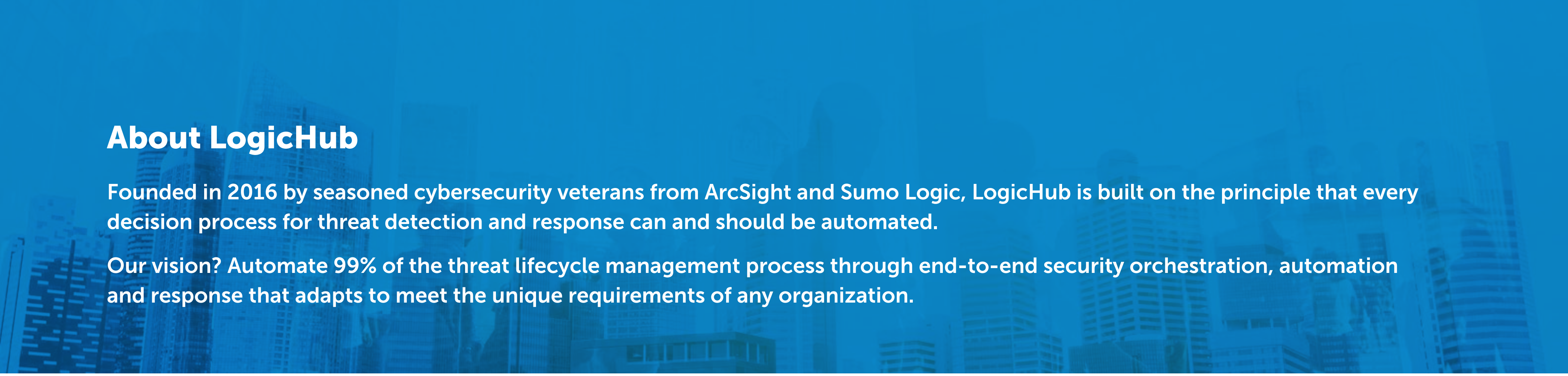
LogicHub

The Definitive Guide to AI- and Automation-Powered Detection and Response

Why Your Next SOC Assistants Are Bots *(and Your Networks Will Be More Secure Than Ever)*

Table of Contents



About LogicHub

Founded in 2016 by seasoned cybersecurity veterans from ArcSight and Sumo Logic, LogicHub is built on the principle that every decision process for threat detection and response can and should be automated.

Our vision? Automate 99% of the threat lifecycle management process through end-to-end security orchestration, automation and response that adapts to meet the unique requirements of any organization.

Meeting the challenge of today's dynamic threat landscape, bot by bot

In 2022, security teams are under more pressure than ever. They juggle the risk of cyber attacks like ransomware along with the challenges of a hybrid or entirely remote workforce, with users logging in from their homes and too many devices to count.

That means most Security Operations Centers (SOCs) are simply overwhelmed: Too much data, too many alerts and a constantly evolving threat landscape. Today's security professionals need help.

Imagine you could hire three, five or 10 assistants for every one of your security analysts and engineers. Think of LogicHub as a platform with which you can do exactly that — by building custom bots you can teach to perform tasks 10, 100 or even 1,000 times faster than people can. Plus, these bot assistants are tireless: They run 24/7.

> **Security teams need intelligent automation designed to augment three key activities of security operations: alert triage, incident response, and threat hunting.**

That means you can free up security teams to focus on the high-level work only they can do; the stuff that's difficult or impossible to automate or requires a deep, human understanding of the domain and the enterprise.

Can you level up your ability to perform triage, threat hunting, and incident response — more efficiently, cost-effectively and consistently? *See for yourself.*

By the numbers

With LogicHub's AI and automation powered detection and response, organizations can benefit from:

95% reduction in false positives

20x false alert investigations

5x better threat detection

3x boost in analyst productivity

The status quo: Gaps in threat detection

At LogicHub, we've talked to literally hundreds of security teams about how they work and the challenges they face every day. Here are just a few:

Heaps of data; *way* too many alerts

SIEM (security information and event management) technology is a first-generation approach to security operations in use for almost 20 years. If a SIEM is serving as your primary source of data, it is time to level-up.

Most enterprises deal with so much data that SIEMs can't parse with enough speed and subtlety to generate meaningful alerts. The data overwhelms the system and creates so much "noise" in the form of alerts that it's virtually impossible to "hear" the real ones.

