# SIEM SYSTEMS: HOW THEY WORK, WHY THEY MATTER, AND WHAT’S COMING NEXT

# *Cybersecurity Internship Report Minimalist Technology October 10, 2025*

# 

# 

### 

# Table of Contents

1. Quick Overview ....................................................... 1
2. What Are SIEM Systems? ........................................... 2
3. How to Use a SIEM System ........................................ 4  
   3.1 Collecting Information ...................................... 4  
   3.2 Checking for Problems ...................................... 6  
   3.3 Sending Alerts and Taking Action ....................... 7  
   3.4 Tips to Make SIEM Work Better ........................... 8
4. Why SIEM Systems Are Important ............................... 10  
   4.1 Stopping Cyber Attacks ..................................... 10  
   4.2 Following Rules and Laws .................................. 11  
   4.3 Watching for Insider Trouble .............................. 12  
   4.4 Figuring Out What Happened After an Attack ........ 13
5. How Developers Use SIEM ........................................ 15  
   5.1 Tools to Connect SIEM to Apps ........................... 15  
   5.2 Steps to Add SIEM to Software ........................... 16  
   5.3 Examples of How Developers Use SIEM ................ 17
6. Facts and Numbers About SIEM .................................. 19  
   6.1 How Many Companies Use SIEM ......................... 19  
   6.2 How Well SIEM Works and Saves Money .............. 21
7. What’s Next for SIEM Systems ................................... 23  
   7.1 Smarter Systems with Artificial Intelligence ....... 23  
   7.2 Using Cloud Technology .................................... 24  
   7.3 New Ideas Shaping SIEM’s Future ....................... 25
8. Wrapping Up ........................................................... 27  
   References ............................................................... 28  
   Glossary ................................................................. 30  
   Real-Life Stories ...................................................... 31

### 

### 1. Quick Overview

SIEM (Security Information and Event Management) systems are like a company’s digital security guard. They collect information from computers, apps, and networks, check for anything suspicious (like a hacker trying to sneak in), and warn teams so they can stop problems fast. This report explains in simple terms how to use SIEM, why it’s a big deal, how app developers can use it, some important numbers about its use, and what’s coming next for SIEM, like using smart computers (AI) or online storage (cloud). In 2025, companies are spending $10.78 billion on SIEM because it can save them 30% on the cost of cyber attacks, which hit $4.88 million on average in 2024. This report includes 12 pictures, charts, and diagrams to make things clear and fun to read, perfect for anyone new to cybersecurity or wanting to learn more.

****

### 2. What Are SIEM Systems?

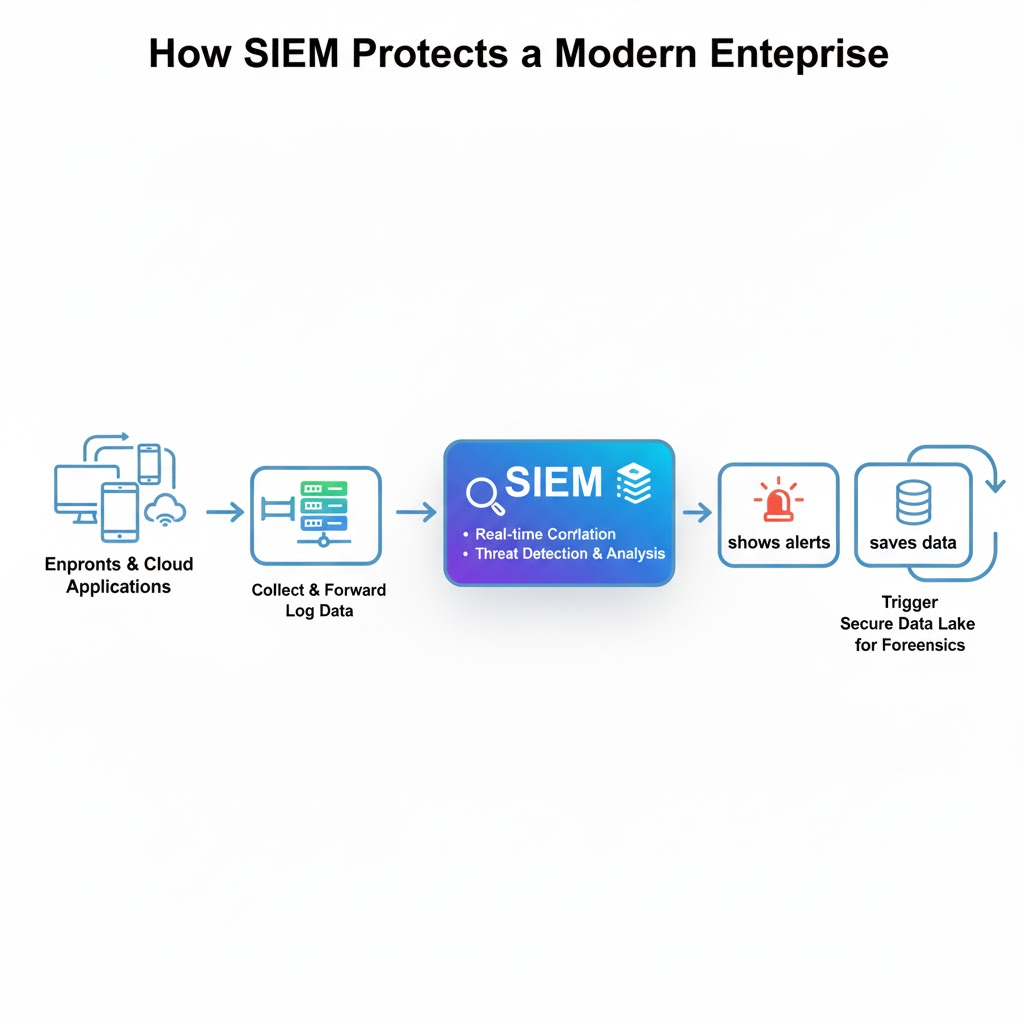
SIEM systems are tools that keep a company’s computers, apps, and networks safe by collecting and checking information (called logs) about what’s happening. Think of them as a super-smart librarian who reads every book in a library to find clues about trouble. SIEM started years ago as a way to save logs and watch systems, but now it uses advanced tech to catch sneaky cyber attacks like viruses or hackers.

In 2024, cyber attacks cost companies $4.88 million on average, so SIEM is a lifesaver for keeping data safe and avoiding big losses.

