the end user without the complication of human-driven scripts. More importantly, it can be adaptive to each and every unique network, task and type of attack. This is the only way to stop any type of DDoS event.



DYNAMIC MAPS

NetBrain Dynamic Map provides data visualization, allowing the visualization of a DDoS. In contrast to a static diagram, the Dynamic Map provides infinite details within a single pane of glass. The mapping is completely automated. It is externally triggered with the ability to track the user's interactions from multiple locations which is a leap forward in diagramming technology. It is data-driven which is similar to the design of Google maps.

Custom Maps are created on demand with the ability to map any two endpoints and search details on that path. The capabilities of data-driven functionality enable the administrators to zoom in for additional information with layers of data that can be dynamically turned on/off. The Heat Map facilities enable administrators to view network performance either in network entirety or specific hot spots that is similar to viewing traffic on Google maps.

The unique discovery and benchmark engine leverages Telnet/SSH in addition to the traditional SNMP to log in to every device and extract configuration and design data. This data is compiled into a mathematical model of the network. Each map represents a live rendering of a mathematical model derived from the live network. The data elements behind each device icon and interface label on the map are a part of that model (e.g. device images, properties, config data, etc.).

The mathematical model of the network enables the ability to render the data efficiently. Filtering views of the map can drill into specific network hot spots when troubleshooting a DDoS attack.

DYNAMIC MAP FUNCTIONS

Map the Network in Seconds: Deep network discovery powered by SNMP, Telnet, and SSH is used to collect the data that creates mathematical models which can be used over again for on-demand mapping. The network is not discovered every time as a mathematical model is used to create the on-demand Maps.

Visualize Any Data on The Map: A Map can be enhanced with any type of I.T data. Within the data view you can turn on various design elements such as routing, QoS, performance, network health, and interface errors. Through integration it details the list and what you can view of a single URL Map is endless.

Trigger Map Creation from External Events: As discussed, a map can be created from an external event such as IDS, allowing immediate troubleshooting to be initiated with no human intervention.

EXECUTABLE RUNBOOKS

A static playbook is like a binder full of steps. It's possible to digitize the process with a playbook but the tracking results and team collaboration is challenging. Executable Runbooks are all about data analysis which can be used to automate security checklists and validate a network design.

Runbooks contain digitized knowledge of how to protect, defend and troubleshoot a DDoS event. They bring the benefits of automation to any workflow. They guide the administrators from all levels with data analysis to help streamline the operations and other tasks.

EXECUTABLE RUNBOOK FUNCTIONS

Make Any Workflow Executable: Not only can you digitize the workflows, you can also make them executable so that every step in the Runbook can be automated with a click of a button for data collection and analysis.

Codify Knowledge with Best Practices: Runbooks employ the best practice of the design and codify it. Earlier, this information was stored in the minds of the engineer but now it is shared and digitized into various Playbooks. Anyone can access the runbook with the appropriate rights, can update it and share the knowledge amongst other team members.

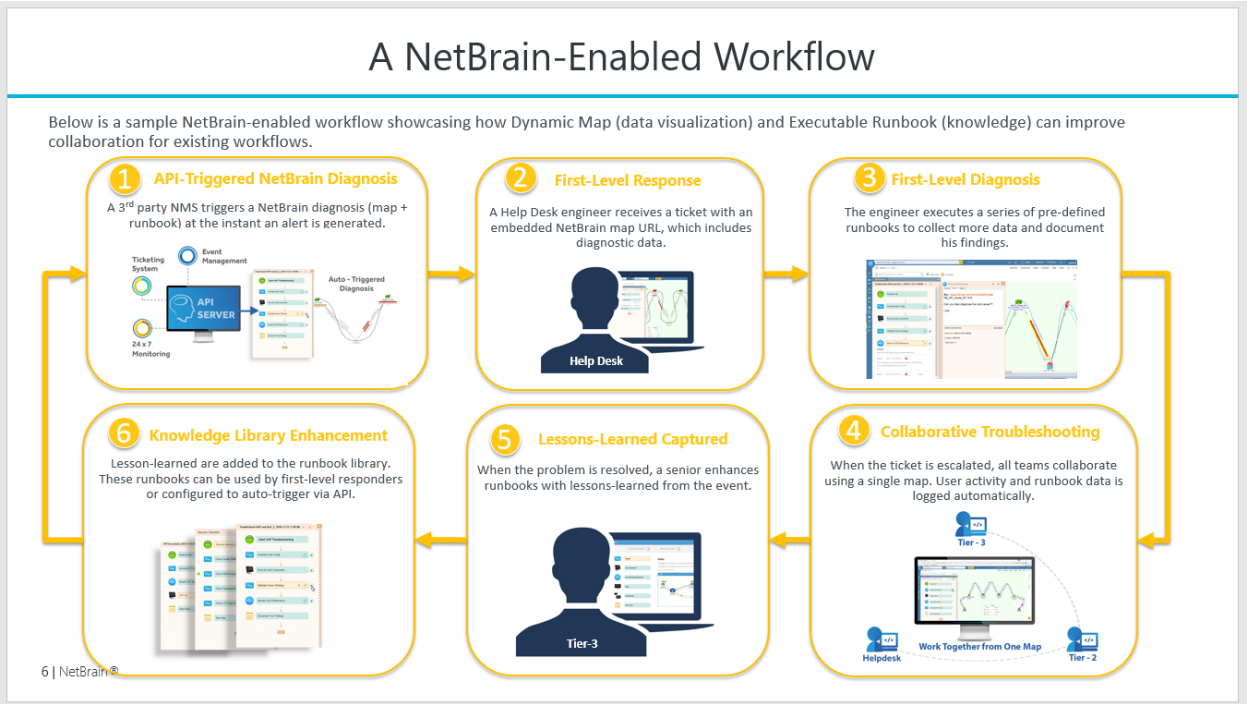
Lessons-Learned: Once the threat has been mitigated, multiple team members both Internal and external can enhance network hardening runbooks with lesson-learned from the event. Enhancing Runbooks from lesson-learns produce a proactive approach to security. Network hardening and vulnerability assessments can be enhanced with the latest cybercriminal knowledge.