If you've been in this business for more than a day, you know that not all alerts are created equal. A team of 10 security engineers might get 100-plus alerts, sometimes even thousands, within a 24-hour period. They simply can't keep up. Naturally, many of the alerts are never examined, triaged or investigated. Plus, it is very difficult to synthesize all these alerts when so many applications (which might include everything from Anomali to Zscaler) are in use.

In some cases, not all the data an organization deals with is available to analyze. Storage costs are skyrocketing, so many SOCs choose to upload only certain data rather than everything, so critical threats may go undetected.

False positives are a net negative

The majority of alerts teams can and do investigate are “false positives” — meaning the alert requires no real response. This is a universal issue regardless of whether the alerts are triaged by people or bots. Without intelligent automation, the sheer volume of false positives lead to the very real phenomenon of alert fatigue. Plus, tasking analysts with reviewing mostly innocuous events is an ineffective use of human resources.

Threat hunting is a luxury

Most SOCs deal with so much data that unless they proactively hunt for threats, it’s easy to miss them. But very few (probably 1% or less) of the security teams we’ve encountered have someone dedicated to threat hunting. That’s not just because they can’t free up the time — threat hunting specialists are highly skilled, highly paid, and in high demand. Threat hunting is a luxury for many businesses.

Quality and consistency may vary

The quality of your investigation and response varies depending on which member(s) of a security team handle threats. Ideally, every investigation and response should be consistent, but human error (and mixed skill levels) are inevitable.

Automation seems just out of reach

Security engineers tell us they know they’re spending a lot of time on tasks that should (and can) be automated. But all of these things often remain aspirational goals, simply because there isn’t enough time, talent, or budgetary resources to make automation happen.

Our teams are teeming with tools

To make this kind of automation work, you need to be able to integrate it with the myriad systems your business uses. We meet security teams with just five people, but those five people rely on 25 to 30 different tools. As much as 70% of their time might be used ping-ponging between different tools, trying to pull together a full picture of — instead of actually responding to — a threat.

If you need to connect the dots between a number of different systems, you're always going to have to rely on people. Which brings us to…

People are people (with limitations)

People can do *so many things* machines cannot. But they do need more time to process data. They need to take breaks; they need to sleep. They need days off and vacations.

Security, however, is a 24/7 pursuit. Attackers don't take weekends off, and you can't afford to leave your SOC unstaffed. Even if you are fortunate enough to employ an around-the-clock team, it will never be large enough to review the massive amounts of data our modern lives create. Resources are tight for most companies, so there are never enough people to meet threats pouring in at machine speeds.

Alert fatigue is real — and can be catastrophic

Alert (or alarm) fatigue is the phenomenon of becoming desensitized to alerts and either ignoring or failing to respond appropriately to such warnings. It is a common phenomenon for IT security operations and constant alarms lose attention-grabbing urgency, which robs critical alarms of the importance they deserve.

Intelligent decision automation: Playbooks FTW

Most SOC operations begin with collecting large amounts of data using a SIEM system or a security data lake (SDL). These systems may feature automation, but it is a basic, rules-based automation that does not evolve.

LogicHub's decision automation is based on a progressive learning model that adapts based on data — and the decisions, actions and techniques of expert analysts and threat hunters. As our AI learns, it applies those lessons to its future work.

That's the difference between a rules engine and a decision engine.

Let's take it from the top...

Ask an analyst: ***If you get this alert, what are the things you would do, and in what order?*** ... Their answers are a playbook — a series of steps to take to solve a problem or achieve a goal.

The process begins with gathering all the data you need to truly understand the issue at hand. And even when you bring all of the data together in one place, you have to be able to make sense of it.

Once you come to that understanding (because you have all the context you need), you must make a conclusion: whether an event (or data you're examining) presents a real threat or not. You must decide whether or not to take action, how quickly to do so and what action(s) to take.

The OODA Loop: Observe, Orient, Decide, Act

Developed by United States Air Force Colonel John Boyd, the OODA Loop describes the cycle of decision-making. Boyd applied the concept to combat operations during military campaigns, but it is now used in litigation, business, and law enforcement as well.

If we apply the OODA Loop to data-based decision making in security operations:

Observe
refers to collecting
data about an event
(typically triggered by an alert)

Orient
is making sense of
the data in context

Decide
is concluding whether
the event constitutes
a real threat

If the threat is real, the last step is to act: Notify someone, block an IP address, stop a process from executing, decommission an account — or all of these; whatever is most appropriate as a countermeasure to the threat.