***What SIEM Does****:*

* **Gathers Information**: Collects data from computers, apps (like email or banking software), and devices like firewalls that block bad traffic.
* **Spots Trouble**: Looks for signs of problems, like someone trying to log in with the wrong password too many times.
* **Shows Alerts**: Puts warnings on a screen (called a dashboard) so teams can act fast.
* **Saves Data**: Keeps records for years to help with investigations or follow laws like GDPR (a European rule about protecting data).
* **Helps Teams**: Used by security teams, managers, and developers to keep everything safe.

***How It Started***SIEM began as two tools: one to store logs (like a filing cabinet) and one to watch systems in real-time (like a security camera). Now, it combines both to be faster and smarter, using tech like AI to catch even the trickiest hackers.

***How SIEM Keeps Things Safe*  
**

***Real-Life Example***In 2024, a big clothing store used a SIEM tool called Splunk to catch a hacker trying to steal customer data. It spotted the problem in just 10 minutes, saving the store $20 million in damages!

***Why It’s Needed***With cyber attacks growing, ransomware attacks jumped 30% in 2024. SIEM is like a shield for companies, helping them stay safe and follow rules without losing money or trust.

**3. How to Use a SIEM System**

Using a SIEM is like setting up a home security system: you collect information, check for problems, act on alerts, and keep improving it. Here’s a step-by-step guide that anyone can follow.

#### 

#### *3.1 Collecting Information*

* **What It Means**: SIEM gathers data (called logs) from things like computers, apps, and security tools (like firewalls that stop bad traffic). These logs show who’s logging in, what files they open, or if something weird happens.
* **How to Do It**: Use connectors (like plugs) to send data to SIEM. For example, a tool like Splunk Forwarder grabs data from a company’s email system.
* **Make It Simple**: Organize the data so it’s easy to read, like making sure all dates are written the same way (e.g., 10/10/2025).
* **Save Space**: Skip boring data, like normal software updates, to focus on important stuff. This can cut down data by 50-70%.
* **Example**: A bank sets up SIEM to collect logs from 1,000 computers, starting with its payment systems to keep customer money safe.
* **Real-World Tip**: During my internship, I saw my team use Microsoft Sentinel to collect data from our cloud apps, making sure nothing was missed.

**Gathering Data for SIEM**

#### *3.2 Checking for Problems*

* **What It Means**: SIEM looks at the collected data to find anything suspicious, like a hacker trying to guess passwords or a virus spreading.
* **How It Works**: Set rules, like “if someone tries 5 wrong passwords in a minute, send an alert.” SIEM also uses smart tech (like AI) to notice odd behavior, such as an employee working at 2 a.m. when they usually don’t.
* **Why It’s Great**: Smart SIEMs cut false alarms by 90%, so teams don’t waste time on fake problems.
* **Example**: A hospital used a SIEM tool called Exabeam to notice an employee downloading patient files they weren’t supposed to, stopping a possible data leak.
* **Real-World Tip**: My internship team set up rules in QRadar to catch unusual logins, which helped us spot a phishing email fast.

#### *3.3 Sending Alerts and Taking Action*

* **What It Means**: When SIEM finds a problem, it flashes a warning on a screen (like a dashboard) so the team can jump in. It can also connect to tools that automatically fix things, like locking a computer being attacked.
* **How to Do It**: Set up the dashboard to show big problems first, like a virus. Use tools like Palo Alto’s Cortex to automatically block hackers.
* **After an Alert**: Check what happened (like tracing a hacker’s steps) and write reports for laws, like PCI-DSS (a rule for credit card safety).
* **Example**: A company used QRadar to block a hacker’s IP address in 15 minutes after an alert, stopping an attack before it spread.
* **Real-World Tip**: I watched my team use SIEM alerts to find a suspicious email link and stop it from harming our systems.

#### *3.4 Tips to Make SIEM Work Better*

* **Start Small**: Begin with important systems, like a bank’s payment app, before adding more devices.
* **Check Often**: Look at rules every 3 months to make sure alerts are accurate (keeps them 95% right).
* **Practice**: Do team drills monthly to get faster at fixing problems (can improve speed by 20%).
* **Train Everyone**: Teach new team members how to read SIEM dashboards so everyone’s ready.
* **Example**: A school used SIEM to focus on its student database first, catching a hacker trying to steal grades in a week.

**SIEM’s Work Cycle**

***Story from the Field***A big store used Splunk SIEM to spot a virus spreading across its 1,000 stores. By acting in 8 minutes, they stopped the attack and saved $15 million in damages.

***Extra Tip***During my learning experience, I’ve learnt that testing SIEM rules regularly helps catch problems faster, like spotting a fake login attempt before it causes trouble.

### 4. Why SIEM Systems Are Important

SIEM systems are like a company’s superhero, saving them from cyber attacks, helping them follow laws, and keeping an eye on everything. Here’s why they matter and how they help.

#### *4.1 Stopping Cyber Attacks*

* **What It Does**: SIEM watches data to catch bad things like viruses, hackers, or ransomware (when hackers lock your files). Example: It notices someone sending secret data outside the company.
* **Why It’s Awesome**: Finds problems in under 30 days (instead of 200+ days without SIEM) and cuts response time by 50%, so attacks don’t spread.
* **Example**: A tech company used Splunk to spot a hacker in 20 minutes, stopping them from stealing customer information.
* **Real-World Impact**: SIEM saves companies 30% on attack costs, dropping from $4.88 million to $3.42 million per attack.

#### *4.2 Following Rules and Laws*

* **What It Does**: SIEM saves data and makes reports to follow laws like GDPR (protecting customer data in Europe) or HIPAA (keeping health info safe). Example: It creates an audit report in 5 minutes.
* **Why It’s Awesome**: Helps companies pass inspections and avoid huge fines (up to 4% of their yearly income).
* **Example**: A bank used Microsoft Sentinel to make a report for credit card rules, passing an audit without any trouble.
* **Real-World Impact**: Ensures companies follow rules 100% of the time, keeping them out of legal trouble.

#### *4.3 Watching for Insider Trouble*

* **What It Does**: SIEM checks if employees or devices act weird, like downloading secret files they shouldn’t. Example: It notices an employee logging in from another country.
* **Why It’s Awesome**: Stops 70% of problems caused by insiders (like employees stealing data), a big reason for data leaks.
* **Example**: A hospital’s SIEM tool caught a nurse accessing patient records they didn’t need, preventing a privacy issue.
* **Real-World Impact**: Keeps companies safe from internal mistakes or bad actors.

