CREATING A BASELINE

& DETECTING DEVIATIONS

ANOMALY DETECTION

Students will learn that IT security today is placed on anomaly detection. Whether it is detecting abnormalities in user behavior, system states or trust relationships governed by keys and certificates, the theory is that the faster you can pinpoint anomalies, the faster you can find malicious threats and close security gaps.

YOUR SUBTLE STATEMENT HERE

THREAT DETECTION OVERVIEW

THREAT DETECTION

Three Types of Threat Detection

Every performance monitoring product is ultimately seeking to provide threat detection. But it can mean a threat from different things. The most basic monitoring allows you to detect deviation from some best-practice default settings for performance metrics.

The performance metrics are identified as leading indicators of overall system performance. And the key is to detect problems early before they affect user performance or impact service level agreements.

The downside to this essential threat detection is balancing the danger of missing problems (false negatives) and the overhead of managing too many false positive alerts. False positives mean the signs are overly cautious and generate warnings when no real underlying problem exists to solve.

There are three important ways security tools detect threats.

Those methods are

- Signature Detection
- Behavior Detection
- Anomaly Detection

Most security tools of one or more of these capabilities to detect threats. The figure represents this concept.

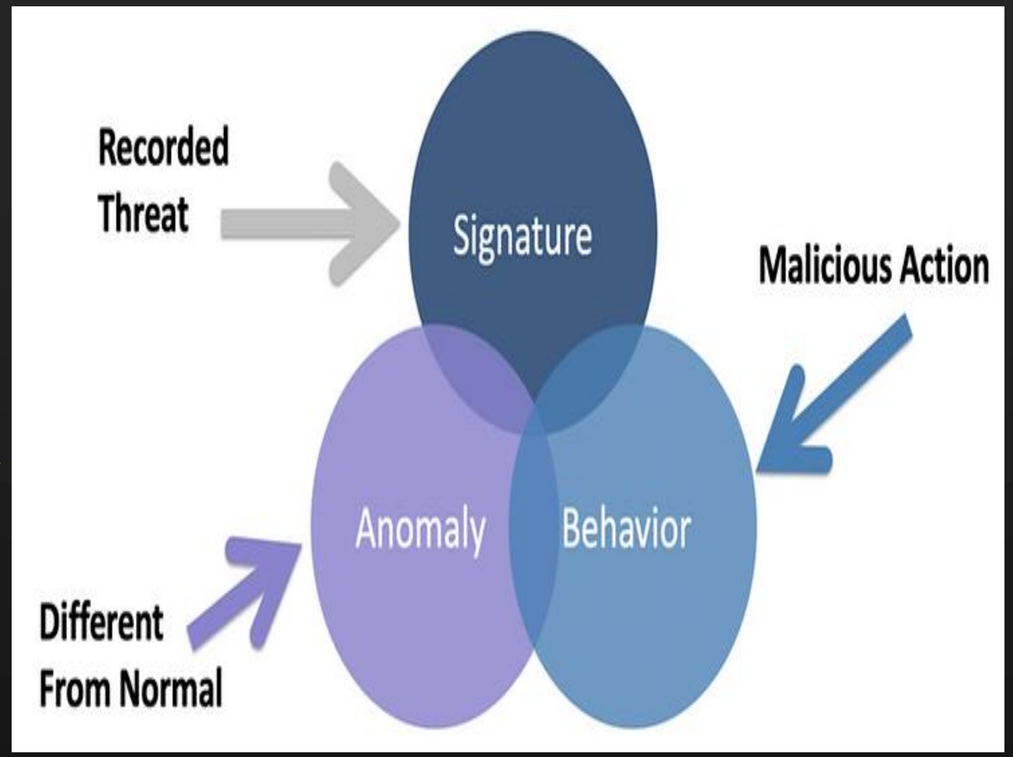


Figure 1: These are three important ways security tools detect threats

THREAT DETECTION

Three Types of Threat Detection (cont)

Signature Detection

Signature detection requires knowing what to look for and comparing hashes or other strings to identify a match.

Signature detection is standard vein within antivirus and IPS/IDS products.

Behavior Detection

Behavior detection looks for malicious or other known behavior characteristics and alarms the SOC when a match is made.

An example is identifying port scanning or a file attempting to encrypt your hard drive, indicating ransomware behavior. Antimalware and sandboxes are examples of tools that heavily leverage behavior detection capabilities.

Anomaly Detection

The third capability I'll focus on in this post is to look for anomalies. This capability is the future of security, and I see this is where a lot of the current innovation is occurring in the security space. It considers hot topics, including big data, threat intelligence, and "zero-day" detection. Hence, everybody needs to know how this approach to security is better to understand the future of the security market space.

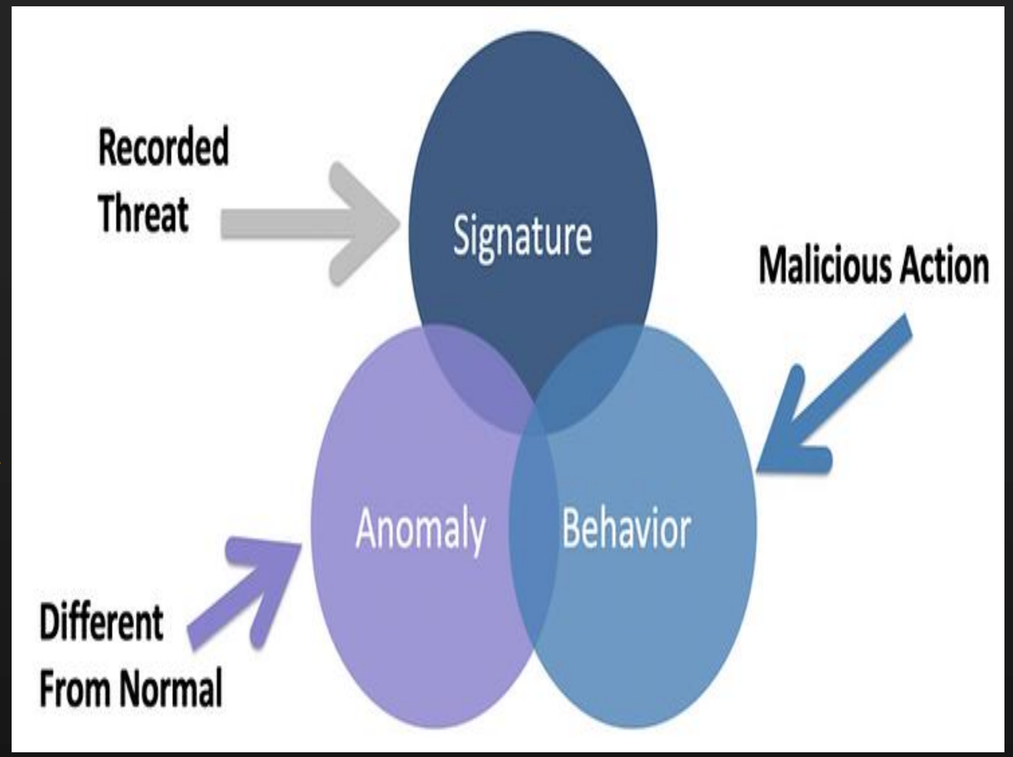
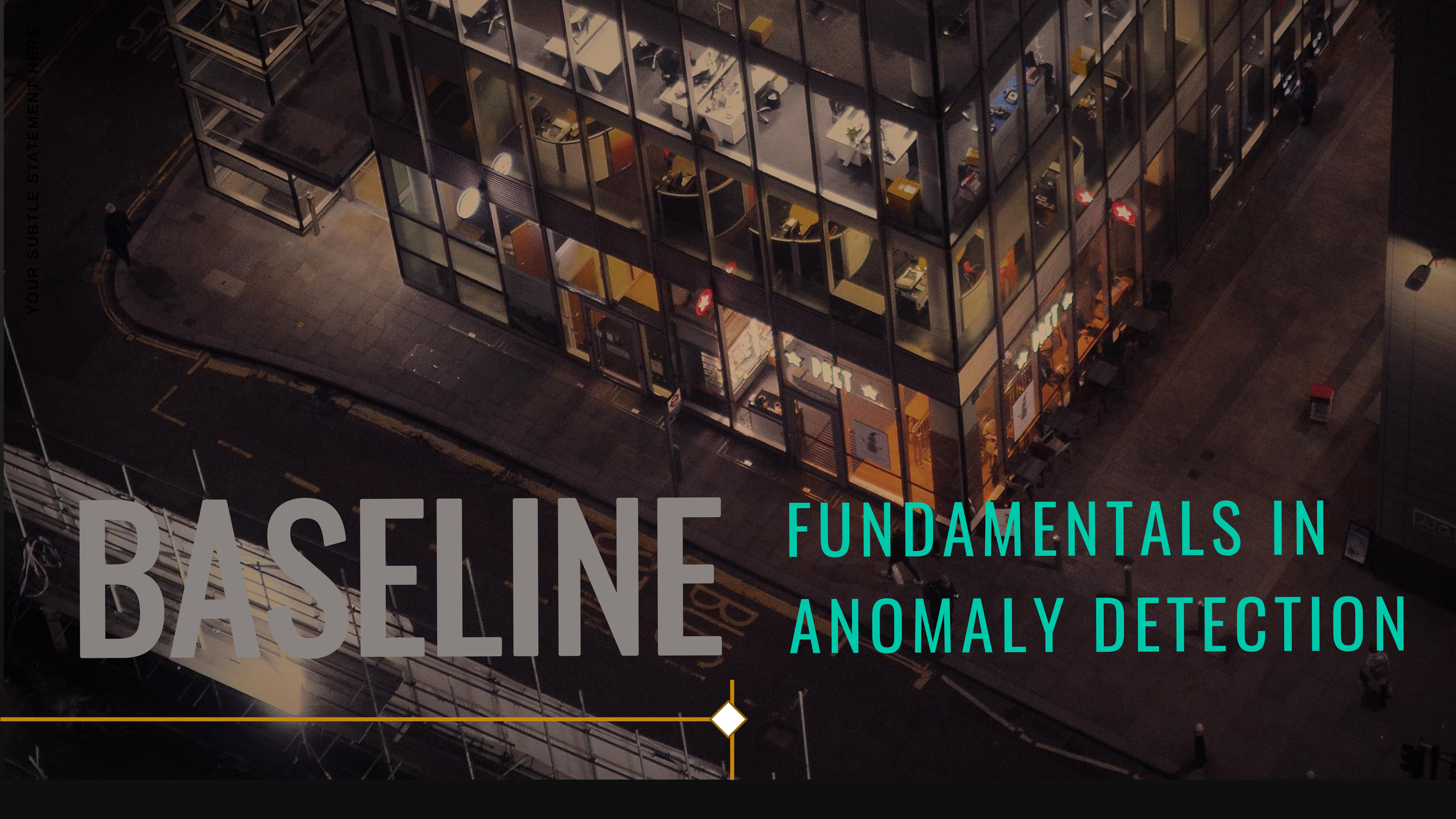


Figure 2: The three important ways security tools detect threats


YOUR SUBTLE STATEMENT HERE
BASELINE
FUNDAMENTALS IN
ANOMALY DETECTION

ESTABLISHING A BASELINE

Identifying Normal

Before determining something is an anomaly, you must first understand what is considered normal. This makes up the first part of any anomaly detection capability which is understanding normal behavior.

Establishing Normal Can Occur In Two Ways:

1. One way is to learn about an environment over time and map out expected behavior, known as baselining the environment.
2. The other approach is to pull in a ton of historical data and immediately compare things against it to find outliers. First, let's look at the first approach, baselining.