Many security teams document their formal or informal playbooks on wikis. Others don't have documentation at all. People just know what to do, based on their five or 10 years of experience in security operations. We call that tribal knowledge, and tribal knowledge cannot scale.

One day, the team member with that particular tribal knowledge will quit or retire or be out sick, and their mental "playbook" walks out the door with them. **So documentation is crucial, but it's just the first step.**

Manually following that documentation could easily take 10, 15, or even 30 minutes per alert. AI can do the same task in a fraction of the time.

LogicHub's platform includes ready-to-go playbooks created by experts — which, of course, are as customizable as your needs demand. And because the actions are carried out by bots that learn progressively from your particular business circumstances, they evolve with your organization.

The ultimate decisions are up to you (humans, we mean)

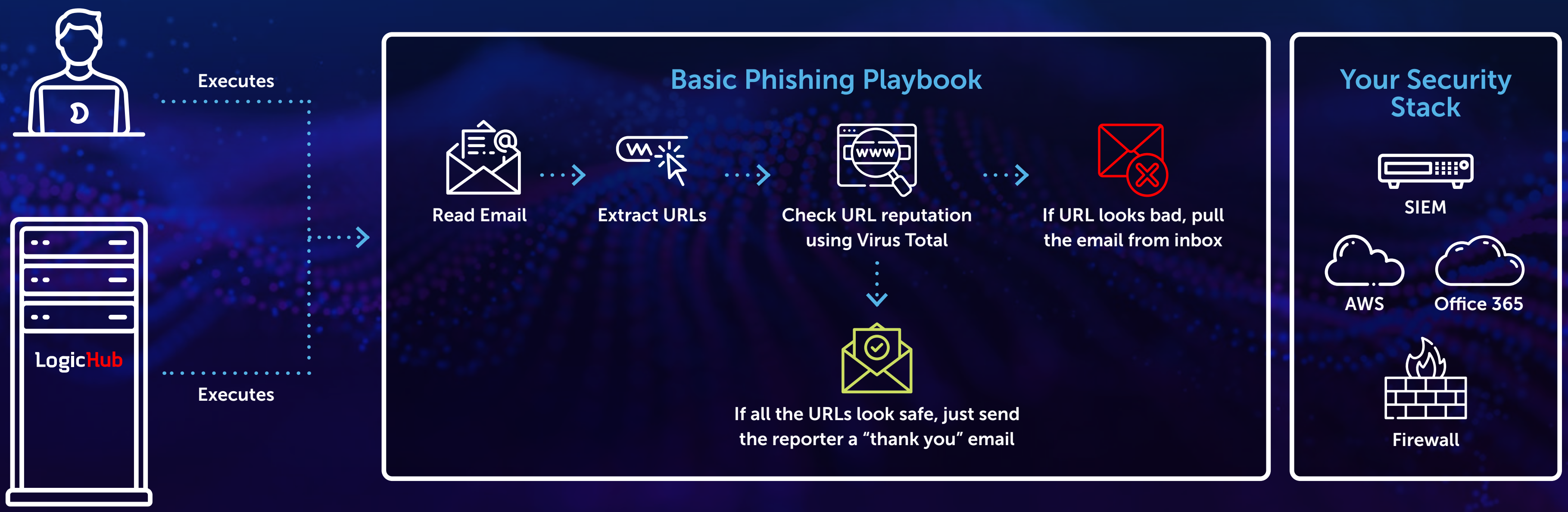
The platform can respond and take some actions automatically. For example, it can notify the SecOps or SOC team; or, raise the risk score for a particular IP address or connect to an integrated app that performs other actions, like opening a support ticket or texting a user.

There might be some actions you don't want to automatically take. We call those human-in-the-loop actions. If you're blocking a URL or an IP address, those actions can have pretty significant side effects and you need to make sure you don't do them accidentally. A human analyst is necessary to review the entire case, including the rationale for it being a critical incident and the suggested action. **But you still need the process to be easy, so LogicHub makes it possible to do in one click.**

This makes a lot of teams much more comfortable with automation. It takes time to build up confidence in automation, and one-click, human-in-the-loop actions are an ideal stepping stone. It's almost like LogicHub begins working in a supervised mode, where you can trust the automation to gather the facts and make the recommendations, but a human analyst takes the final action.

