Sparsh Kulshrestha
/usr/bin/id

- CTI & THREAT HUNT FOR A CYBERSECURITY VENDOR
- OFFENSIVE SECURITY ENTHUSIAST, VAPT & BUG BOUNTIES
- FOSS ENTHUSIAST, LIKES BUILDING OFFSEC RELATED TOOLS
- SPEAKER @ BSIDES AHMEDABAD, BSIDES SINGAPORE, C0C0N

🌐 dotdotslash.in

in /in/sparshkulshrestha

𝕏 @dotdotslash_

m @dotdotslash@mastodon.social

ARE WE WINNING OR LOSING THE WAR AGAINST HACKERS?

AT&T's data breaches affect "nearly all" of its customers, and many more non-customers

Budget, budget everywhere, but no cyber funds in sight!

As per industry reports, India saw a significant surge in cyber attacks, with a 46% year-over-year increase. Indian organizations encountered an average of 3,201 attacks per week.

Data of 750 million telecom users in India being sold on dark web, cyber experts claim

A massive security breach has exposed the personal data of 750 million telecom users in India, with the data being sold on the dark web, according to cybersecurity firm CloudSEK.

Why?

- SECURITY OFTEN SEEN AS A COST.
- OPEN SOURCE: FREE BUT COMPLEX TO IMPLEMENT AND MANAGE.
- COMMERCIAL SOLUTIONS: HIGH COST, LIMITED ACCESSIBILITY.
- REDUNDANT IN-HOUSE EFFORTS ACROSS ORGANIZATIONS.

The Firewall Project

OPEN SOURCE, SHIFT-LEFT, SECURITY PLATFORM

What?

