Research Report

Presented by Manikanta Kumar

TABLE OF CONTENTS

1. SOUTH AFRICA CONNECT

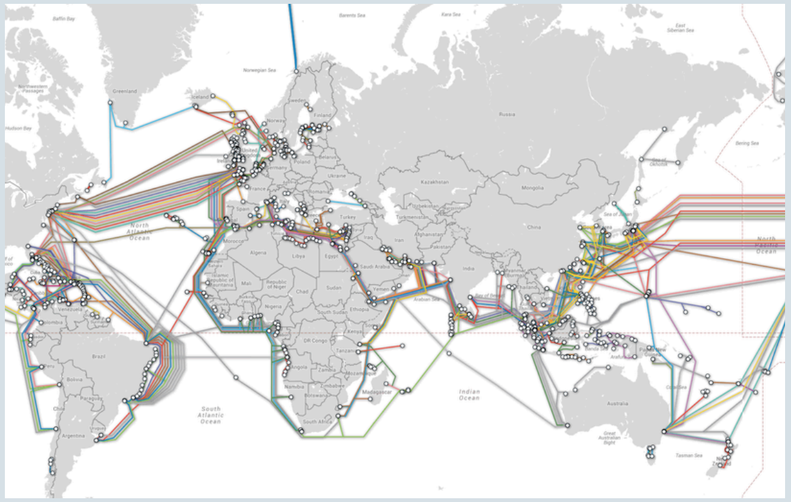
South Africa has been actively pursuing initiatives to enhance internet connectivity and bridge the digital divide. The cornerstone of these efforts is the South Africa Connect program, the country's national broadband policy and implementation plan, approved by the Cabinet in 2013.

1. **Objective:** Improve digital connectivity across South Africa.
2. **Key Focus:** Expanding broadband, deploying 5G, and enhancing telecom infrastructure.
3. **Challenges:** High costs, regulatory issues, and rural connectivity gaps.
4. **Impact:** Boosts internet access, economic growth, and digital inclusion.
5. **Future Goal:** Achieve universal connectivity by 2030.

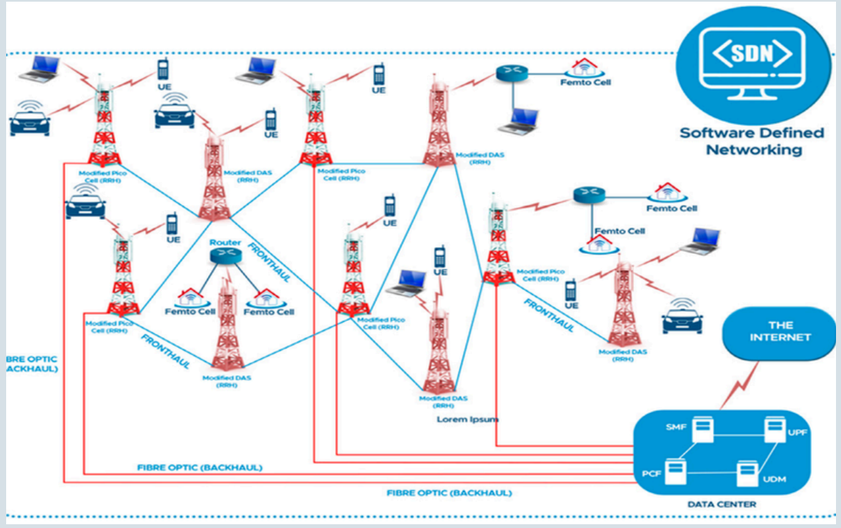
For more details, Click here

2. INTERNET TRAVELLING

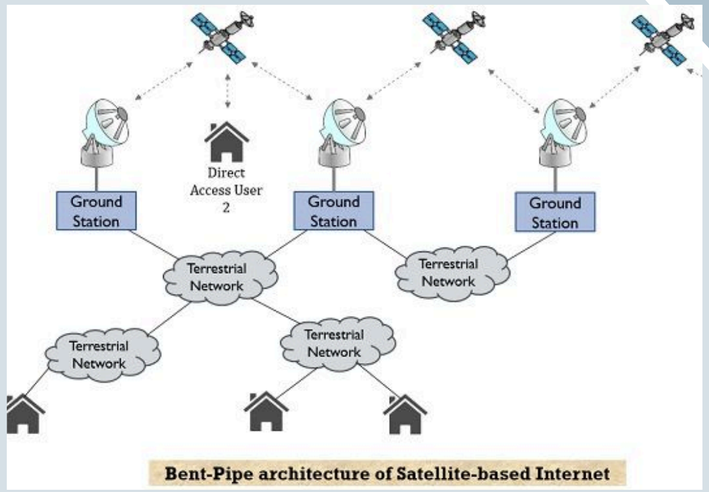
The internet travels across the globe primarily through a combination of submarine fiber-optic cables,terrestrial networks, and satellites.