We've found that often, once security teams use the automation for two or three months, they become very comfortable with LogicHub's analysis. At any point, you can take the human out of the loop and fully automate the action.

The Playbook



Executes

LogicHub

Executes

Basic Phishing Playbook

Read Email

Extract URLs

Check URL reputation using Virus Total

If URL looks bad, pull the email from inbox

If all the URLs look safe, just send the reporter a “thank you” email

Your Security Stack

SIEM

AWS

Office 365

Firewall

The anatomy of a playbook

To build playbooks for automation, you need powerful integration with your systems. **Two kinds of integrations are crucial: 1) Pulling data together and 2) Invoking actions.**

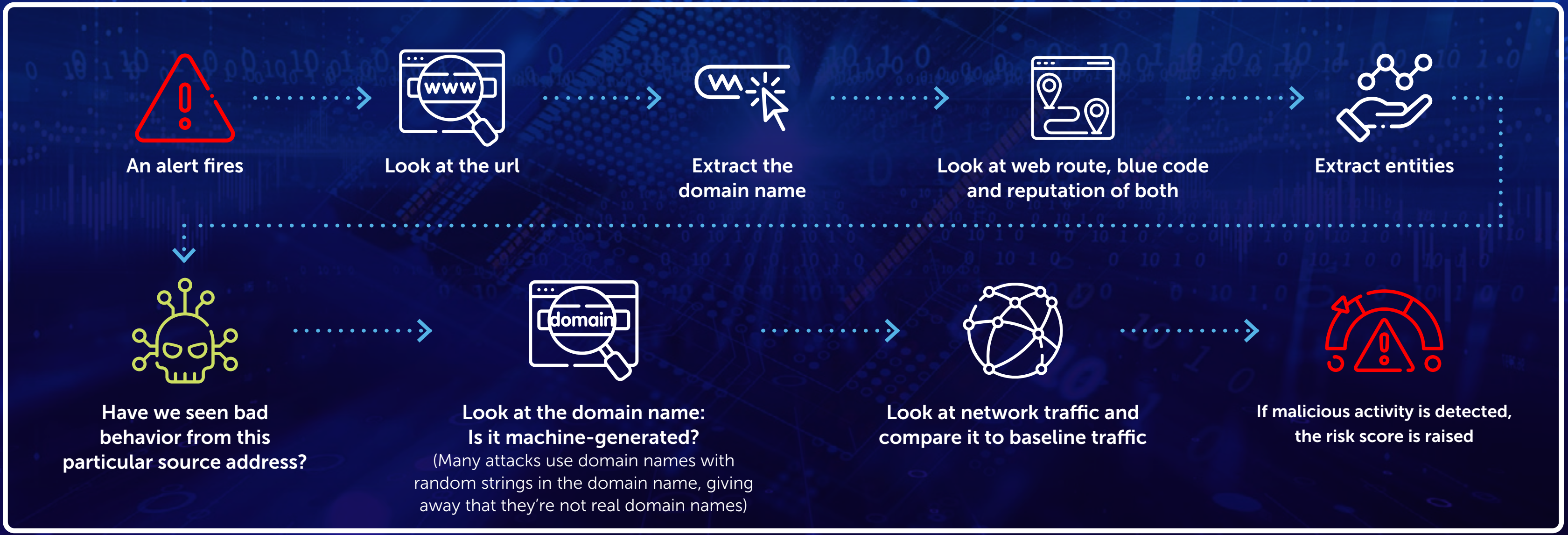
If you need to look at one set of data from one system, another set of data from a second system, and yet another set of data from the third system, you need that to be part of the playbook. The playbook will then take them all together and come up with conclusions. In response to those conclusions, you’ll want to take specific action. Some of those actions might need to take place within yet another system. Maybe you want to block an IP address or a subnet on your firewall. That’s an example of an action that can be automated.

Often, an alert looks like a garbled mess of text, which creates difficulty for an analyst to make sense of the data. This is where automation becomes a game-changer: It provides the analyst a much clearer and contextualized view. LogicHub’s platform parses and enriches the alert information with other sources of data for context, and makes a clear case, essentially telling you: *This truly is a critical incident and here’s why.*

Here’s what a very simple playbook would look like. For the sake of simplicity, this one is quite small. In reality, playbooks are anywhere from five to 50 or more steps. They might have some branches, as well.