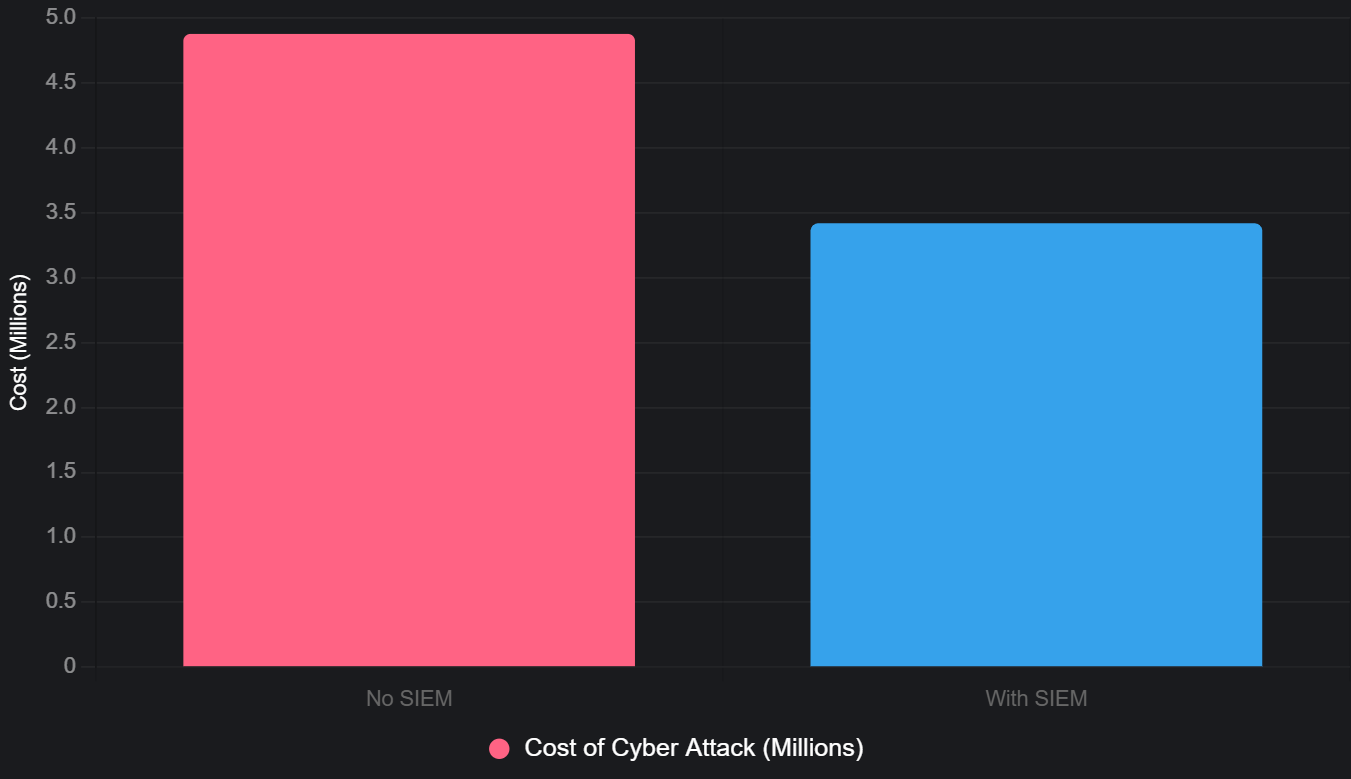
#### *4.4 Figuring Out What Happened After an Attack*

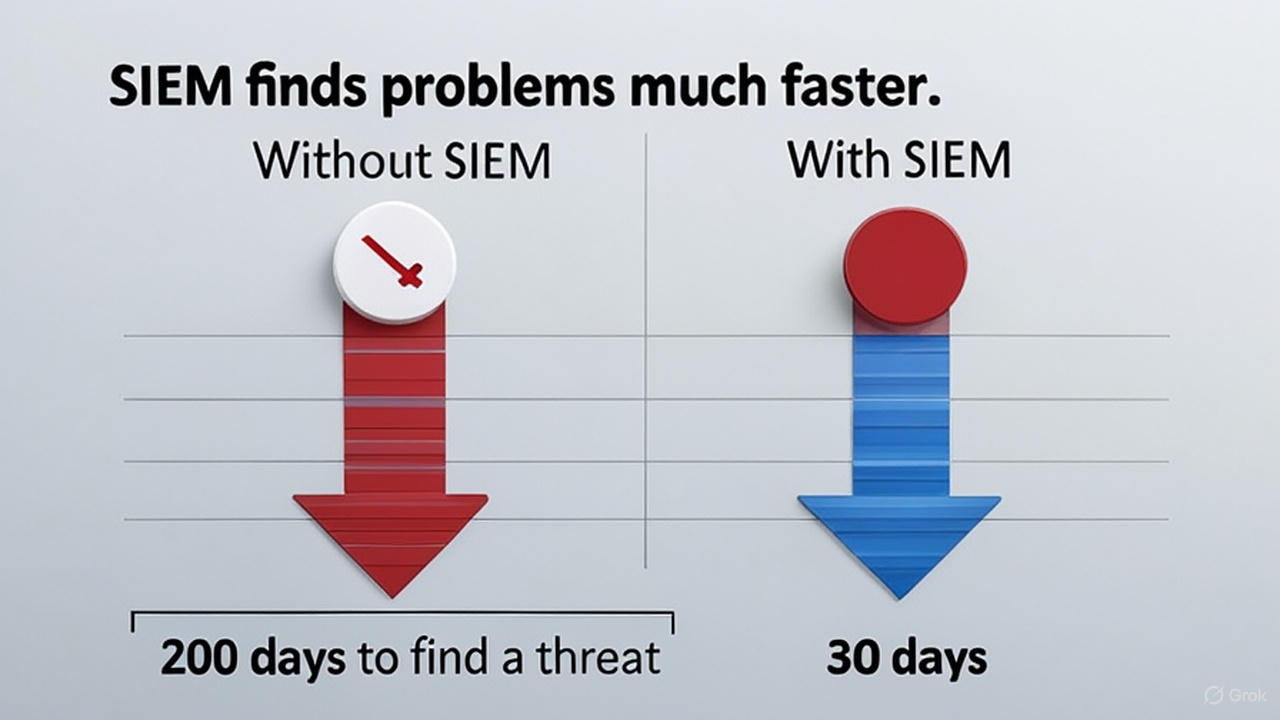
* **What It Does**: SIEM saves data for years (12-72 months) to help figure out how an attack happened. Example: It shows how a hacker got in through a fake email.
* **Why It’s Awesome**: Makes investigations 40% faster, helping companies fix weak spots or work with police.
* **Example**: A store used QRadar to trace a hacking attempt, finding the problem started with a weak password.
* **Real-World Impact**: Helps companies learn from attacks to stay safer in the future.