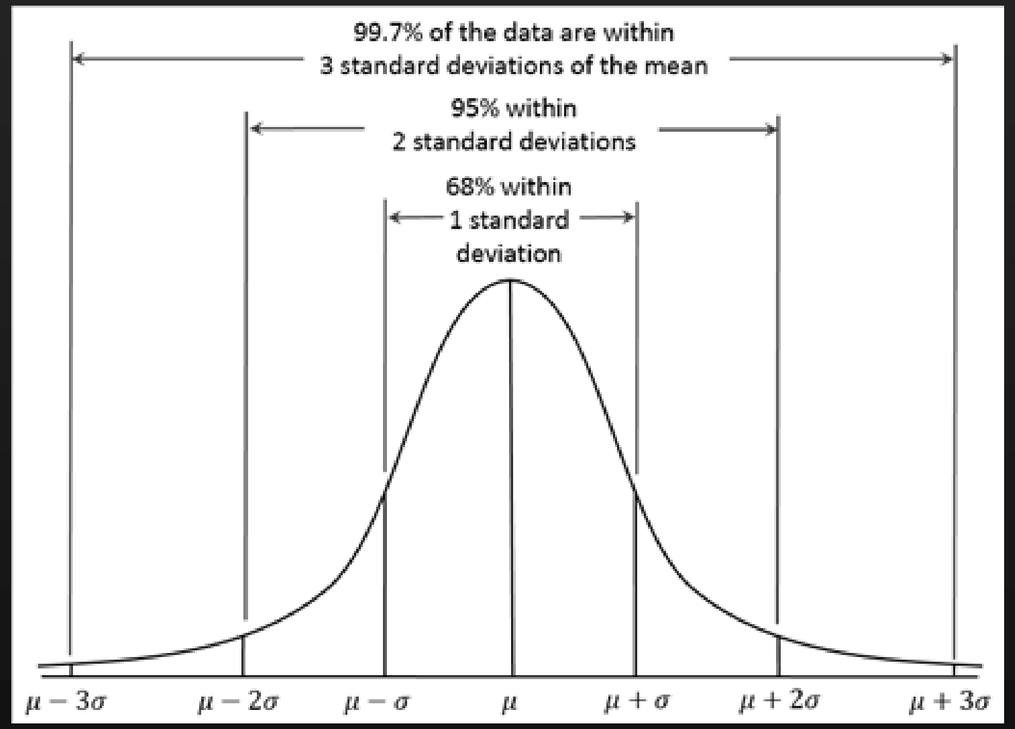


Figure 3: Before determining something is an anomaly, you must first understand what is considered normal. This makes up the first part of any anomaly detection capability which is understanding normal behavior.

ESTABLISHING A BASELINE

Baselining

So, what do consultants mean when they advise you to "take a baseline" as the first step to monitoring and improving performance?

At its most basic definition, a baseline is any starting measurement you take to evaluate future changes against the same. It doesn't have to be representative; it doesn't have to be taken over time. But if you want it to be meaningful, you will want to take it at an appropriate time when you want to compare future measurements, and you will want to take multiple sizes to ensure you don't have an "outlier" as your baseline.

The best way to accomplish this task is to take many measurements and evaluate those measurements statistically to determine a "normal" operating range for your system.

Of course, you need to take these measurements when the overall performance is acceptable. You don't want your "normal" to be "abnormal" from your users' perspective. Learning about an environment means collecting data. Many bleeding-edge host security tools are designed to monitor any process running on a host and map out its behavior.

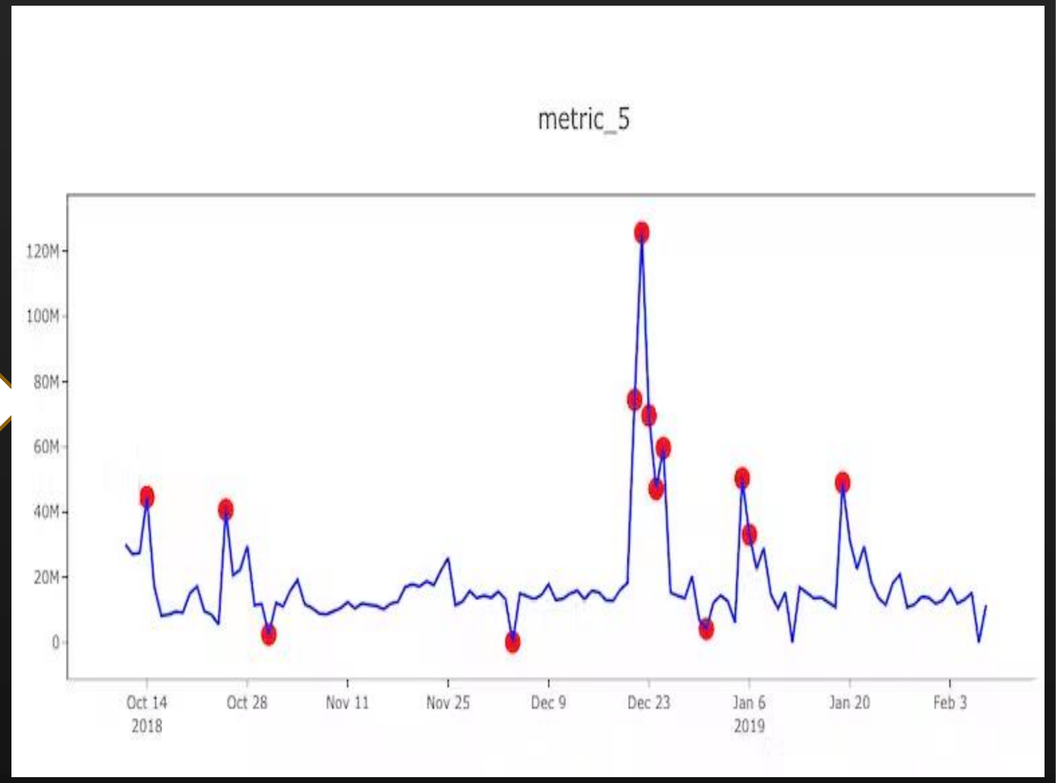


Figure 4: At its most basic definition, a baseline is any starting measurement you take to evaluate future changes against the same.

ESTABLISHING A BASELINE

Technology Behavioral Profiling

Over some time, one process of talking to different approaches can also be part of the baseline if this activity is considered normal behavior. This larger baseline concept leads to the ability to dynamically learn and adjust an allow list without human interaction since changes are considered normal; hence the technology can permit the traffic based not just on a permit list but permit behavior that has been established within the baseline.

The figure shows an example of Cisco Tetration baselining workload distribution behavior, network traffic behavior via how applications communicate with the network, and child activity, also known as processes being run.

There Are Network Tools That Can Also Function Similarly

Cisco Stealthwatch and Plixer are two examples of tools that learn network behavior through baselining and identify when unusual behavior is seen.

In both the endpoint and network example, the longer the tools run, the more normal data is collected, and a better baseline is established.

Unlike other threat detection approaches, administrators do not need to spend countless hours adjusting the tools, also called "tunning."

Anomaly tools get smarter over time on their own just by collecting data. The following image shows Cisco Stealtwatch using baselining to detect various network-based threats.

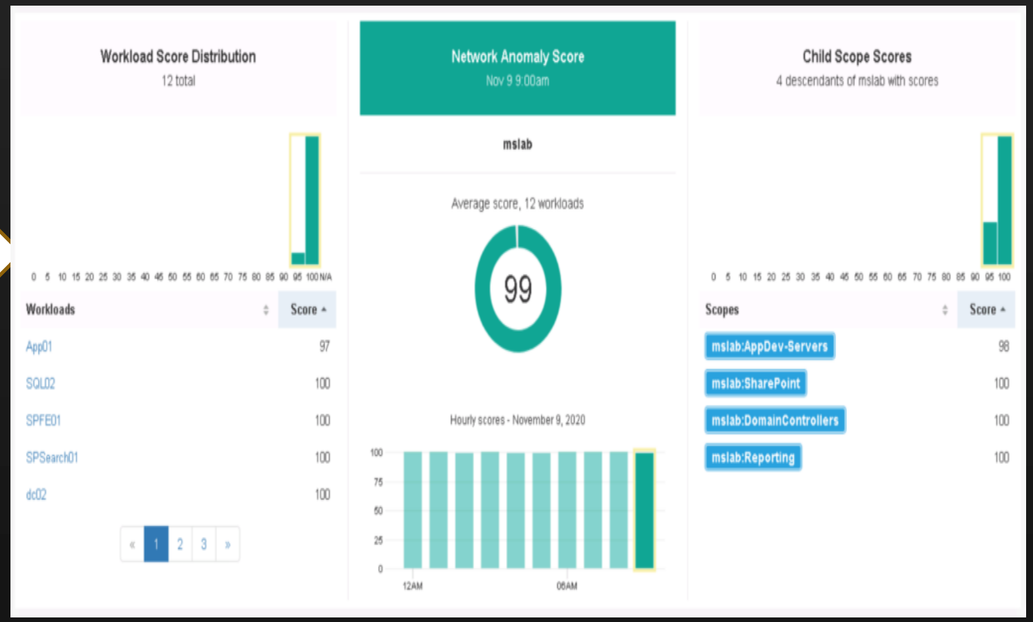


Figure 5: Cisco Tetration baselining workload distribution behavior, network traffic behavior via how applications communicate with the network, and child activity, also known as processes being run.

ESTABLISHING A BASELINE

Big Data Baselining

The second approach to understanding normal behavior leads us to extensive data conversation.

The previous baseline approach is good, but it is limited to what is expected within what the security tool can see.

If other people's baselines are added into the mix, you open up a much more robust understanding of the concept of normal. For example, let's say there is a new day zero that nobody has ever seen, and it's trying to install itself on your endpoint. Its activity should look different than the behavior of any application that has established itself on your host.

Now think about seeing how similar applications have acted across thousands of systems worldwide along with the baseline of what you know as normal. If day zero claims to be a upgrade.exe file for a Microsoft product, threat intelligence based on big data can take that file and see how it compares to other upgrade.exe file activity as a similar file is installed on thousands of systems around the world.

If 99.99999% of the time the file acts one way and you find your version is acting different, a significant data baseline will immediately point out that your understanding of upgrade.exe is not standard.

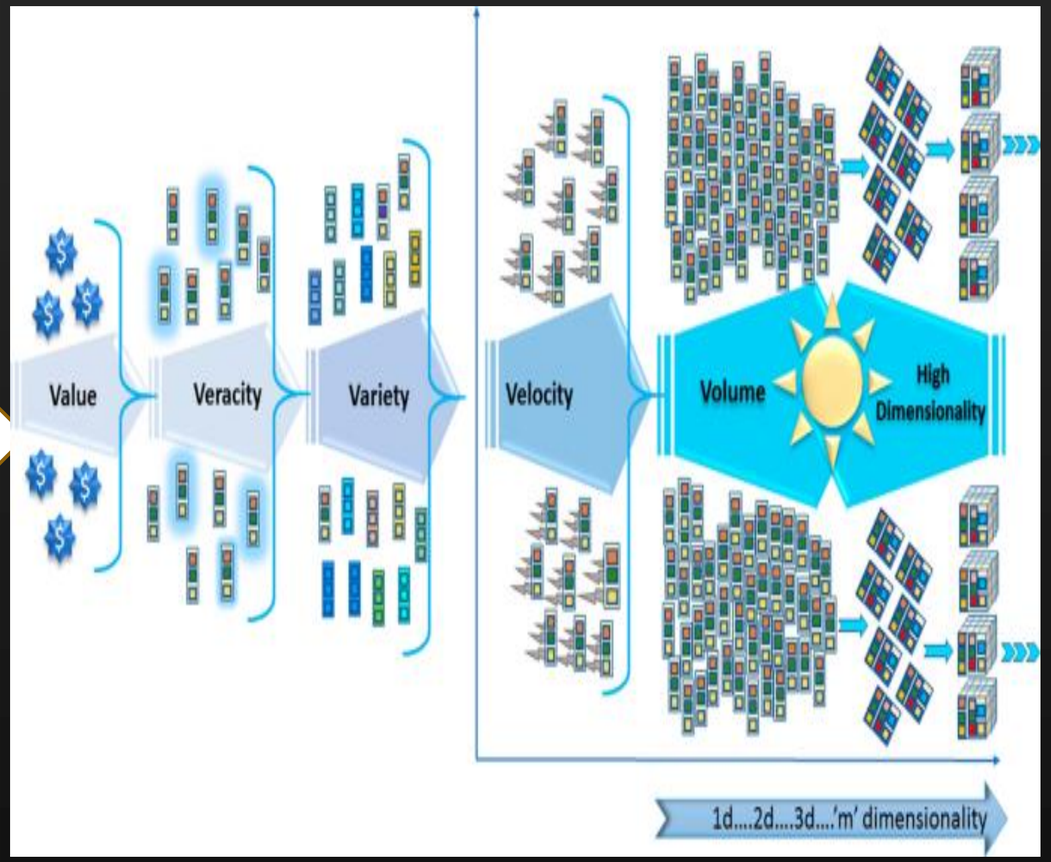


Figure 6: A comprehensive survey of anomaly detection techniques for high dimensional big data

YOUR SUBTLE STATEMENT HERE

ANOMALY DETECTION FUNDAMENTALS

ANOMALY DETECTION BASICS

What is Anomaly Detection?

