GPT-3 Outputs

Copy-pasted results of prompts I gave to the model. Each model output is in a new color.

As the world moves increasingly online, securing your company from digital threats has become essential. A strong cybersecurity program can mean the difference between weathering the storm and being brought to your knees by a cyberattack.

But where do you start? There are a lot of factors to consider when building a cybersecurity program, and it can be difficult to know where to begin. In this blog post, we'll discuss the three pillars of a strong cybersecurity program.

One way to think about automating security is to consider it in the same way that you would any other business process. By identifying the inputs, outputs, and key steps in the process, you can start to map out how best to automate it. The same is true for security policies. Rather than writing a separate policy for each individual system, it's much more efficient to write one policy that can be applied across the board. This will not only save you time in the long run, but it will also help to ensure compliance with industry regulations.

In order to maintain visibility across all of your company's cloud environments, you need to have a centralized system in place that can track and monitor activity. This system should be able to provide you with real-time alerts so that you can quickly identify and respond to any potential incidents. Additionally, it's important to have a team in place that is dedicated to monitoring the system and responding to any alerts. By having this visibility in place, you can help to prevent incidents before they happen.

In the event of an incident, you need to be able to rely on your systems to provide suggestions for remediation that are both smart and context-aware. This means having a system in place that can quickly identify the root cause of the problem and provide a recommended course of action. Additionally, the system should be able to adapt its recommendations based on the specific circumstances of the incident. By having a system like this in place, you can minimize the impact of incidents and get your business back up and running as quickly as possible.

Edits

Light touch editing for style, adding a conclusion and an industry expert quote for good measure.

As the world moves increasingly online, securing your company from digital threats has become essential. A strong cybersecurity program can mean the difference between weathering the storm and being brought to your knees by a cyberattack.

But where do you start? There are a lot of factors to consider when building a cybersecurity program, and it can be difficult to know where to begin. In this blog post, we'll discuss the three pillars of a strong cybersecurity program.

One way to think about automating security is to consider it in the same way that you would any other business process. By identifying the inputs, outputs, and key steps in the process, you can start to map out how best to automate it. The same is true for security policies. Rather than writing a separate policy for each individual system, it’s much more efficient to write one policy that can be applied across the board. This will not only save you time in the long run, but it will also help to ensure compliance with industry regulations.

In order to maintain visibility across all of your company's cloud environments, you need to have a centralized system in place that can track and monitor activity. This system should be able to provide you with real-time alerts so that you can quickly identify and respond to any potential incidents. Additionally, it's important to have a team in place that is dedicated to monitoring the system and responding to any alerts. By having this visibility in place, you can help to prevent incidents before they happen.

In the event of an incident, you need to be able to rely on your systems to provide suggestions for remediation that are both smart and context-aware. This means having a system in place that can quickly identify the root cause of the problem and provide a recommended course of action. Additionally, the system should be able to adapt its recommendations based on the specific circumstances of the incident. By having a system like this in place, you can minimize the impact of incidents and get your business back up and running as quickly as possible.

Final

It’s bland, but that’s fine! This whole process took <1 hour.

As the world moves increasingly online, securing your company from digital threats has become essential. A strong cybersecurity program can mean the difference between weathering the storm and being brought to your knees by a cyberattack.

But where do you start? There are many factors to consider when building a cybersecurity program, and it can be difficult to know where to begin. In this blog post, we'll discuss the three pillars of a strong cybersecurity program.

Define once, use many policies

One way to think about automating security policies is to consider them in the same way that you would any other business process. By identifying the inputs, outputs, and key steps in the process, you can start to map out how best to define and automate them. The same is true for security policies. Rather than writing a separate policy for each individual system, it’s much more efficient to write one policy that can be applied across the board. This approach creates efficiency within your security regime, making your policy more easily adopted by developers and other technical users.

Centralized visibility

In order to maintain visibility across all of your company's cloud environments, you need to have a centralized system in place that can track and monitor activity. This system should be able to provide you with real-time alerts so that you can quickly identify and respond to any potential incidents. No matter the system you choose to fill this roll, you should prioritize alerting that is proactive, sufficiently detailed, and actionable Additionally, it's important to have a team in place that is dedicated to monitoring the system and responding to any alerts. By having this visibility in place, you can help to prevent incidents before they happen.

Proactive remediation

In the event of an incident, you need to be able to rely on your systems to provide suggestions for remediation that are both smart and context-aware. This means having a system in place that can quickly identify the root cause of the problem and provide a recommended course of action. Additionally, the system should be able to adapt its recommendations based on the specific circumstances of the incident. Art Vandelay, CISO of Vandelay Industries says, “While we ultimately chose Snyk to secure our cloud environments, intelligent remediation was a top-of-mind feature throughout the whole RFP process.”

However you structure your cloud security program, focusing on automation, visibility and proactive remediation should be at the forefront of every CISO’s must-have list. The Snyk cloud security platform is built on these foundational principles. Get in touch today for a demo.