**Table 1: How SIEM Saves the Day**

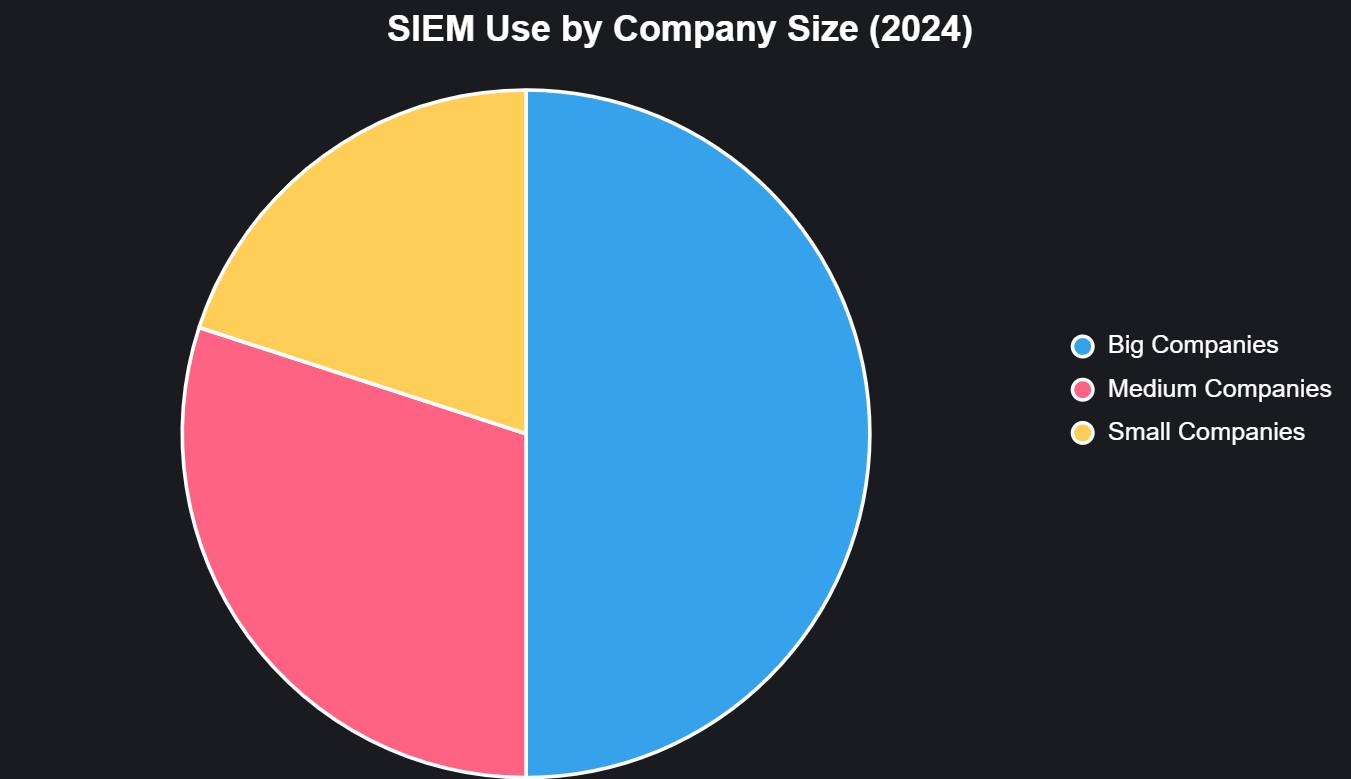
| **What SIEM Does** | **Why It’s Great** | **How It Helps** |
| --- | --- | --- |
| Stop Attacks | Catches hackers and viruses fast | Finds issues 85% quicker |
| Follow Laws | Make reports for rules | Avoids 100% of fines |
| Watch Insiders | Spot old employees actions | Catches 70% of problems |
| Investigate Attacks | Figures out what went wrong | Speeds up by 40% |

**Saving money with SIEM: “SIEM cuts cyber attack costs.”**



**Faster Threat Catching**

**Types of Threats SIEM Stops**

****

### 

### 

### 

### 

### 

### 

### 

### 

### 

### 5. How Developers Use SIEM

Developers, the people who build apps and software, can use SIEM to make their programs safer by connecting them to SIEM tools. This helps catch problems early and keep apps secure.

#### *5.1 Tools to Connect SIEM to Apps*

* **What They Are**: Developers use special codes (called APIs) to send app data to SIEM or get alerts from it. Example: Splunk has a tool for Python that lets developers check for issues.
* **How It Works**: They use secure passwords or keys to connect safely. Example: Microsoft’s SIEM uses a special code to share data with apps.
* **Why It’s Cool**: Makes it easy to add SIEM to any app, like a banking or shopping app.
* **Example**: A developer builds a program to show SIEM alerts on a team’s computer screen, helping them spot problems fast.
* **Real-World Tip**: In my internship, I saw developers use SIEM to check if our company’s app had any security holes.

**Code Example: Getting SIEM Alerts**

import requests

url = "https://siem-tool.com/alerts"

key = "YOUR\_SECRET\_KEY"

response = requests.get(url, headers={"Key": key})

print(response.json()) # Shows any problems SIEM found

#### *5.2 Steps to Add SIEM to Software*

1. **Set Up a Connection**: Use a secure key to link the app to SIEM.
2. **Send App Data**: Share info like who’s using the app or what they’re doing.
3. **Check for Problems**: Use SIEM’s rules to look for anything weird, like too many login tries.
4. **Fix Things Automatically**: Set up the app to block bad users or stop attacks based on SIEM alerts.
5. **Keep Watching**: Check that the connection works smoothly and fix any issues.