Anomaly detection is a relatively new way to identify and classify a rare event or observation data that doesn't fit the norm.

Outlier Detection

Also referred to as outlier detection, this is the term given to unlabelled data by data scientists and cybersecurity analysts for network security to identify intrusions, cyberattacks, or misuse of systems, including information leaks and fraud. Anomaly detection promises to be unsupervised by design.

Rare & Infrequent

It should be noted that critical in defining and classifying anomalies is the characteristic that they're rare and infrequent deviations from normal behavior and existing data sets. But not every rare monster flagged is terrible, so a quick and intelligent intervention is needed. Given the amount of network data flowing in and out of any given SOC, the number of attacks they've seen is relatively low, and attacks evolve daily.

Hence, an algorithm is the best bet for finding that dangerous needle in a cyber-haystack so that an analyst can address the anomaly.

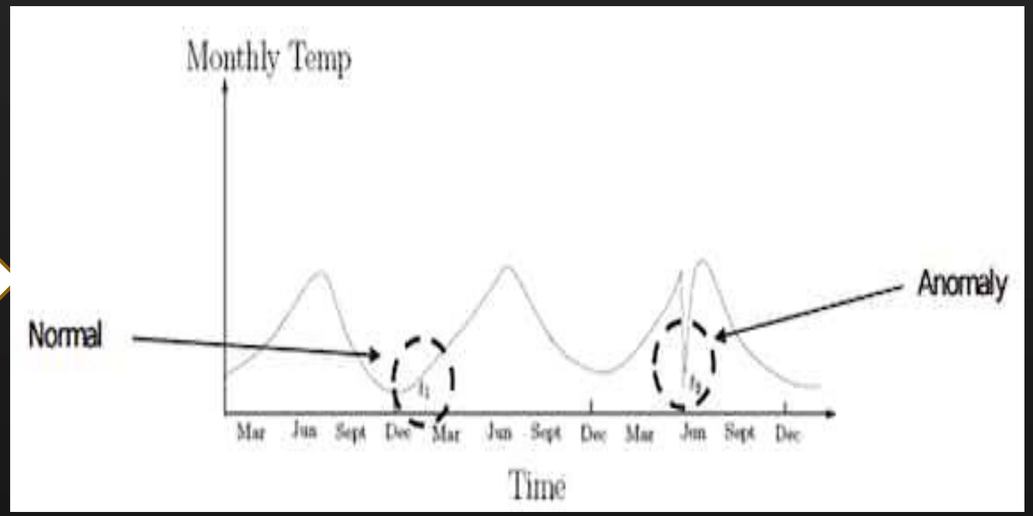


Figure 7: It should be noted that critical in defining and classifying anomalies is the characteristic that they're rare and infrequent deviations from normal behavior and existing data sets.

ANOMALY DETECTION BASICS

Anomaly Detection Needs (Mis)Use Cases

As promising as it sounds like relying on intelligent technology, AI, and Machine Learning to detect these new and diverse types of attacks, several procedural factors should be considered.

As mentioned earlier, not every deviation from the normal is terrible. Large computer networks have a pattern or rhythm; processes run periodically, the same users do the same things every day, and so on. But network traffic is far from regular at the best of times.

Operational events stemming from system errors and misconfigurations often interrupt the routine. Or system changes and patches are deployed to address security vulnerabilities and offer new features. Even job responsibilities change in the natural cycle of hiring, promotions, or resignations. Is it difficult to classify these events as "anomalies" with so many irregular changes?" The answer is yes. And no.

Every network ecosystem is constantly changing, and relying on an anomaly detection algorithm to detect cyber-attacks 100% accurately will be a challenge. When it comes to intrusion detection, not every unexpected piece of data is wrong. If your software doesn't know any better, it might flag a benign action as something more serious.

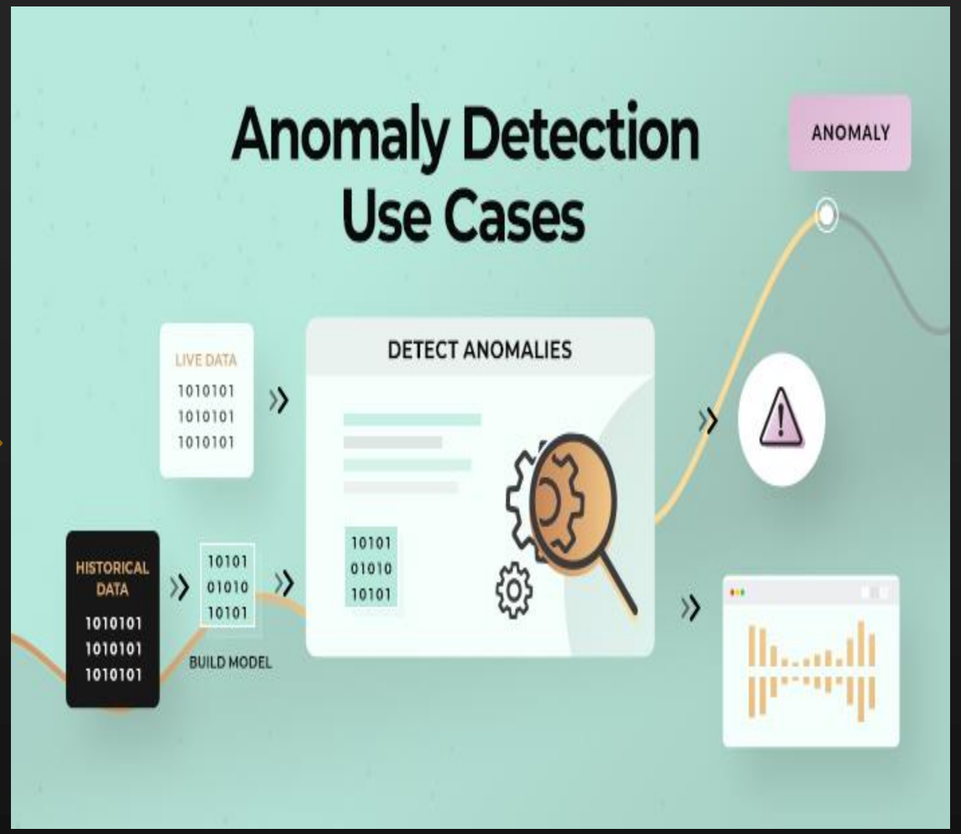


Figure 8: As mentioned earlier, not every deviation from the normal is terrible. Large computer networks have a pattern or rhythm; processes run periodically, the same users do the same things every day, and so on. But network traffic is far from regular at the best of times.

ANOMALY DETECTION BASICS

Anomaly Detection - Limitations

As discussed above, anomaly detection techniques rely on a generic statistical measure or a set of data points that need to be programmed into the algorithm. And as we also mentioned, benign activity can sometimes be classified as an anomaly when it is not a security risk.

Not Every Rare Event Is Bad

Not every rare event is bad, so the goal is to find the "rare rare" events and behaviors that are malicious. But again, this lends itself to the all-too-common problem of a large number of false positives, which requires an analyst, or a senior member of the team, to manually verify each one via a costly and time-consuming investigation.

Unsupervised Anomaly Detection? Not Yet.

This also requires a full roster of capable but possibly overworked analysts in your SOC to conduct the investigations.

Consequently, when an analyst is presented with a set of anomalies, there's the possibility that they may not know why the items are considered anomalous since some algorithms utilize an underlying detection technique that may be a black box and does not reveal what features led to the alert.

Newer processes introduced into anomaly detection platforms may incorporate features such as Sequential Feature Explanation (as an example), which can direct researchers to focus only on the associated data that triggered the alert. This clearly is far from the unsupervised anomaly detection process that a SOC hoped for.

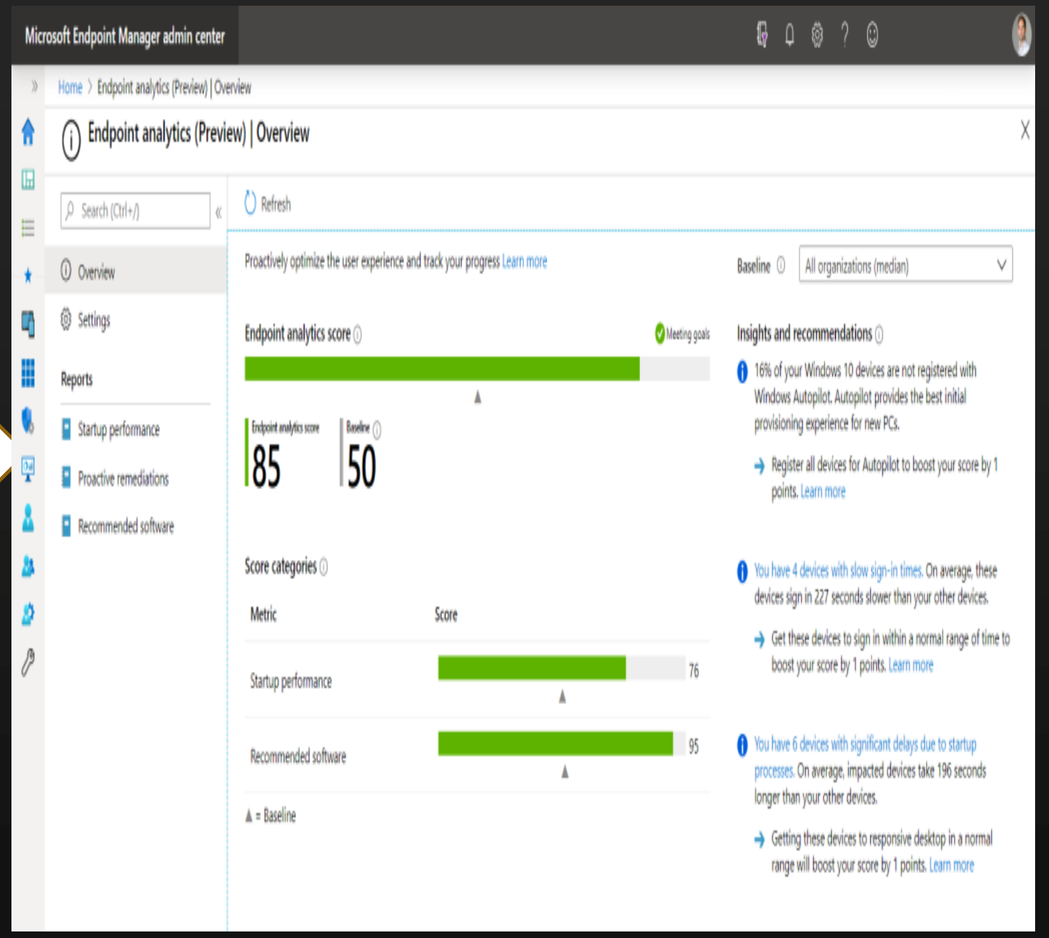


Figure 9: Administrators can define a rule for such endpoints and profile all of them at once. After previously unknown endpoints are profiled, this learning can be made part of a shared knowledge base to benefit other organizations in their own deployments.