How does it all work?

A bot is like a human analyst working continuously and immersed in analyzing data. Let's say in the last 15 minutes, 30 alerts have fired. The bot can analyze those alerts and determine that it looks like 28 out of those 30 alerts were benign — but two represent real incidents.



An alert fires

Look at the url

Extract the domain name

Look at web route, blue code and reputation of both

Extract entities

Have we seen bad behavior from this particular source address?

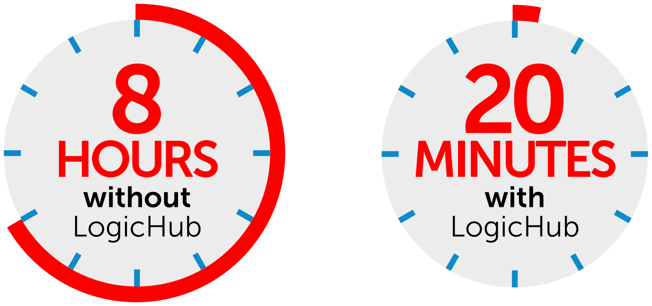
Look at the domain name: Is it machine-generated?

(Many attacks use domain names with random strings in the domain name, giving away that they're not real domain names)

Look at network traffic and compare it to baseline traffic

If malicious activity is detected, the risk score is raised

Running through playbooks like this could be someone's full-time job. Many playbooks can take days to weeks to build. With LogicHub, users can build playbooks in under 30 minutes. **And once automated, an entire day of work can shrink down to about 20 minutes.** That's how big a difference it makes.



8 HOURS without LogicHub

20 MINUTES with LogicHub

But can we trust it?

That's what we almost always hear from security teams: Great, we can automate this playbook — but how can we make sure it's doing all the right things? Yes, it can make decisions but can it really make decisions as well as we — the humans — can?

It's a very common (and reasonable!) question.

We're engineers, so we answer in a scientific way. The first thing we have to do is define the criteria for trust. **When people ask whether they can really trust the AI, we have to be able to measure the quality of its decisions.**

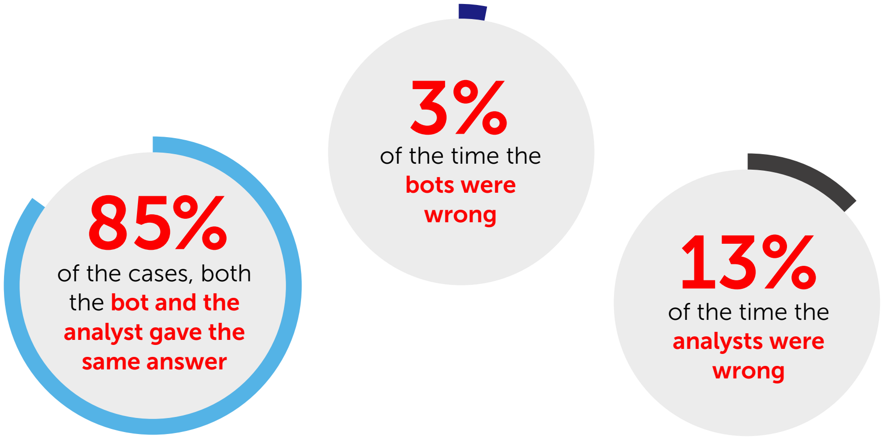
That's quite simple: Review its work, just like you'd review a junior analyst's work. You should always review how a bot is performing.

Let's say, using the previous playbook example, that among 30 alerts, two are real concerns. We can run the bot in parallel with a security analyst. The bot can do the same analysis. And at the end of the day, you can compare those 30 and ask if the bot made the same decision as the human.

The most interesting cases are where they differ because one of them is going to be right. But this allows you to come up with an accuracy metric.

What we have found is that in just a few weeks, you can build bots that are **100 times faster than human analysts** and even more accurate. One of our experiments examined 30 alerts and in about 85% of the cases, both the bot and the analyst gave the same answer. Three percent of the time the bots were wrong, and 13% of the time the analysts were wrong. The reason the analysts were wrong was that they were not carrying out the entire playbook in depth.

By defining and measuring accuracy in this way, you can make an objective decision about how much to rely on automation.