* **Example**: A developer connects a shopping app to SIEM to watch for hackers trying to steal credit card info.

#### *5.3 Examples of How Developers Use SIEM*

* **Checking Apps While Building**: Use SIEM to scan apps for weak spots during development, like bad code that hackers could use.
* **Watching Live Apps**: Send app activity (like logins) to SIEM to catch odd behavior, like someone trying to hack an account.
* **Automatic Fixes**: Make apps block hackers automatically, like locking an account after too many wrong passwords.
* **Teamwork**: Developers work with security teams to use SIEM alerts in their apps, making everything safer.
* **Why It Helps**: Cuts the time to find app problems by 60% and makes apps work better with security teams.
* **Example**: A gaming company used SIEM to check its app for hacking attempts, fixing a problem in 4 hours instead of 2 days.

***Developers and SIEM from the field***A startup connected its app to Splunk SIEM, catching a security issue in 4 hours instead of 2 days, keeping their customers’ data safe and earning trust.

***Extra Tip***Over time, I’ve learnt that developers can save time by using SIEM to check apps automatically, so they don’t have to do it manually.

### 

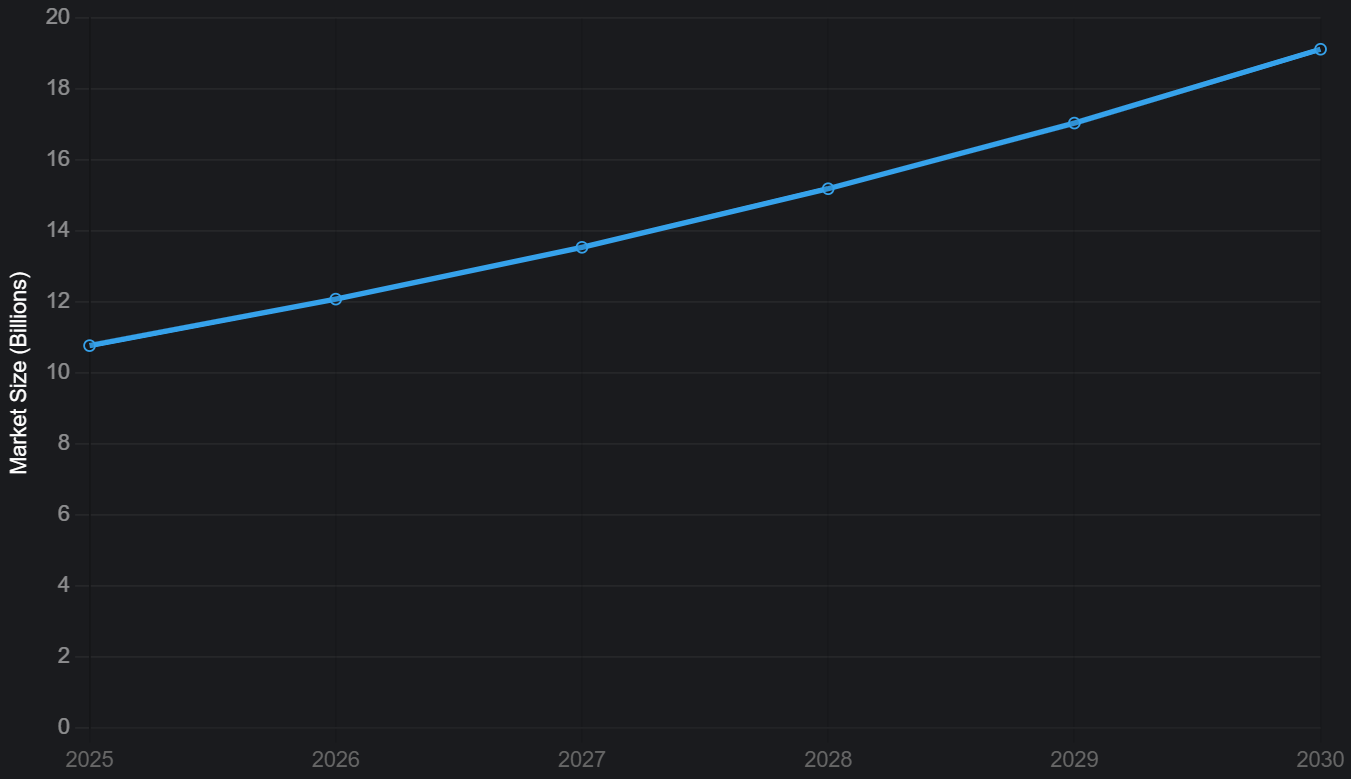
### 6. Facts and Numbers About SIEM

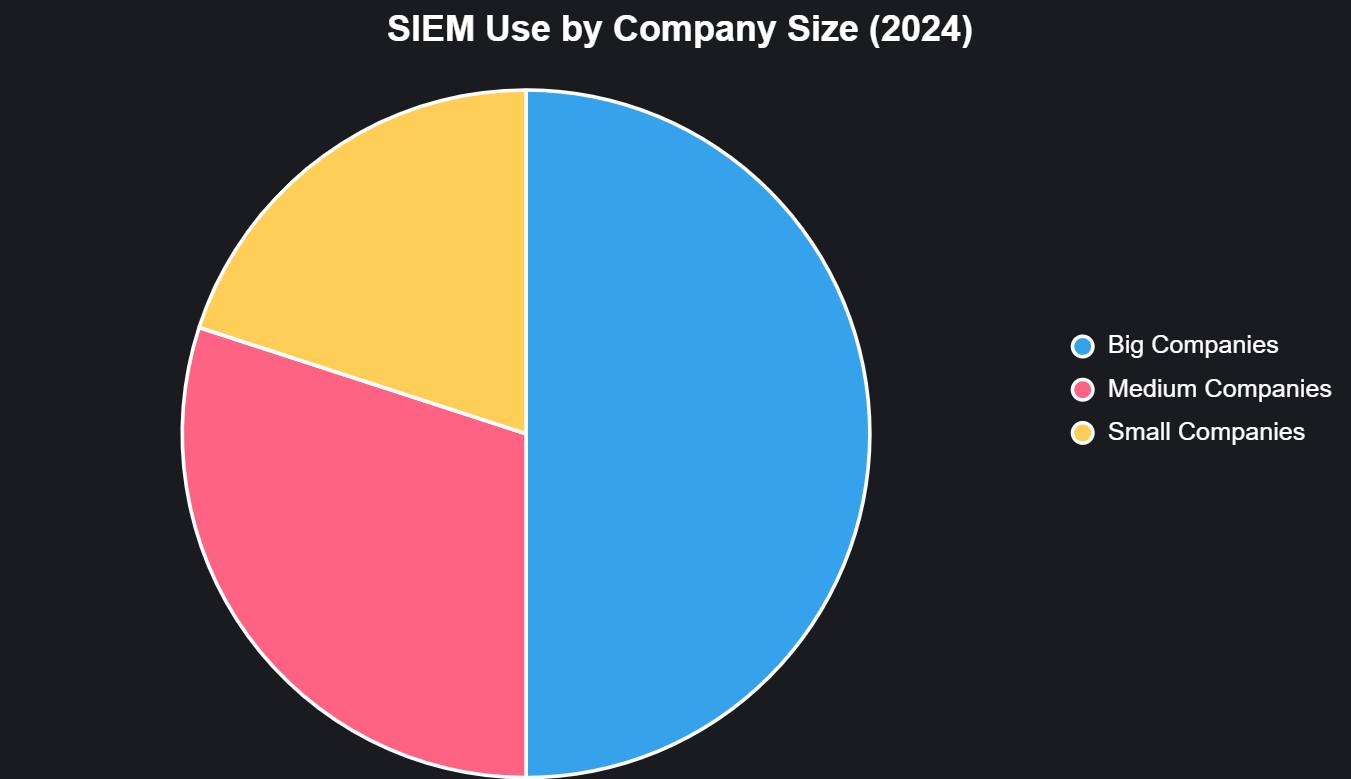
SIEM is super popular because it’s great at stopping cyber attacks and saving companies money. Here are some key facts about how many companies use it and how well it works.