ANOMALY DETECTION BASICS

Anomaly Detection Needs Baseline Management

The final limitation stems logically from the first two. While anomaly detection relies on the key factors of rich data sources, data science, domain knowledge of attack behavior, predictive algorithms within the AI, and machine learning, as we've indicated above, it's not enough.

Continuously Manage Baselines And Exception Handling

The next challenge for security analysts is finding ways to continuously manage baselines and exception handling without relying on cybersecurity experts and people power. This aspiration, however, is proving to be elusive.

There's no debate that the growing sophistication of AI technologies for predictive risk intelligence offers promise.

An Imperfect System

A report by Deloitte posits that AI has reached the point where it can generate its hypothesis, predict attack techniques, and provide recommendations for them. While this may be true, it's an imperfect system.

Intelligent cyber technologies and AI complement existing security controls to detect progressive, emergent, and unknown threats. The human element still needs to teach, train, and manage the AI-powered detection system to ensure maximum efficacy.

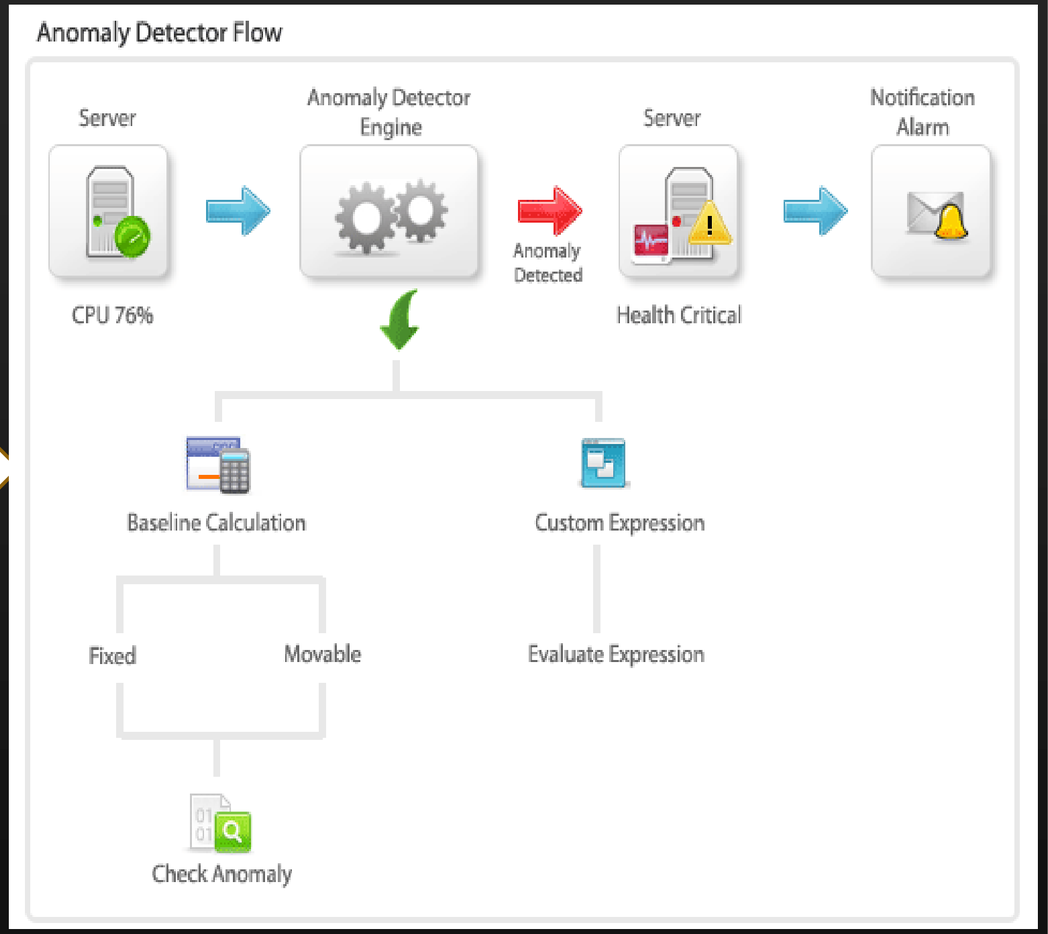


Figure 10: The final limitation stems logically from the first two. While anomaly detection relies on the key factors of rich data sources, data science, domain knowledge of attack behavior, predictive algorithms within the AI, and machine learning, as we've indicated above, it's not enough.

ANOMALY DETECTION EPILOGUE

Improve Anomaly Detection with a Hybrid Model

As previously mentioned, the most optimal future for a secure infrastructure is AI-Assisted Cybersecurity as part of a hybrid model with analysts.

A future-proof SOC can emerge by combining an AI capable of deep learning and anomaly detection with the extra input of human creativity, common sense, and knowledge from analysts.

The goal is to manage those baselines (which cause false positives/difficulty understanding the anomaly) without requiring extensive knowledge. Hence, artificial intelligence offers assistance.

Once an abnormality is detected and an alert issued, an AI-Assisted Cybersecurity tool such as Arcanna.ai streamlines the time-consuming work of a large number of the cybersecurity workforce.

It frees up an analyst's capacity to deal with threats. This is the critical strength of relying on AI. Their institutionalized knowledge is continually integrated with the AI-Assisted Cybersecurity tool to get the most out of the algorithm.

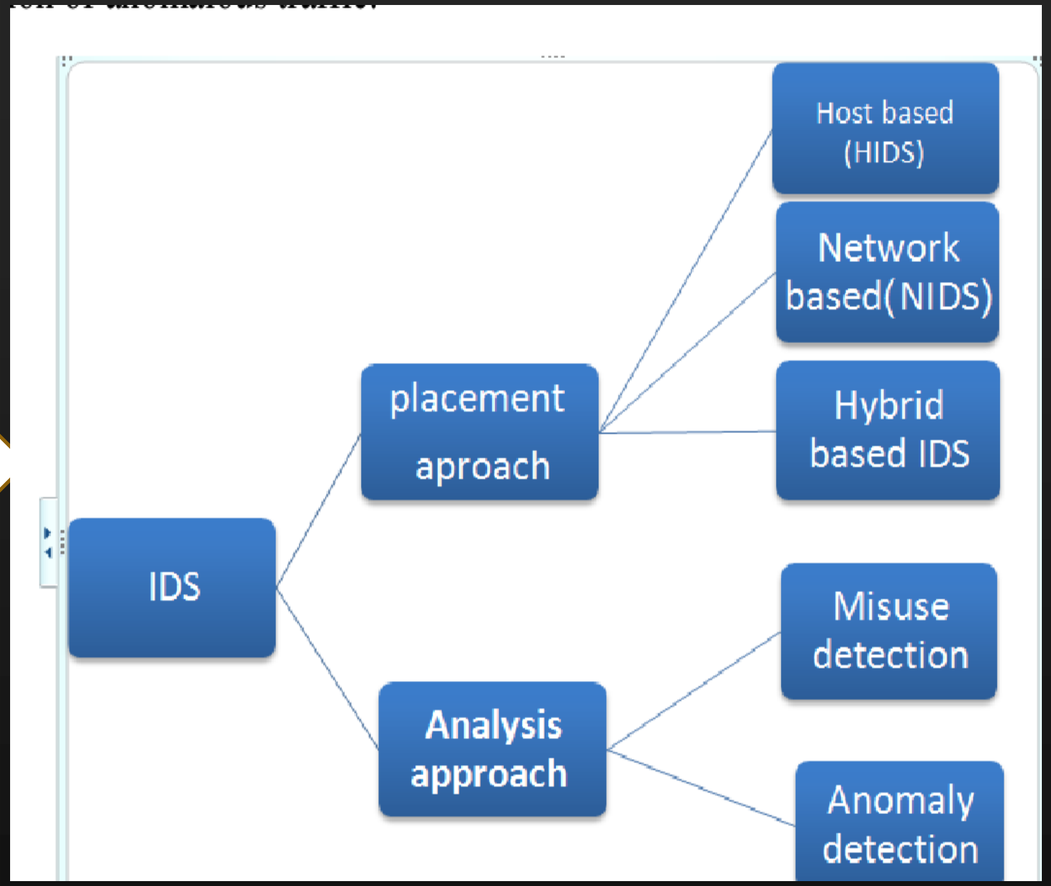


Figure 11: A future-proof SOC can emerge by combining an AI capable of deep learning and anomaly detection with the extra input of human creativity, common sense, and knowledge from analysts.

YOUR SUBTLE STATEMENT HERE

ANOMALY DETECTION

MUST-HAVE FEATURES

ANOMALY DETECTION EPILOGUE

Top 5 Key Must-Have Features of Network Behavior Anomaly Detection Tools

Network behavior anomaly detection refers to the process of continuously monitoring network packets to identify patterns and look for suspicious actors or threats. Key Must-Have Features of Network Behavior Anomaly Detection Tools

Different network data packets have unique signatures such as headers, correct formats, code practices, etc. Using network behavior anomaly detection, enterprises can automatically map network packets' acceptable behavior to highlight any unusual events.

Data from these unusual events are further analyzed to filter out the noise and false positives. The resulting alerts are sent to the network management team or the information security team for speedy resolution.

Network behavior anomaly detection tools simplify this process by providing pre-built analytical models, integrations, and false-positive mitigation measures. It can also identify anomalies that have evaded traditional endpoint security systems.

73% of cybersecurity professionals agree that monitoring the network is critical for gaining comprehensive visibility into security anomalies and protecting endpoints, as per the 2021 Network Detection and Response Report by ENEA Qosmos.

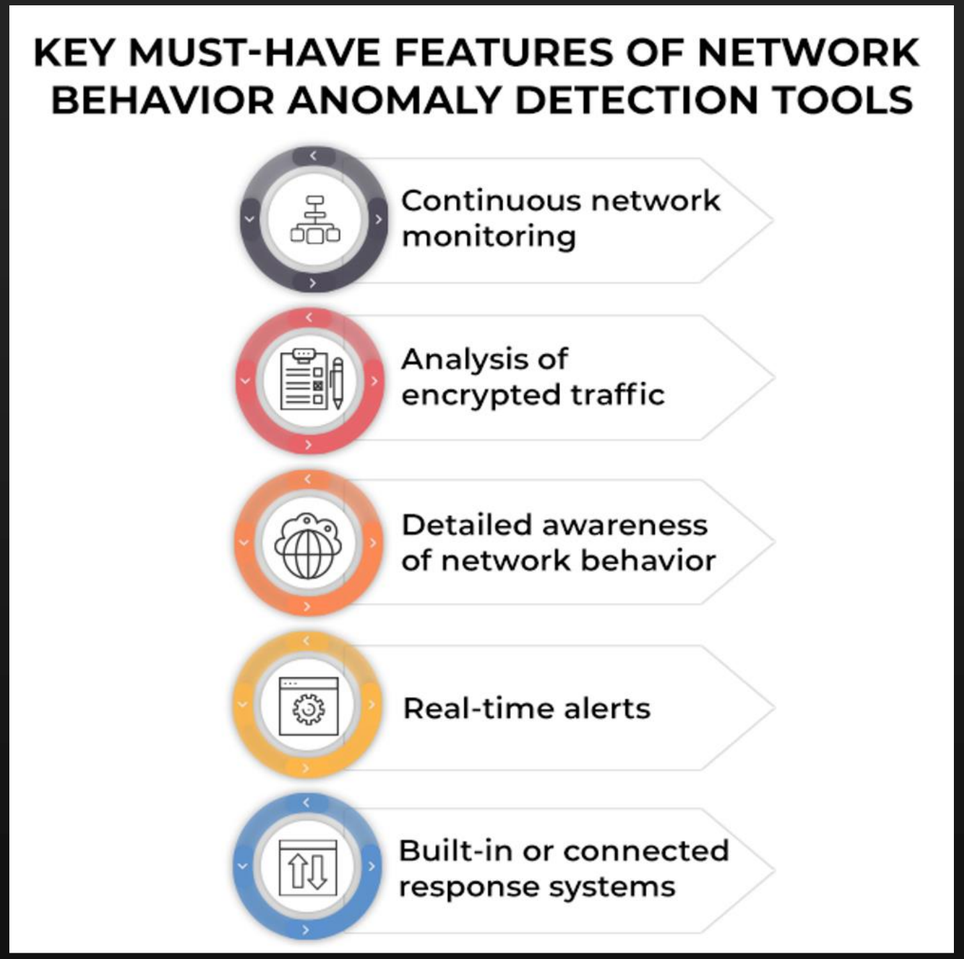


Figure 12: Endpoint security is often seen as cybersecurity's frontline and represents one of the first places organizations look to secure their enterprise networks.