Document and Share Workflow Data Automatically: Executable Runbooks are tracked and everyone involved is collaborated and aligned. Results are easily shared from one Map URL and multiple teams can work collaboratively from this map. When data is collected with a Runbook, there is the concept of what's known as the results. The results are stored inside the runbook and are self-documenting. All the data captured during a Runbook execution is stored inside the Runbook as a result and that is attached to the Map for easy access and sharing. This is an imperative phase for team collaboration as emailing logs and text files is not the way forward.

Knowledge sharing and lessons learned are then inputted into the Runbook repository: This allows seamless collaboration of sharing the best practices and knowledge gained from the event. Having a central repository with guided steps that are shared among all members, proactively protects against non-compliance.

WORKFLOW INTEGRATION

The Dynamic Map combined with Executable Runbooks enhances the collaboration, making the end-to-end process of troubleshooting more streamlined. The diagram below displays 6 keys steps of the DDoS troubleshooting process. NetBrain's solution glues these steps together systematically for the dispersed teams and systems to interact more smoothly.



1. Step 1: A 3rd party system, for example, an IDS detects an anomaly and triggers a certain type of Dynamic Map and Executable Runbook. Different Runbooks are selected based on different types of anomalies. For example, a Runbook may be selected to do an overall network performance health check.

2. Step 2: The first-line engineer automatically receives a ticket containing all relevant information about the newly detected threat. Each Map is referenced with a single map URL.

3. Step 3: The first-line engineer digs deeper into the problem with systematic troubleshooting steps by running predefined Executable Runbooks created by senior engineers.

4. Step 4: The ticket gets escalated to a number of internal and external teams for additional analysis. All user activity is tracked and automatically logged within one single Map URL.

5. Step 5: Once the event is successfully troubleshooted, lessons learned and knowledge gained is captured in the Runbook.

6. Step 6: The enhanced Runbook is added to the Runbook library which is made available to first-line help desk engineer and any other 3rd Party systems. This approach reduces Mean-Time-To-Repair (MTTR) for the next DDoS event.

NETBRAIN'S API INTEGRATION

NetBrain's rich API offers endless integration points enhancing the details both from the security configuration and design perspective, all through a single pane of glass. NetBrain can integrate with literally any other system, offering Layer 1 to Layer 7 details along with the ability to be triggered to run specific events. This enables continuous automation to stop DDoS event from taking the service offline.

INTEGRATION POINTS FOR CONTINUOUS AUTOMATION

A new generation of thought proposes Continuous Automation. It involves a new automation framework consisting of many autonomous, communicating with no human interaction.

Continuous Automation takes you to the next level that enables the automatic shunting of traffic, disables affected ports or apply security patches in response to a threat. New workflow and connectivity models of how security services interact with each other are formulated in an entirely automated fashion.

For example, NetBrain can integrate with an IDS for automatic triggering based on anomaly detection. A security breach detected by the IDS can trigger a number of Executable Runbooks to perform different security checks on the network. An example of a basic security check would focus on high congestion points while a more advanced check would analyze various traffic patterns on the network, signaling an advanced type of DDoS attack.

The only way to stop day zero attacks is to automate and implement end-to-end DDoS solution completely. IDS anomaly detection and specific network conditions can trigger Runbooks and certain Runbooks can trigger events forming layers of Continuous Automation.

Regular server patching is the first tactical area to prevent DDoS. NetBrain integration points can also tie with an external patching system. If a server does not have an up to date patch, a series of network activities can be executed with runbooks.

SUMMARY

We are entering new territory of DDoS while most companies are still using traditional methods. These conventional methods are necessary but by themselves not an appropriate antidote for the current and future problems is something that we call as an 'unchartered territory' for such accustomed remedies. This is just like travelling in a glider in the era of 'jet age'. We are already observing this with some major networks being taking offline.

With the passage of time, the attacks have surged immensely, so should be the defense. Security professionals require a new approach to troubleshooting and team collaboration; a solution that can integrate with literally any other DDoS system providing the missing piece of the puzzle in the DDoS struggle. It's the right time to fortify our system with the tailored solution and banish the orthodox approach.

ABOUT NETBRAIN TECHNOLOGIES, INC.

Founded in 2004, NetBrain is the market leader in network automation. Its ground-breaking platform leverages the power of Dynamic Maps and Executable Runbooks to provide CIOs and network teams with end-to-end network visibility and analysis across physical, virtual, and software-defined networking environments. Today, more than 1,800 of the world's largest enterprises and managed service providers use NetBrain to automate network documentation, accelerate troubleshooting, and strengthen network security—while integrating with a rich ecosystem of partners.

NetBrain is headquartered in Burlington, Massachusetts, with offices in Sacramento, California; Munich, Germany; and Beijing, China. For more information, visit https://www.netbraintech.com/. NetBrain® and the NetBrain logo are registered trademarks of NetBrain Technologies.