Platform

Firewall Secrets

Manages and protects sensitive data

Firewall SCA

Ensures security compliance and standards

Firewall ASM

Monitors and manages application security

Getting Started – Deployment

- **DOCKER COMPOSE**

- **CLOUD MARKETPLACES**

- **CFT AND HELM**

Platform Configuration

- **SOURCE - SCM/CLOUD**

- **WEBHOOKS**

- **SSO & RBAC**

- **ALERTS - SLACK/JIRA**

Understanding the UI/UX

- **DASHBOARDS**
- **ASSETS**
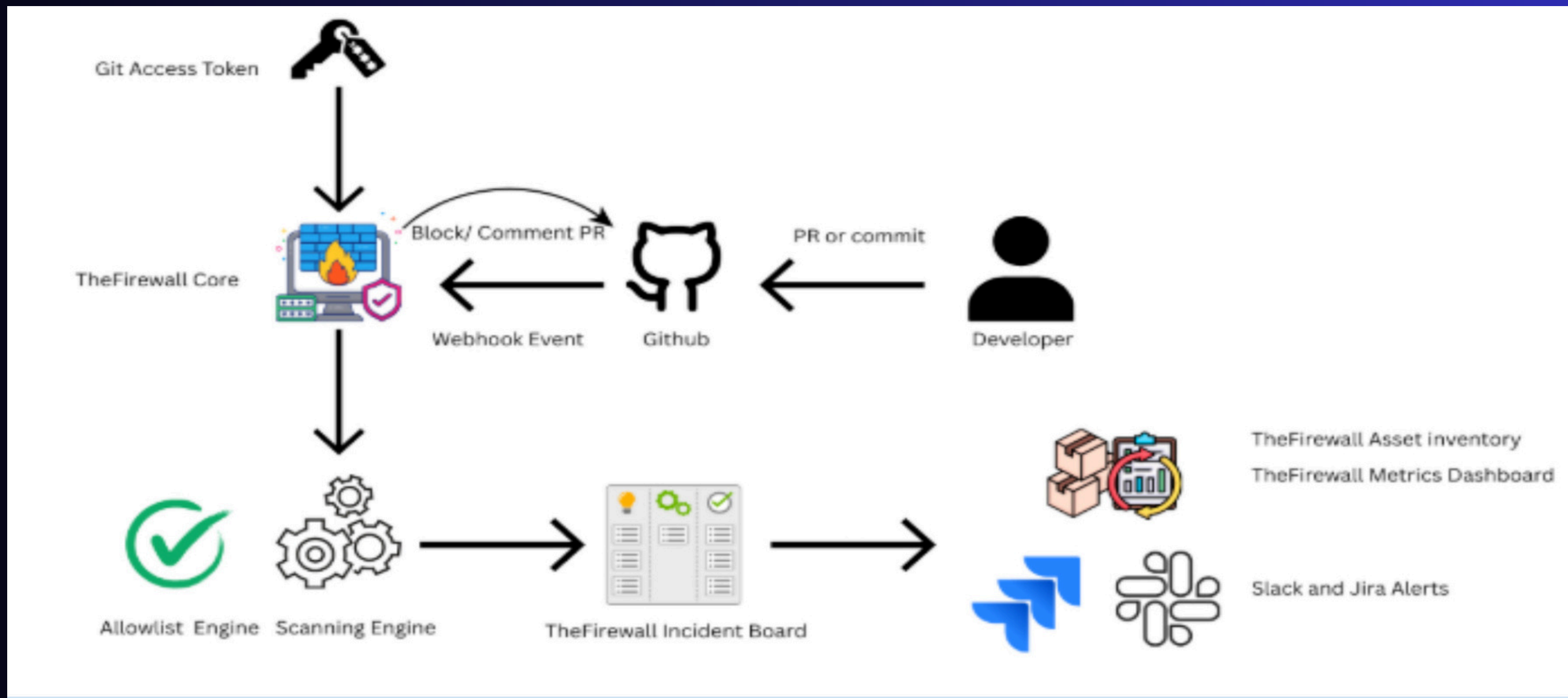- **SCANS**
- **INCIDENTS**
- **SETTINGS**