ANOMALY DETECTION EPILOGUE

Top 5 Key Must-Have Features of Network Behavior Anomaly Detection Tools

Here are the five key features of network behavior anomaly detection tools that help achieve this:

1. Continuous Network Monitoring

Network behavior anomaly detection is a permanent fixture in an information security landscape. It is an "always-on" activity, continuously monitoring network behavior to look for potential threats. Key behavioral parameters are benchmarked against acceptable standards and historical patterns so that the tool highlights any event that stands out.

2. Analysis Of Encrypted Traffic

The tool should analyze encrypted traffic and regular packets shared across public networks. This is because network security tools are typically deployed in private, enterprise environments, where most traffic volume is encrypted. The tool must monitor and analyze encrypted flows for threats and non-compliance risks to provide comprehensive visibility.

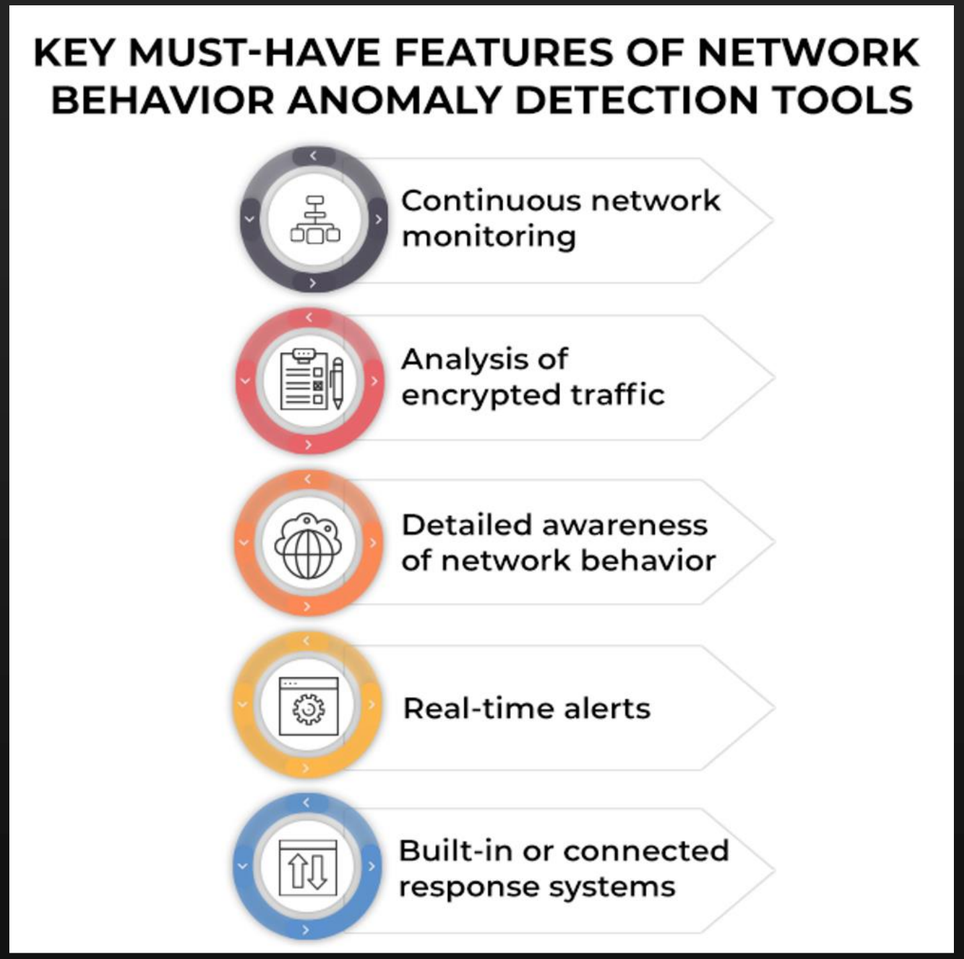


Figure 13: Endpoint security is often seen as cybersecurity's frontline and represents one of the first places organizations look to secure their enterprise networks.

ANOMALY DETECTION EPILOGUE

Top 5 Key Must-Have Features of Network Behavior Anomaly Detection Tools

3. Detailed Awareness Of Network Behavior

It isn't enough to simply highlight an unusual network event without any background information. For example, the tool may inform the network manager about unusually high bandwidth utilization by an app. But is this behavior legitimate, arising from a new high-demand business process, or is it the result of malware? The tool must provide detailed awareness and contextualized insights to enable the appropriate action.

4. Real-time Alerts

This is a core feature in a network behavior anomaly detection tool. Real-time alerts allow the network management team to receive information about a potential threat as soon as it is detected, without waiting for a scheduled report or checking a dashboard. The tool should ideally integrate with a security information and event management (SIEM) system to send these alerts.

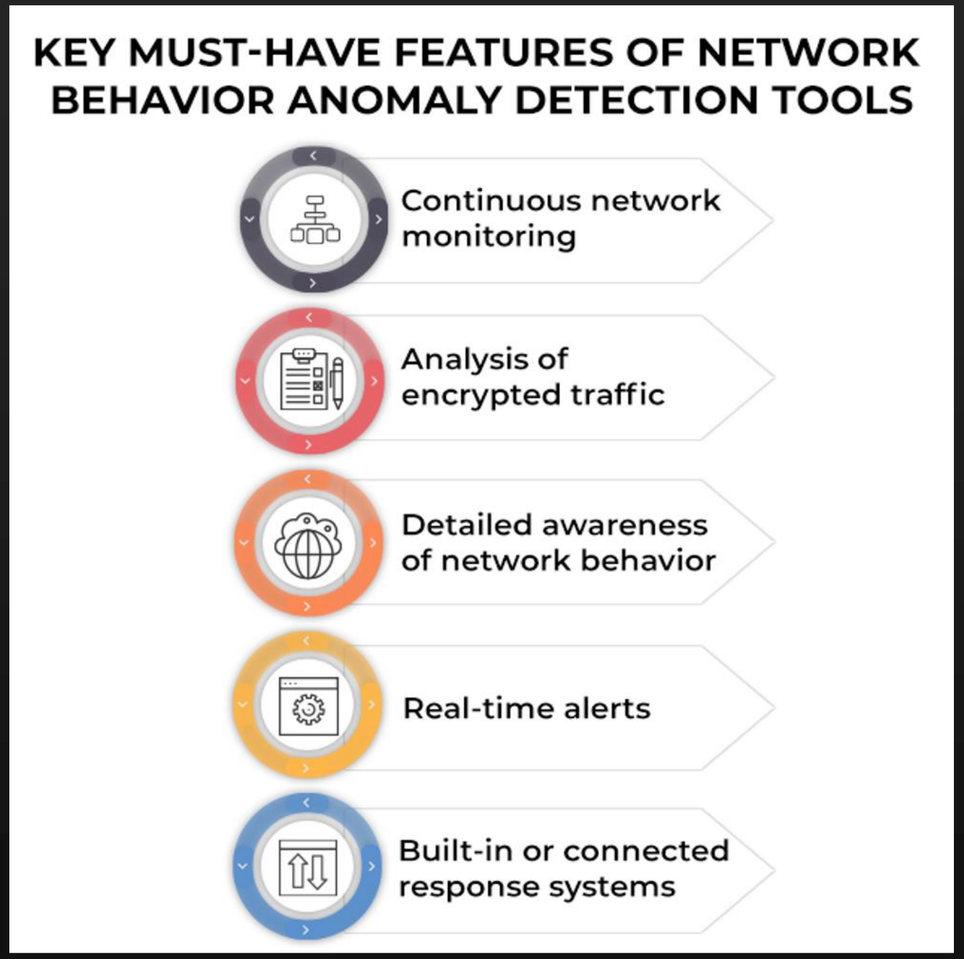


Figure 14: Endpoint security is often seen as cybersecurity's frontline and represents one of the first places organizations look to secure their enterprise networks.

ANOMALY DETECTION EPILOGUE

Top 5 Key Must-Have Features of Network Behavior Anomaly Detection Tools

5. Built-in Or Connected Response Systems

Detecting network behavior anomalies is part of the larger network detection and response (NDR) function. Like other security systems like firewalls or intrusion prevention software send alerts to the NDR, network anomaly data will also be processed for a speedy response. Some tools have a built-in NDR functionality so that users can investigate anomalies and respond to them in one workflow. Others may be connected to third-party NDR software or a SIEM system with NDR functionalities.

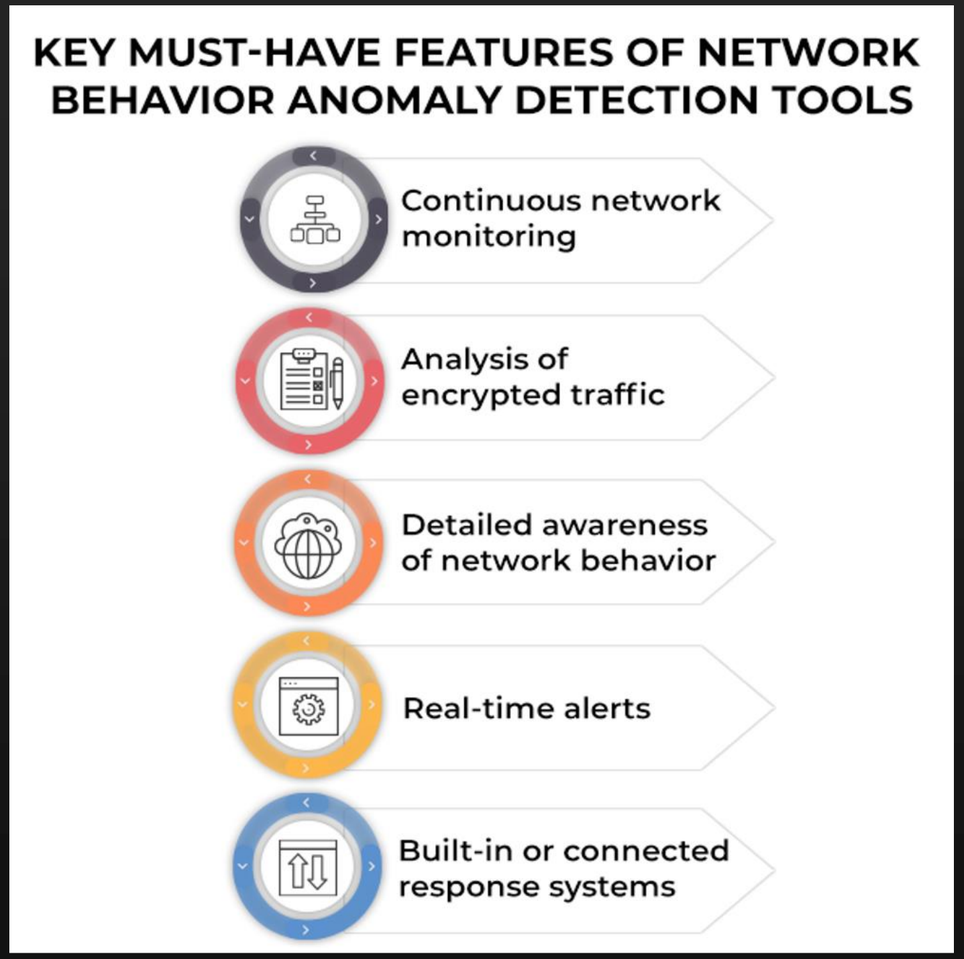


Figure 15: Endpoint security is often seen as cybersecurity's frontline and represents one of the first places organizations look to secure their enterprise networks.