85%
of the cases, both the **bot and the analyst gave the same answer**

3%
of the time the **bots were wrong**

13%
of the time the **analysts were wrong**

Build a bot, plan the playbook

Here's the method we recommend for building a bot that carries out a playbook for decision automation. It's based on a technique called the "Five Whys," developed by the founder of Toyota Industries.

The Five Whys is a method for discovering the root cause of errors. It's simple: You repeat the question, *Why did [x problem] happen?* — until you get to the bottom of it. (The "five" is apparently the most common number of iterations needed to resolve the problem.)

To apply the Five Whys to building playbooks, an analyst looks at an alert and asks, *Is this a real incident? Is it not? Why is this a real incident or a false positive?* In their answers are the multiple factors they considered to make the determination. Some of the factors might not be available in the alert, but the analyst will often look at how some data correlate with other data to come up with a new factor. This is what we refer to as multifactor analysis. We use those factors to create an AI model leveraging a process we call feature engineering.

Our platform enriches the data around any given alert to extract the relevant features. The end output is a recommended decision.

Skilled human threat hunters can encode their techniques, capturing and turning their expertise and decision processes into scoring and decision playbooks. And because LogicHub's AI keeps learning, your automated detection and response will continuously improve.

The Five Whys

This technique was the brainchild of inventor and industrialist Sakichi Toyoda, who is often called the "Japanese Thomas Edison."

Over the course of his career in the early 20th century, he invented and innovated a number of textile weaving devices. His most famous invention was an automatic power loom, which ran on the principle of *Jidoka* (autonomous automation). *Jidoka* means that the machine stops itself when a problem occurs.

After Toyoda's death in 1930, his son went on to found the Toyota Motor Corporation, where the company fine-tuned the Five Whys as a critical component of its problem-solving training.

Taiichi Ohno, who developed the Toyota Production System with Jidoka and the Five Whys at its core, once said:

> *"The basis of Toyota's scientific approach is to ask why five times whenever we find a problem … By repeating why five times, the nature of the problem, as well as its solution, becomes clear."*

This concept is used today in Lean methodologies to solve problems, improve quality and reduce costs.

Threat hunting with the decision engine

An enterprise can collect millions of events every day. No human being can review even a tiny fraction of that manually.

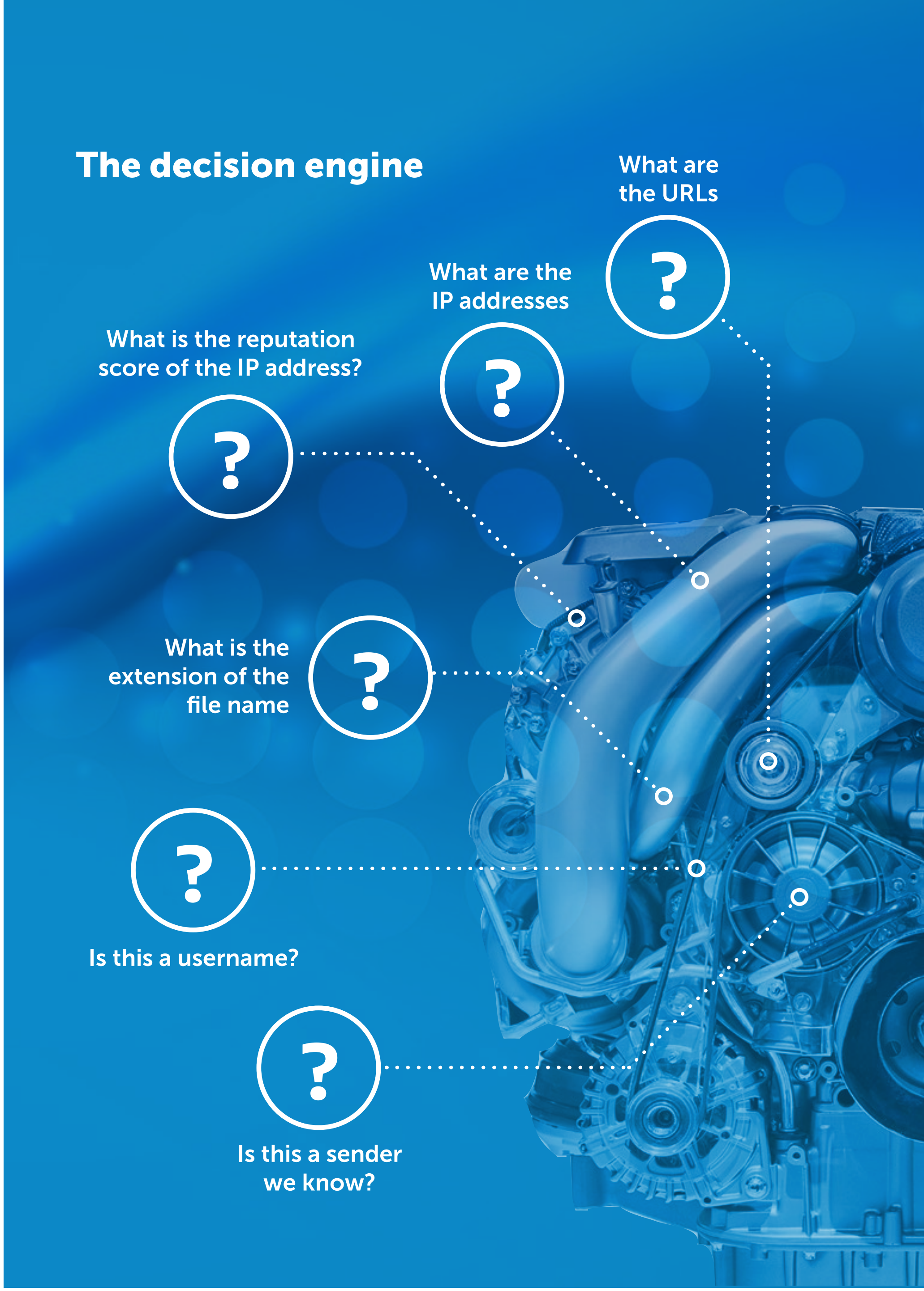
This is where automation truly shines. Because if you're looking at small amounts of data, humans perform at a high level. But as data exponentially increases, the efficacy of a human analyst decreases dramatically (and they'll need a lot more time, too).