Platform Features

- **METRICS DASHBOARDS**

- **RISK BASED PRIORITIZATION**

- **ASSETS GROUPING**

- **SSO & RBAC**

- **REAL TIME ALERTS**

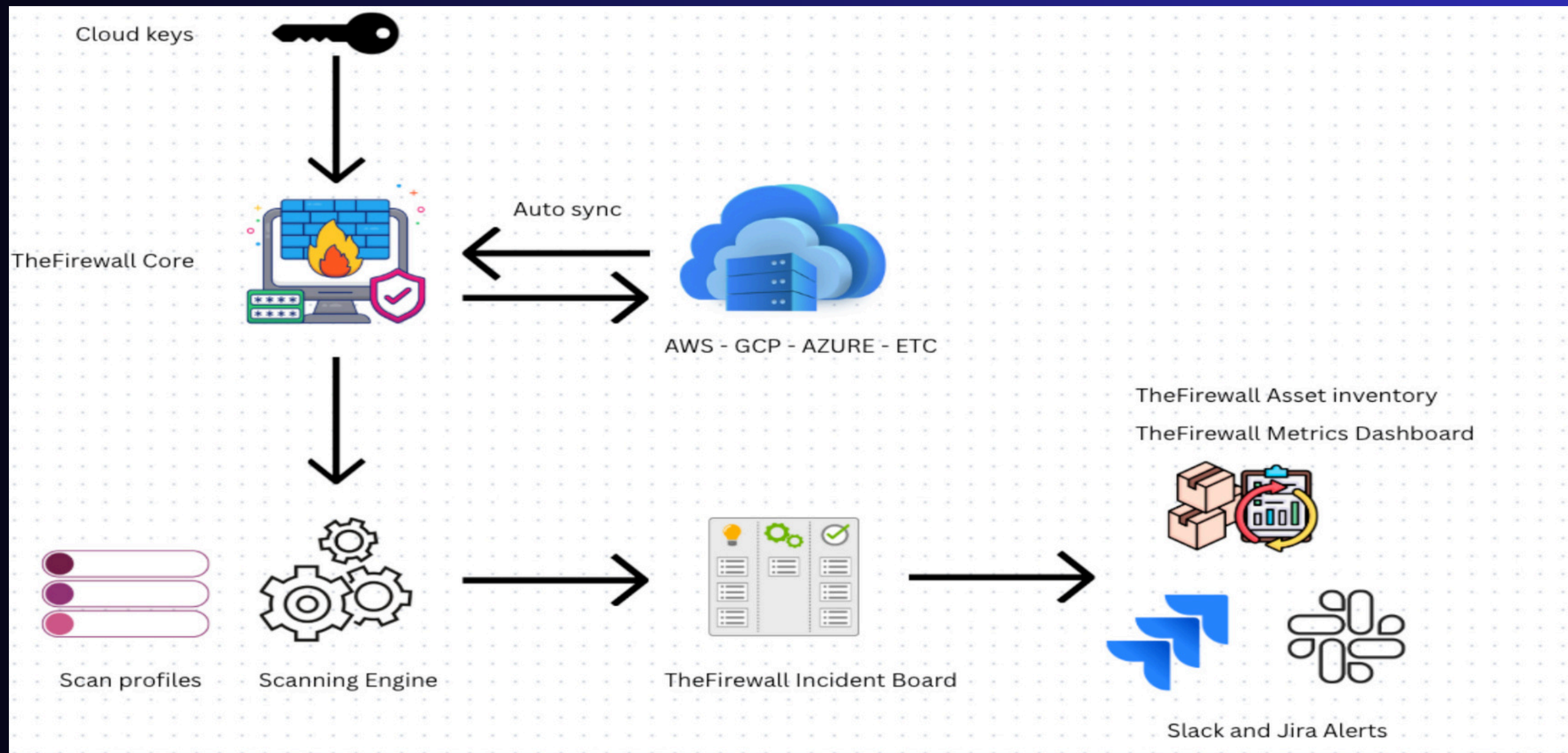- **1-CLICK DEPLOYMENT**

Secrets & SCA

Secrets & SCA Features

- PR & POST COMMIT SCANS

- ASSETS, SECRETS & VULNERABILITIES INVENTORY

- STREAMLINED INCIDENT MANAGEMENT

- FLEXIBLE AUTO-ALLOWLIST

- SBOMS & LICENSES

ASM

Cloud keys

TheFirewall Core

Auto sync

AWS - GCP - AZURE - ETC

TheFirewall Asset inventory

TheFirewall Metrics Dashboard

Scan profiles   Scanning Engine   TheFirewall Incident Board

Slack and Jira Alerts

ASM Features

- **SCAN PROFILES – CVES, MISCONFIGURATIONS, DEFAULT LOGINS, SSL, DNS, OWASP TOP 10, DAST**
- **REAL-TIME SCANS FOR NEW ASSETS/VULNERABILITIES**
- **PRE/POST AUTH SCANNING**
- **ASSETS & VULNERABILITIES INVENTORY**
- **SCANS SCHEDULER**
- **CUSTOM TEMPLATES USING TEMPLATE EDITOR**

Roadmap

Q2 — AI agents

Q3 — AI powered remediation assistance

Q4 — K8s & Container Security

Conclusion

- MISSION: DEMOCRATIZING CYBERSECURITY

- CATCH VULNERABILITIES EARLY, REDUCE COST

- YOUR FEEDBACK IS CRUCIAL FOR US

- WE ARE ALWAYS HERE TO SUPPORT YOU IN YOUR
  PLATFORM JOURNEY

Thanks & Credits

- **LAVLESH JOSHI**
- **SHIVAM GOYAL**
- **RAJESH YEMINENI**
- **SHASHANK**
- **AYAN KHAN**
- **MOUNISH**
- **FOSS & INFOSEC COMMUNITY**

thefirewall.org

/company/the-firewall-appsec

@tfirewall_

discord.gg/jD2cEy2ugg