YOUR SUBTLE STATEMENT HERE

ANOMALY DETECTION BEST PRACTICES

ANOMALY DET BEST PRACTICES

Anomaly Detection Best Practices for 2022

Are you considering adopting a network behavior anomaly detection solution for your organization? The best practices listed below can help you make the most of it in

2022.

1. Automate Your Analytics

Network behavior anomaly detection solutions use AI algorithms to analyze millions of network actions in just a few seconds. While this alone can significantly decrease the probability of threats making it through your network, automating all related analytics solutions can help boost your security team's efficiency. If you have a relevant use case, adopt end-to-end network analytic solutions for your enterprise to ensure maximum efficacy.

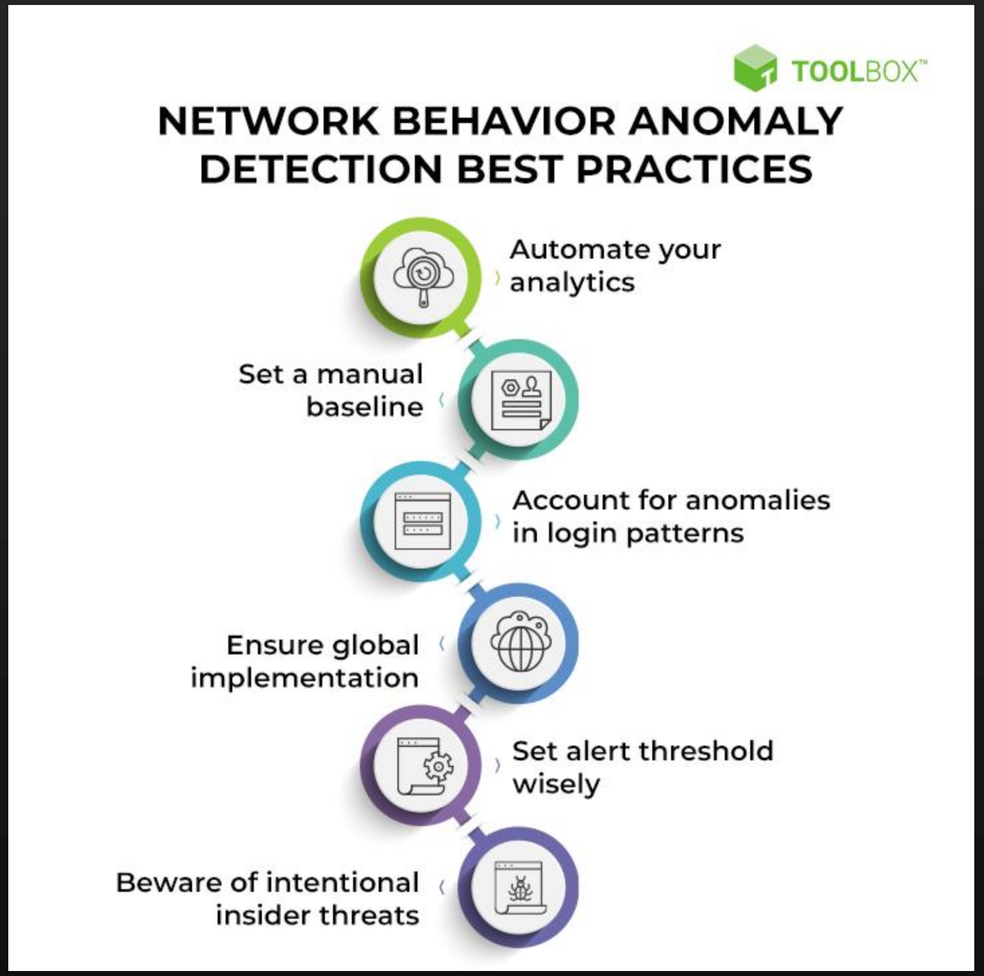


Figure 16: Endpoint security is often seen as cybersecurity's frontline and represents one of the first places organizations look to secure their enterprise networks.

ANOMALY DET BEST PRACTICES

2. Set A Manual Baseline

While anomaly detection solutions can set a baseline for network behavior, security teams might occasionally interfere with the alert settings. This can lead to them not being notified of certain abnormal user activities, such as the sudden downloading of massive volumes of data or the network being accessed from a new location.

While it is understandable if your security team wants to block specific alerts because the data is noisy, being utterly unaware of bizarre incidents might lead to data leaks or other cybersecurity incidents. Therefore, if keeping watches activated all the time is not an option, consider creating a manual baseline that can enable your security team to check the logs and spot uncharacteristic activities. This would help spot outliers such as a download being initiated in an untimely manner or a user accessing the network after work hours.

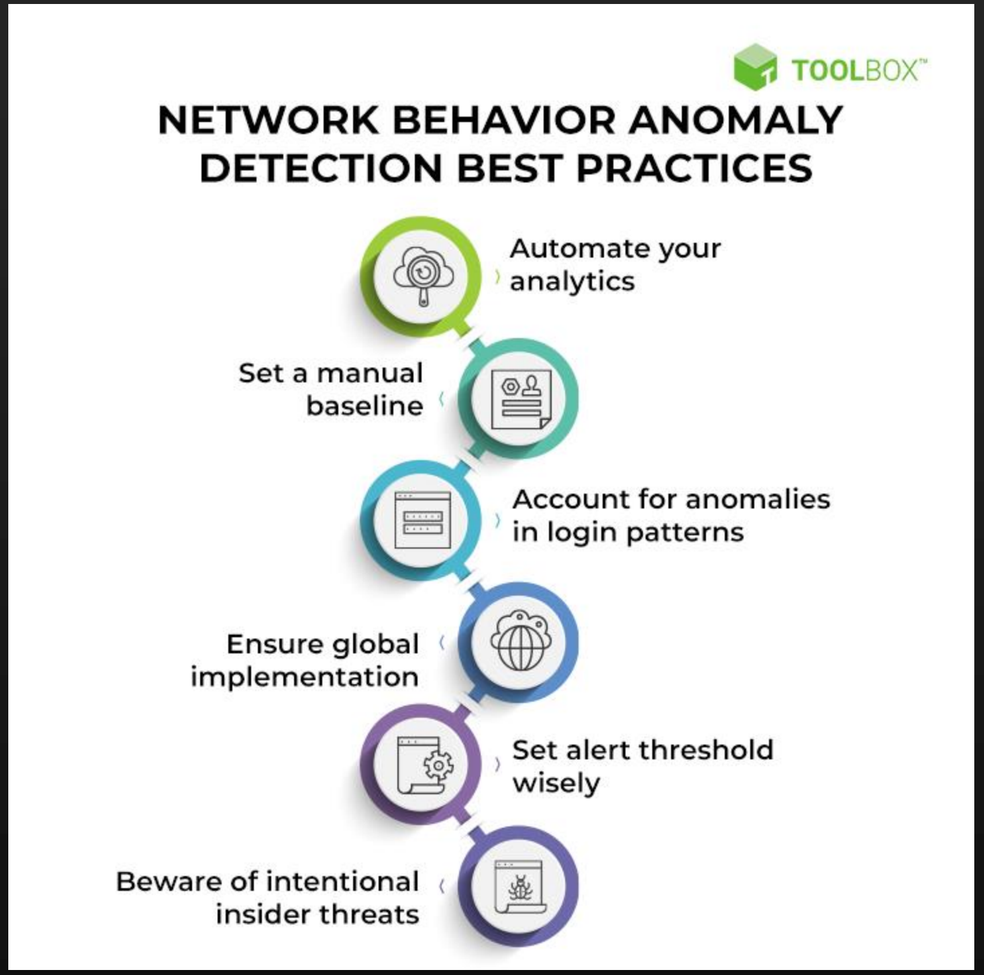


Figure 17: Endpoint security is often seen as cybersecurity's frontline and represents one of the first places organizations look to secure their enterprise networks.

ANOMALY DET BEST PRACTICES

3. Account For Anomalies In Login Patterns

Remote work is still trending in 2022 and may last until 2023. Configure your network behavior anomaly detection solution to notify yourself of outliers in login patterns, even if this is inconvenient due to the dynamic nature of remote work. Less tech-savvy employees might access the corporate network over a public Wi-Fi connection, leading to their credentials being compromised. Additionally, credentials may fall into the wrong hands due to phishing and related malicious activities. While the login patterns of some employees may lead to constant 'annoying' alerts, security teams must use network behavior anomaly detection to account for anomalies in login patterns. This is because other cybersecurity solutions might not be able to prevent cybercriminals from misusing leaked credentials.

4. Ensure Global Implementation

Network behavior anomaly detection detects covert threats anywhere on the network, as long as it has access to the entire network. If your enterprise network has a large, complex structure, ensure the network behavior anomaly detection solution is configured to reach even the most remote corners. Set up other security solutions, such as firewalls and encryption tools, to prevent them from blocking network behavior anomaly detection from reaching its full potential.

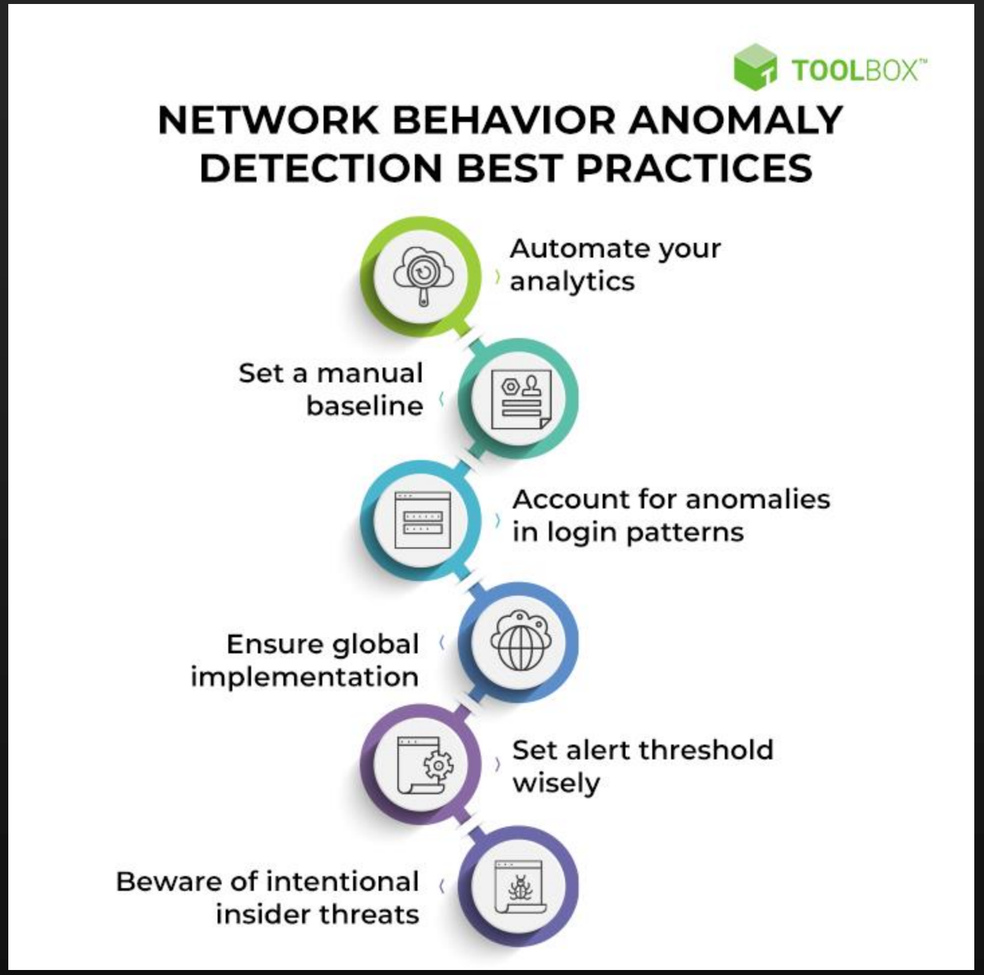


Figure 18: Endpoint security is often seen as cybersecurity's frontline and represents one of the first places organizations look to secure their enterprise networks.