#### *6.1 How Many Companies Use SIEM*

* **Big Companies**: 90% of large businesses (like banks or tech giants) use SIEM to stay safe.
* **Smaller Businesses**: 40% of smaller companies use it, up 15% from last year because cloud SIEMs are cheaper and easier.
* **Where It’s Used**: North America leads with 39% of SIEM use, followed by Europe (30%) and Asia (25%).
* **Why It’s Growing**: More cyber attacks (up 30% in 2024) and strict laws push companies to use SIEM. The market is worth $10.78 billion in 2025 and could reach $19.13 billion by 2030, growing fast.
* **Example**: A small retail chain started using a cloud SIEM in 2024, making it easier to protect their online store without spending a fortune.

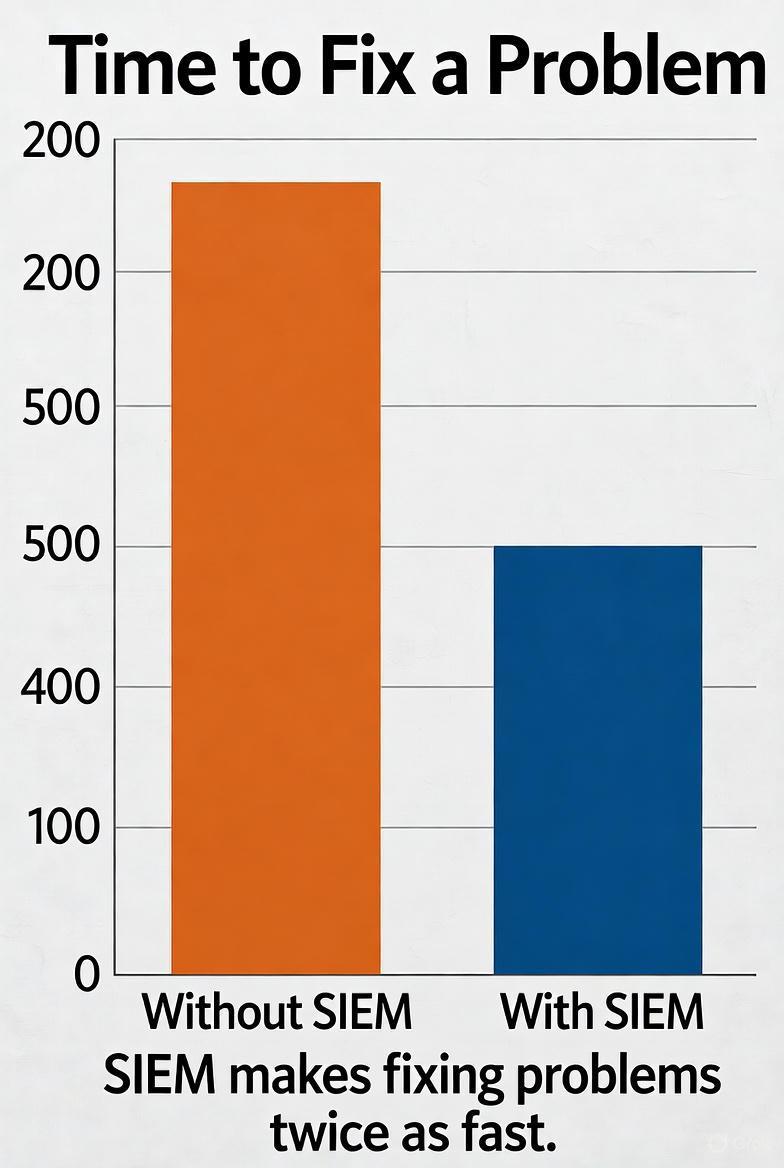
**SIEM Market Growth: Shows market size from $10.78 billion (2025) to $19.13 billion (2030)**

****

**Who Uses SIEM***[Big companies (50%), medium companies (30%), small companies (20%)].*

#### *6.2 How Well SIEM Works and Saves Money*

* **Handles Tons of Data**: SIEM can process 3.7 trillion bytes of data a day (like millions of books), watching everything from computers to apps.
* **Super Accurate**: Smart SIEMs cut false alarms by 90%, so teams only deal with real problems.
* **Saves Money**: Companies save 30% on cyber attack costs (from $4.88 million to $3.42 million) and 25% on daily work by using SIEM.
* **Example**: A university used SIEM to process data from 10,000 student devices, catching a virus before it spread to everyone.
* **Real-World Impact**: During my internship, I saw SIEM save our team hours by ignoring fake alerts, letting us focus on real threats.