To solve this problem, LogicHub's AI takes those 100,000 (or 100 million) data points and breaks them down into much smaller factors. For example:

- *What are the IP addresses?*
- *What are the URLs?*
- *What is the reputation score of the IP address?*
- *What is the extension of the file name?*
- *Is this a username?*
- *Is this a sender we know?*

Taking all of these factors (or more), our platform combines them into one final score. This is what we call a *decision engine*.

The decision engine



What are the URLs

What are the IP addresses

What is the reputation score of the IP address?

What is the extension of the file name

Is this a username?

Is this a sender we know?

LogicHub's AI is always learning

Every system, whether powered by humans or AI, will make errors. If nothing changes, it will keep making the same mistake again and again. The ability to incorporate feedback and be able to learn from errors is critical.

Machine learning is a distinctive feature of LogicHub's decision engine. **Our platform includes supervised machine learning, in which the AI can learn from human feedback, as well as unsupervised machine learning algorithms that can learn from data alone.**

One of the reasons SOCs have dealt with so many noisy alerts for so long is because most SIEM systems use rule engines. One of the deep flaws of a rule engine is that it is cumbersome and lacks the ability to change or apply any kind of feedback.

But LogicHub's intelligent AI hits the sweet spot: easy to operate, easy to adapt, and able to learn from feedback.