ANOMALY DET BEST PRACTICES

5. Set Alert Threshold Wisely

We discussed above how disabling alerts might lead to missed threats until it's too late. Building on that, it is essential to set an alert threshold that filters out (most of) the noise without any important alerts being skipped. Threats nowadays are no longer as overt as they used to be—criminals can penetrate a corporate system and make away with sensitive information. The only hint you would have is the out-of-place behavior detected by network behavior anomaly detection. Whenever possible, give preference to examining alerts, no matter how noisy they may be, instead of ignoring them.

6. Beware Of Intentional Insider Threats

No security solution, not even network behavior anomaly detection, might be able to account for every intentional (and sometimes unintentional) action of insiders. A sufficiently crafty (or unaware) internal stakeholder with enough access privileges might be able to get away with anything. This is because network behavior anomaly detection relies on detecting anomalies based on historical data, and insiders might act with malicious intentions while performing their daily activities. Ensure measures such as awareness training and robust security policies are implemented to prevent malicious insiders from compromising the integrity of your organization.

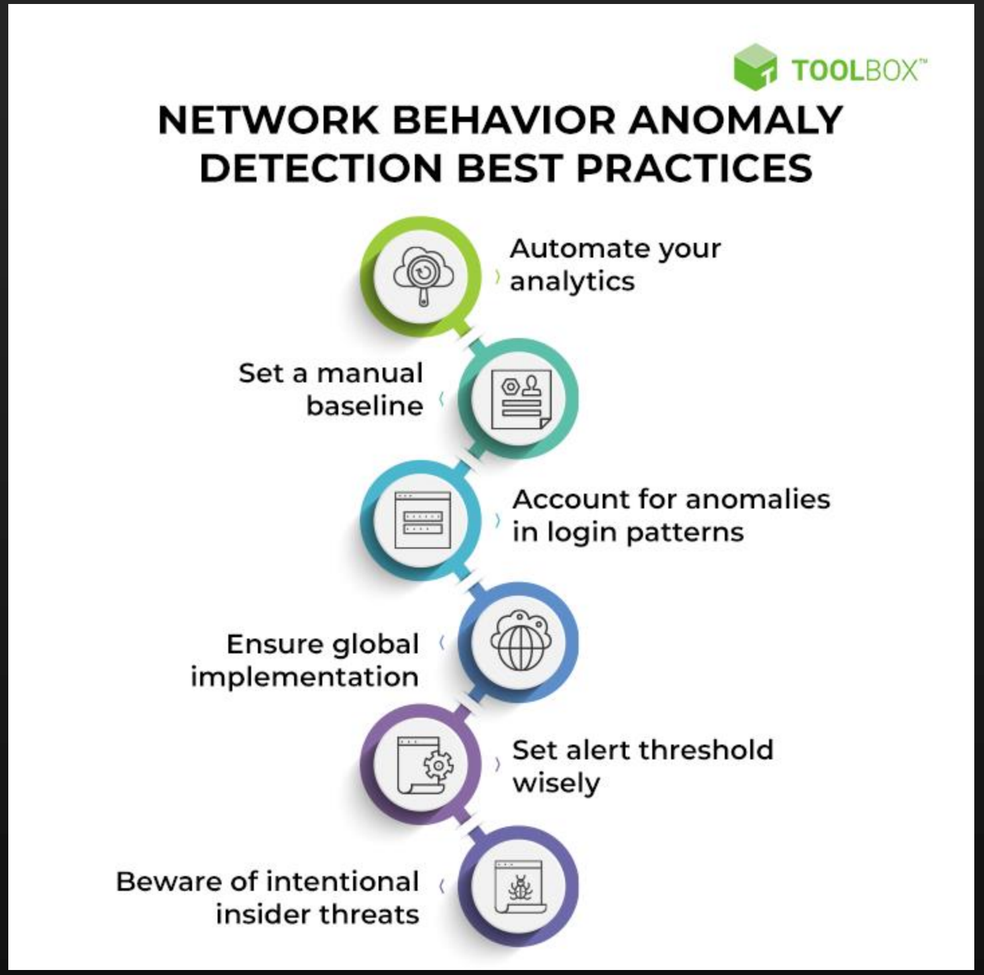


Figure 19: Endpoint security is often seen as cybersecurity's frontline and represents one of the first places organizations look to secure their enterprise networks.

ANOMALY DET BEST PRACTICES

7. Watch Out For False Positives

Networks are more dynamic in a remote work environment, blurring the distinction between normal network operations and abnormal activities. Many network behavior anomaly detection solutions rely, to a certain extent, on probability scores to define anomalies, which could lead to false positives. For instance, an unexpected system update would also transfer a large amount of data to a particular endpoint. Network behavior anomaly detection might mark this innocuous activity as an outlier. Frame your policies to acknowledge the possibility of false positives and give your security team enough authority to make a call if they detect an uncertain situation. This is an excellent alternative to forcing them to investigate every alert, which consumes resources and might divert them from the actual threats.

8. Use Metadata To Monitor Encrypted Traffic

Data encryption is widely prevalent in today's corporate landscape. While this is great from a security perspective, it can also transmit threats through encrypted communications. To prevent this, set encryption to take place at the application level. This would enable network behavior anomaly detection to perform the statistical analysis of destination ports, IP addresses, and other related metrics for incoming and outgoing encrypted communications. This way, encryption would not wholly block anomaly detection, even though it might lead to fewer anomalies being detected.

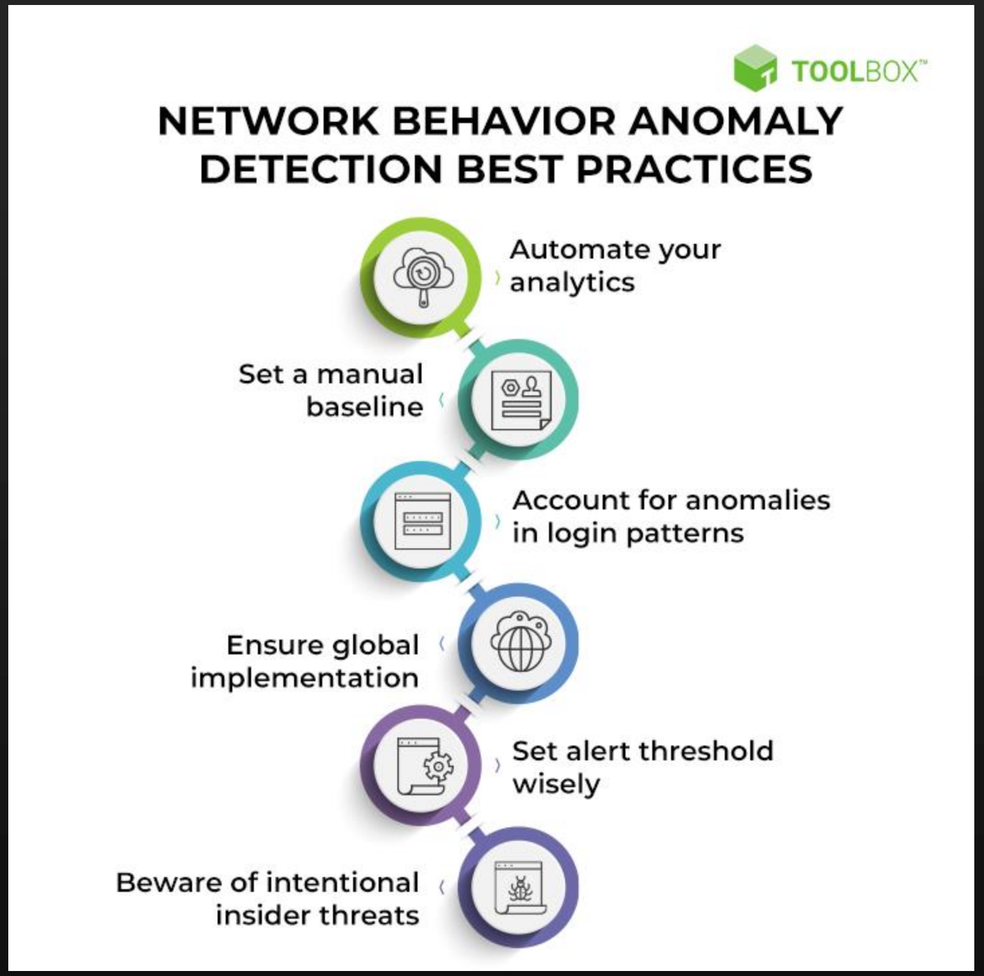


Figure 20: Endpoint security is often seen as cybersecurity's frontline and represents one of the first places organizations look to secure their enterprise networks.

ANOMALY DET BEST PRACTICES

10. Finally, Don’t Rely On Network Behavior Anomaly Detection Alone

Network behavior anomaly detection is an excellent solution for detecting and preventing cyber criminals from exploiting your network. However, it works best when combined with other security solutions.

- **Use A Firewall** to prevent known threats from entering your network
- **Use Intrusion Detection Systems (IDS)** to spot more common malicious activities
- **Use Intrusion Prevention Systems (IPS)** to prevent cyber criminals from executing known attacks
- **Use Network Access Control (NAC)** software to restrict network access to only those endpoints that comply with existing security policies

Other security tools that further boost the overall security posture include web filters, proxy servers, anti-DDoS solutions, load balancers, and spam filters.