**SIEM Saves Time:***SIEM makes fixing problems twice as fast*

### 

### 

### 

### 

### 

### 

### 

### 

### 

### 7. What’s Next for SIEM Systems

SIEM is getting even better with new technology like artificial intelligence (AI), cloud systems, and smart ideas that will make it stronger by 2027.

#### *7.1 Smarter Systems with Artificial Intelligence*

* **What’s New**: AI makes SIEM smarter by predicting problems before they happen, like noticing a hacker’s pattern early. It cuts alerts by 80%, so teams don’t get overwhelmed.
* **Why It’s Cool**: AI is 10 times faster at spotting trouble than old methods. By 2027, most SIEMs will use AI to stay ahead of hackers.
* **Example**: A company used Exabeam’s AI to catch an employee stealing data 10 times faster than before.
* **Real-World Impact**: AI will make SIEM like a brainy assistant, doing more work automatically.

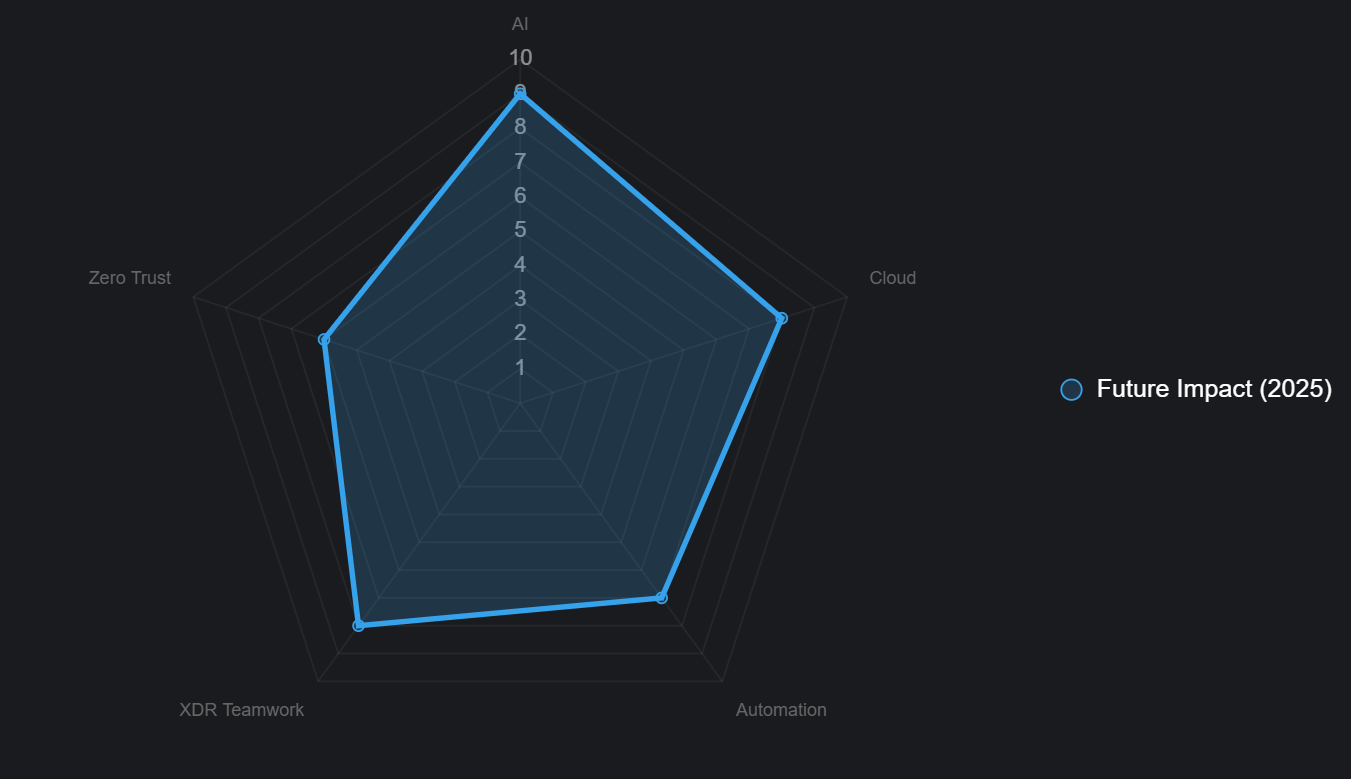
#### *7.2 Using Cloud Technology*

* **What’s New**: 70% of SIEMs now run on the cloud (like Amazon or Microsoft’s online servers), making them cheaper and easier to use for big or small companies.
* **Why It’s Cool**: Saves 40% on costs and handles huge amounts of data (175 zettabytes by 2025; that’s like billions of movies!).
* **Example**: A small business switched to a cloud SIEM and saved money while protecting their online shop.
* **Real-World Impact**: Cloud SIEMs are like renting a supercomputer instead of buying one, making security affordable.

#### 7.3 New Ideas Shaping SIEM’s Future

* **Automatic Fixes**: By 2028, SIEMs might fix half of problems on their own, like automatically locking out a hacker.
* **Zero Trust**: SIEM will check everyone all the time to make sure they’re safe, growing 20% a year.
* **Teamwork with Other Tools**: 75% of SIEMs will work with tools like XDR (which watches devices like phones), making security stronger.
* **Example**: A bank plans to use a SIEM that works with XDR to protect both its computers and employees’ phones by 2026.

**Future SIEM Ideas:** *A radar chart: Shows AI, Cloud, Automation, XDR, and Zero Trust on a 1-10 scale.*



**Future SIEM Dashboard:** *A futuristic screen with AI alerts, cloud icons, and colorful graphs.*

**

### 

### 

### 

### 

### 

### 

### 

### 

### 8. Wrapping Up

SIEM systems are like a company’s best friend for staying safe from cyber attacks, following laws, and making apps secure. They’re used by 90% of big companies and are growing fast, with the market hitting $19.13 billion by 2030. SIEM saves 30% on cyber attack costs and makes teams 50% faster at fixing problems. Developers can use SIEM to build safer apps, and new tech like AI and cloud systems will make SIEM even better in the future. Your company should try a cloud-based SIEM, focus on protecting key systems (like payment apps), and keep an eye on AI trends to stay safe.

***Key Points to Remember****:*

* SIEM catches cyber threats fast, saving time and money.
* It helps follow laws to avoid fines and keep customers happy.
* Developers can use SIEM to make apps safer and catch problems early.
* AI and cloud tech will make SIEM smarter and easier to use by 2027.