Machine learning in action

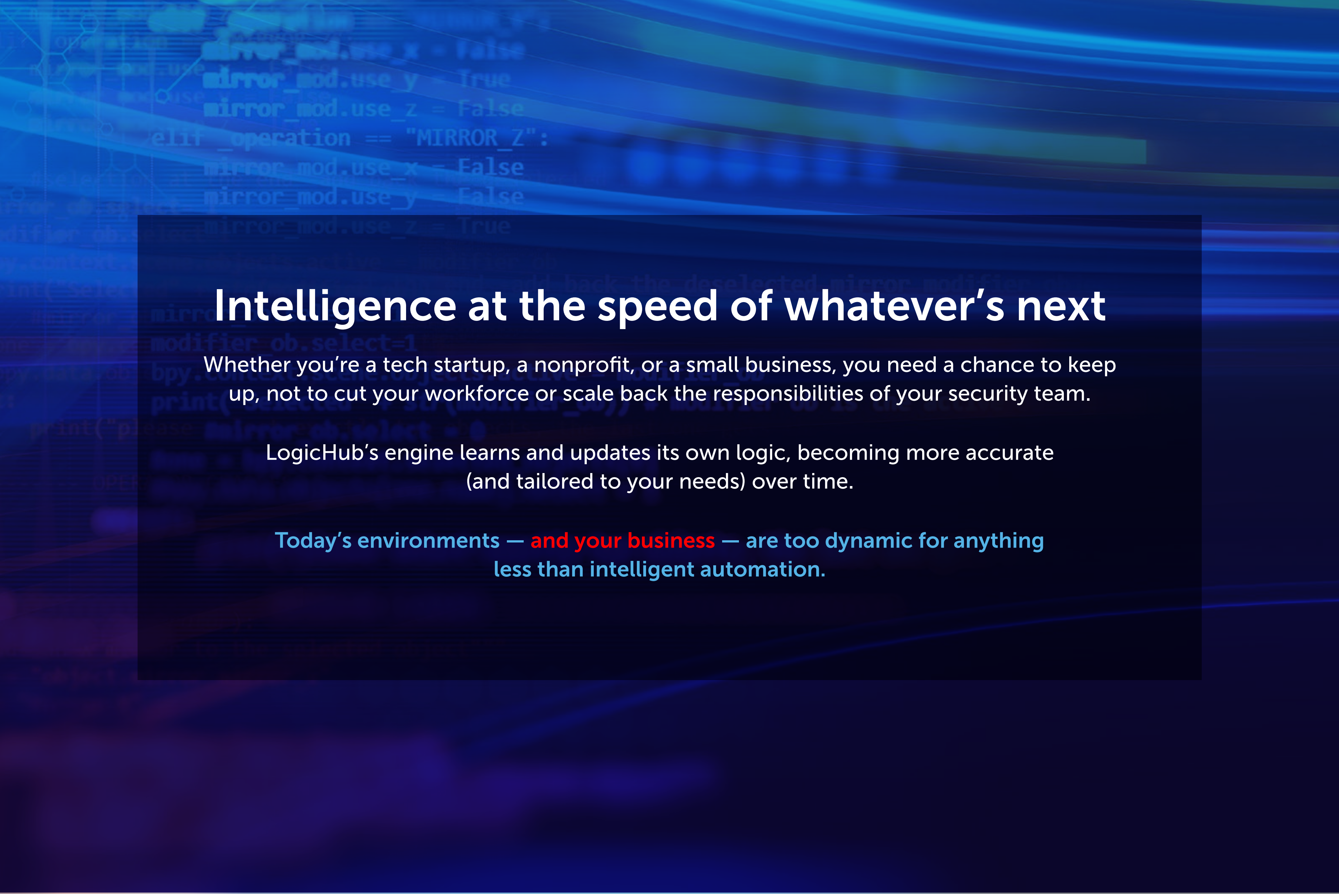
We deployed our decision engine to security operations for a client that runs its own enterprise version of GitHub. They want to protect their "crown jewel" servers, the repositories of all their IPs. Tens of thousands of developers are constantly accessing their projects on these servers.

This client's security team was overwhelmed with access logs, most of which are normal. But determining which ones were not was extraordinarily difficult. And they provide a good example of extracting the features that matter most to your business.

These access logs included the user's ID (username), their IP address and how many different IP addresses the user employed every day. LogicHub's AI found that some user IDs were logged into sessions that came from 50-plus different IP addresses. That's not physically possible for one user. It indicated that these user accounts were most likely being shared. That was a surprise to this company's security team.

The usernames did not indicate what these users' roles were in the organization. But we could profile them. We found developers who worked on the same project simply by looking at their access patterns. We could cluster users based on their behavior. So the client could see when a developer working on a particular project accessed a different project, one that no other users with similar behavior would access — which raised eyebrows and invited further investigation.

Our AI might score that last scenario as a 10, whereas 99% of the access logs are scored as a 0 or 1. Anything scored 8 or above triggers an alert that the security team should scrutinize in more detail. Because intelligent automation frees them up to investigate the ones that matter, even small or less mature SOCs can scale their efforts in ways that are commensurate with the ever-evolving threats they face.



Intelligence at the speed of whatever’s next

Whether you’re a tech startup, a nonprofit, or a small business, you need a chance to keep up, not to cut your workforce or scale back the responsibilities of your security team.

LogicHub’s engine learns and updates its own logic, becoming more accurate (and tailored to your needs) over time.

Today’s environments — and your business — are too dynamic for anything less than intelligent automation.