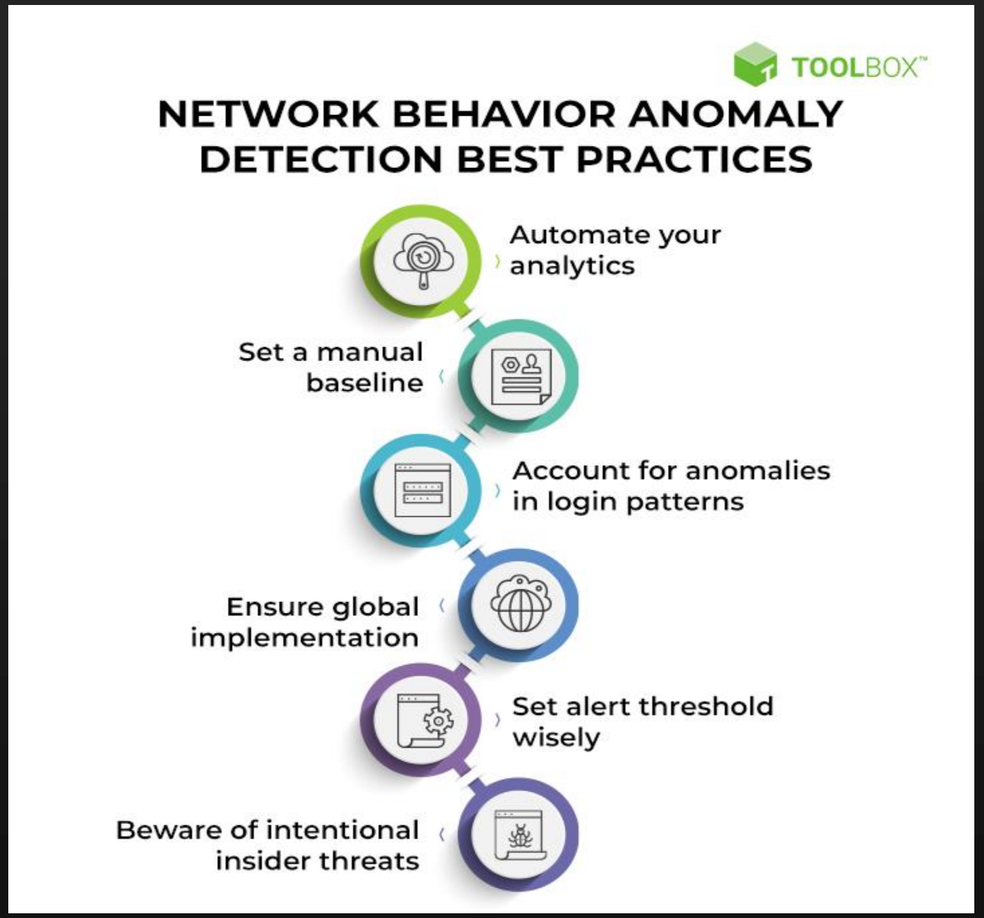


Figure 21: Endpoint security is often seen as cybersecurity's frontline and represents one of the first places organizations look to secure their enterprise networks.

ANOMALY DETECTION

TOP 10 TOOLS

ANOMALY DETECTION EPILOGUE

Product Comparison of Top 10 Network Behavior Anomaly Detection Tools in 2022

Here are the key highlights of these tools at a glance:

Solution Name	USP	Pricing	Toolbox Comments
Awake Security Adversarial Modeling	Awake can be deployed in a modular manner, which drives greater scalability.	Pricing starts at $1 per year per connected	It may not be ideal for companies that need an integrated anomaly detection and response
Cisco Stealthwatch	You can purchase the tool for a specific cloud environment. This simplifies deployment and	Pricing starts at $1,000 and may vary as per	Cisco provides one of the most informative tools in the market., However, you may face
Flowmon NBAD	It has features designed for insider threat detection through network behavior analysis.	Pricing starts at $3,625 per month for the	Flowmon is extremely feature-rich and relies on cutting-edge AI and ML. However, users have
Gurucul ML XDR	Gurucul converts correlation into causation by leveraging its big data architecture.	Pricing starts at $80 per user per year.	While Gurucul offers false-positives-free insights, adoption can be a challenge. It does not offer
IBM QRadar Network Insights	IBM complements network behavior anomaly detection with industry-leading managed	The tool offers three pricing models starting	It is a comprehensive solution and can scale effectively. However, users report a complex setup
LMNTRIX Detect	LMNTRIX can be deployed as either a virtual sensor or a physical appliance, making it easy to	Pricing for LMNTRIX is undisclosed.	LMNTRIX takes a managed service approach. Therefore, the cost may be higher than the
LogRhythm MistNet	The tool leverages a mesh computing system called TensorMist-AI™ to analyze network	Pricing for LogRhythm starts at $2.46 per GB of	While it comes with AI-based analytics, it isn't suited for standalone implementations.
NetFlow Network Anomaly Detection	NetFlow has built-in algorithms that help reduce false positives and personalize the insights.	NetFlow is available with free and paid options	It meets the needs of small and mid-sized organizations. However, it lacks the sophisticated
NetWitness Detect AI	The tool applies a dynamic statistical risk scoring model to alert users to the most urgent anomalies.	Pricing starts at $8567 per month.	The AI consumes a lot of bandwidth. Customers have also noted that the documentation could be
Zabbix Network Monitoring	Zabbix has a unique escalation feature that lets you customize alert workflows and drive	It is free to use.	Zabbix has an open architecture. However, you may face issues with auto-discovery, and large

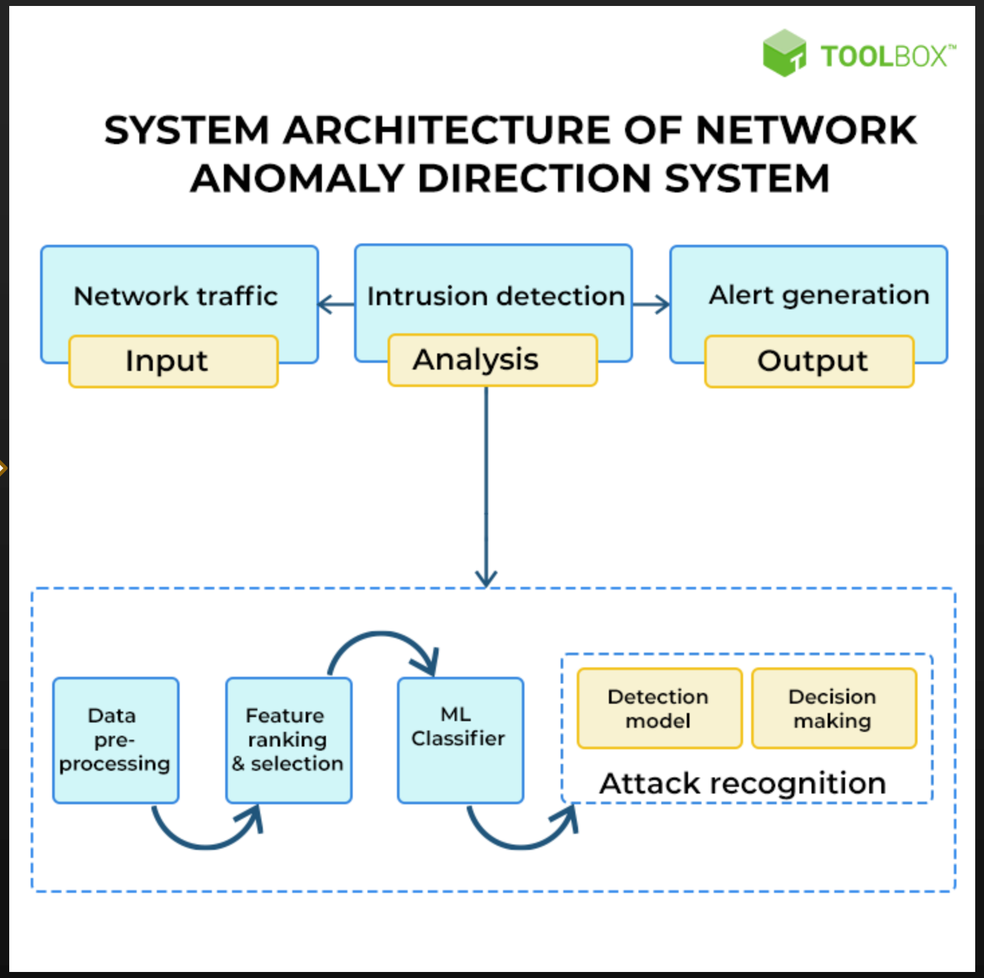


Figure 22: Anomaly Detection Tool Architecture

BASELINE

& ANOMALY DETECTION EPILOGUE

ANOMALY DETECTION EPILOGUE

Anomaly Detection's Future

Investment in network security is on the rise, and network behavior anomaly detection tools are essential for strengthening your enterprise perimeter. Particularly in the era of remote and hybrid work, these tools are more relevant than ever before.

In its State of Network Security 2021 survey, Barracuda found that 94% of employees use company-issued devices on their home internet, risking network-related attacks. 64% also direct enterprise traffic through public cloud providers.

The ten tools we discussed scan these and other network behaviors for anomalies. They raise real-time alerts for valid anomalies so that IT teams can resolve them and maintain a relentless focus on enterprise security.

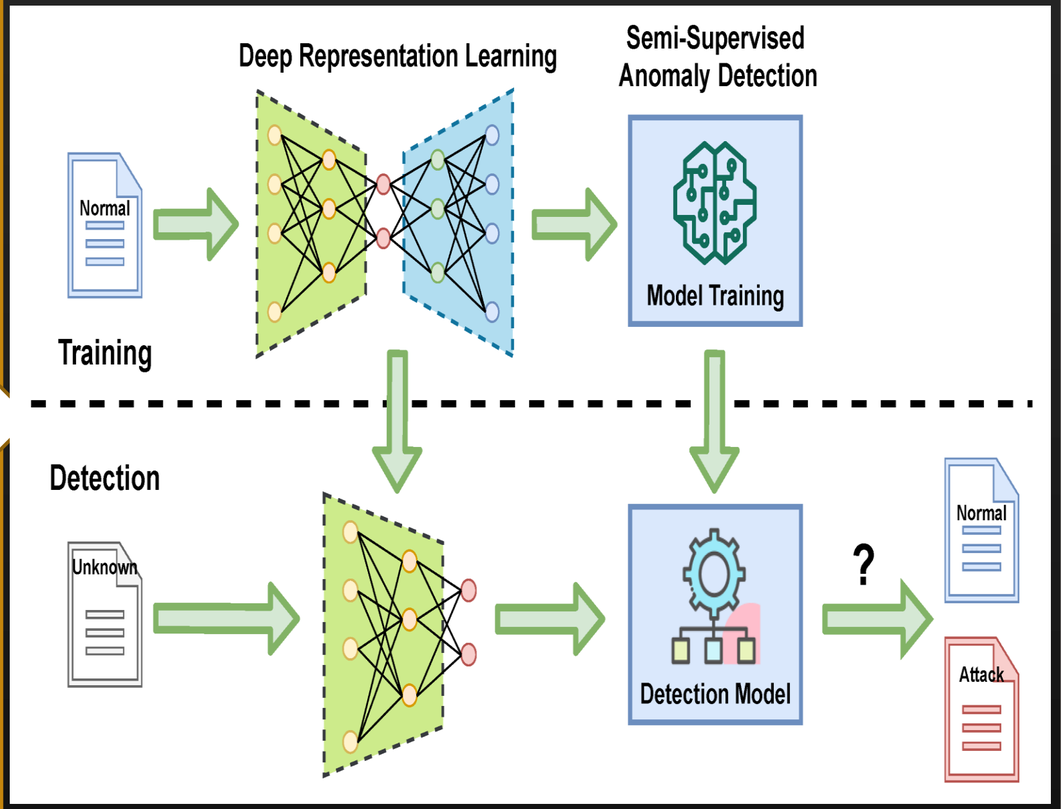


Figure 23: Investment in network security is on the rise, and network behavior anomaly detection tools are essential for strengthening your enterprise perimeter. Particularly in the era of remote and hybrid work, these tools are more relevant than ever before.

LAB Exercise

Perform the Tasks Prescribed

WHAT ARE THE THREE(3) TAKEAWAYS FROM THIS CLASS?

There are three important ways security tools detect threats. Those methods are: Signature Detection, Behavior Detection, & Anomaly Detection

Before determining something is an anomaly, you must first understand what is considered normal. This makes up the first part of any anomaly detection capability which is understanding normal behavior, a Baseline.

Detecting network behavior anomalies is part of the larger network detection and response (NDR) function. Like other security systems like firewalls or intrusion prevention software send alerts to the NDR, network anomaly data will also be processed for a speedy response.


TROUBLE
QUESTIONS
COMMENTS
DILEMMA
DOUBT
EXPRESS
UNCERTAINTY
COMMENTS
QUESTIONS
DOUBT
UNCERTAINTY
TROUBLE

QUESTIONS?