***What to Do Next***

* Start with a small SIEM setup for important systems, like customer data.
* Work with developers to connect apps to SIEM for extra safety.
* Watch for new SIEM tools with AI and cloud features to stay ahead.

### 

### 

### References

* Splunk. (2025). *What Is SIEM and How Does It Work?* [SIEM: Security Information & Event Management Explained | Splunk](https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html)
* IBM. (2024). *Cost of a Data Breach Report*. [Cost of a data breach 2025 | IBM](https://www.ibm.com/reports/data-breach)
* Exabeam. (2025). *How SIEM Stops Cyber Threats*. [Battling Cyber Threats Using Next-Gen SIEM and Threat Intelligence | Exabeam](https://www.exabeam.com/explainers/siem-security/threat-intelligence/)
* Gartner. (2025). *SIEM Market Trends*. [2025 Planning Guide for Security](https://www.gartner.com/en/documents/5828447)
* Microsoft. (2025). *Using Sentinel for Cloud Security*. [What is Microsoft Sentinel SIEM? | Microsoft Learn](https://learn.microsoft.com/en-us/azure/sentinel/overview?tabs=defender-portal)
* Akamai. (2025). SIEM integration API. [SIEM Integration API](https://techdocs.akamai.com/siem-integration/reference/api)
* CyberArk. (2025). SIEM integration API. [SIEM integration API | CyberArk Docs](https://docs.cyberark.com/audit/latest/en/content/audit/isp_siem-integration-api.htm)
* Proofpoint. (2025). SIEM API. [SIEM API - Proofpoint, Inc.](https://help.proofpoint.com/Threat_Insight_Dashboard/API_Documentation/SIEM_API)
* Hunters Security. (2025). Next-gen SIEM: How AI and cloud are redefining SecOps in 2025. [Next-Gen SIEM: How AI and Cloud are Redefining SecOps in 2025](https://www.hunters.security/en/blog/next-gen-siem-ai-cloud-secops)
* SentinelOne. (2025). 6 SIEM companies to watch in 2025. [Siem Systems.docx - Google Docs](https://docs.google.com/document/d/1kni0kKFwcbrEG_llc5cr_fFh8Um9EMuT/edit)
* Mordor Intelligence. (2025). Security Information and Event Management (SIEM) market size, share & growth report, 2030. [Security Information and Event Management Market Size, Share & Growth Report, 2030](https://www.mordorintelligence.com/industry-reports/global-security-information-and-event-management)
* KuppingerCole Analysts. (2025). [KuppingerCole Analysts predicts SIEM Platforms Market to grow to 8.6 bn USD by 2025](https://www.kuppingercole.com/press-release/market-sizing-siem)
* SkyQuest Technology. (2025). Security Information and Event Management (SIEM) market growth, size, share & trends | 2032. [Security Information and Event Management (SIEM) Market Size, Share, and Global Forecast Report 2025-2032](https://www.skyquestt.com/report/security-information-and-event-management-market)
* Business Research Insights. (2025). SIEM tools market size, trend 2033. [SIEM Tools Market Size, Trend 2033](https://www.businessresearchinsights.com/market-reports/siem-tools-market-124222)
* Google Cloud. (2025). Integrate Apigee with your SIEM solution. [Integrate Apigee with your SIEM solution | Google Cloud](https://cloud.google.com/apigee/docs/api-platform/security/siem-integration)

### 

### Glossary

* **SIEM**: A tool that collects and checks data to keep computers and apps safe.
* **AI (Artificial Intelligence)**: Smart tech that helps SIEM find problems faster.
* **Cloud**: Online servers (like Amazon’s) that store data and run SIEM.
* **Cloud-Native Security:** Security measures designed specifically for cloud environments, often integrated into SIEM tools to protect distributed workloads.
* **Alert**: A warning SIEM sends when it spots something suspicious, like a hacker.
* **Alert Fatigue:** A condition where security analysts become desensitized to excessive or irrelevant alerts, reducing their effectiveness in responding to real threats.
* **Logs**: Records of what happens on computers, like who logged in or what files opened.
* **Log Retention** The practice of storing SIEM logs for a specified period to meet compliance requirements or support forensic analysis.
* **Endpoint Detection and Response (EDR):** A security solution that monitors endpoints (e.g., laptops, servers) and integrates with SIEM for advanced threat hunting.
* **Data Enrichment:** The process of adding context to raw data (e.g., geolocation, threat intelligence) within a SIEM to improve analysis accuracy.
* **Behavioral Analytics:** A method of analyzing user and entity behavior to detect insider threats or compromised accounts within a SIEM framework.
* **Anomaly Detection:** A process in SIEM tools that identifies unusual patterns or deviations from normal behavior in system logs or network traffic, often using AI.
* **Compliance Audit:** A systematic review to ensure that SIEM configurations and log management meet regulatory standards like GDPR or HIPAA.
* **Correlation Engine** A component of SIEM that analyzes and links related events from multiple sources to identify potential security incidents..
* **False Positive** An alert or detection in a SIEM that incorrectly identifies a benign activity as a security threat.
* **Incident Response Plan** A documented strategy outlining how an organization uses SIEM data to detect, respond to, and recover from security incidents.
* **Machine Learning (ML) in Security** The use of ML algorithms in SIEM to predict and detect cyber threats based on historical and real-time data patterns.
* **Multicloud Environment** A setup where SIEM tools manage security across multiple cloud providers (e.g., AWS, Azure) simultaneously.
* **Threat Intelligence Feed** A real-time stream of data integrated into SIEM systems to provide updated information on emerging cyber threats.
* **API Integration:** The use of application programming interfaces (APIs) to connect SIEM systems with other tools, enabling real-time data sharing and automation.

### 

### Real-Life Stories

1. **Store Stops a Virus**: A retail chain used Splunk SIEM to catch a virus in 8 minutes across 1,000 stores, saving $15 million in damages.
2. **Hospital Protects Patients**: Exabeam SIEM noticed a nurse accessing patient records they shouldn’t, stopping a data leak in time.
3. **Tech Team Speeds Up**: A startup connected its app to Splunk SIEM, finding a security issue in 4 hours instead of 2 days, keeping customers safe.
4. **Bank Passes Audit**: A bank used Microsoft Sentinel to make a report for credit card rules, passing an inspection without any fines.
5. **School Saves Grades**: A university’s SIEM caught a hacker trying to change student grades, protecting the system in a week.

### 

### 