- Contains 99% global internet traffic.
- Data travells at light speed (400 Tbps).
- These cables are laid across the ocean floors, connecting continents.



- Once the data reaches a country, it moves through fiber-optic cables, cell towers, and data centers.
- Used in urban and rural areas for home broadband and mobile networks.
- Speed: Varies (Fiber: 1–10 Gbps, 4G/5G: 100 Mbps–10 Gbps).

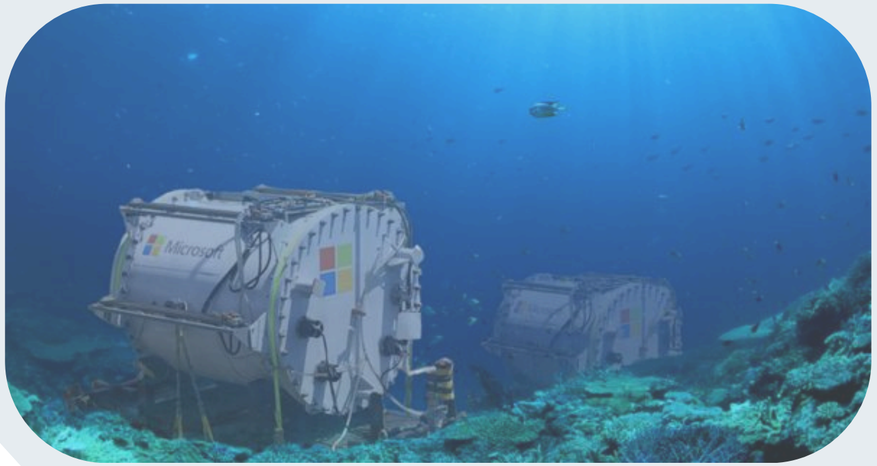


- Used in remote areas where cables can't reach.
- Satellites beam internet signals to ground stations and directly to users.
- Speed: Slower than fiber (50–250 Mbps, higher latency).

3. PROJECT NATICK

50% of us live near the coast. Why doesn't our data?

- Microsoft's Project Natick was an experimental initiative aimed at exploring the feasibility of underwater data centres to enhance energy efficiency and reduce latency. Launched in 2015, the project underwent two significant phases before concluding in 2024.
- **Key Features:**
  - ✅ Sealed Capsule: A submarine-like data center deployed deep underwater.
  - ✅ Energy Efficient: Uses ocean cooling and runs on renewable energy.
  - ✅ Reliable Performance: Lower failure rates than land-based data centers.
  - ✅ AI Monitoring: AI and robotics manage maintenance without human intervention.



For more details, Click here

4. APOLLO HOSPITAL CYBER ATTACK

Apollo Hospitals Ransomware Attack - October 2022.

- Attackers: Kill Security (hacker group)
- Type of Attack: Ransomware
- Date of Attack: October 2022
- Data Compromised: Patient names, medical conditions, diagnostic results
- Threat: Hackers threatened to release the stolen data by October 28, 2024
- Affected Individuals: 94 people (including 58 third-party individuals and 3 employees)
- Security Flaws: Outdated software and weak cybersecurity defences made the system vulnerable
- Response: Apollo Hospitals worked on securing its systems and protecting patient privacy
- Impact: Raised concerns about cybersecurity in healthcare institutions

5. RAJINI++ LANGUAGE

Rajini++ was created by Ajay Venkatesh and a group of developers as a fun, esoteric programming language inspired by the legendary Indian actor Rajinikanth. The language was designed with humor in mind, incorporating Rajinikanth's larger-than-life persona into programming syntax.

Key Features-

- Rajini-Themed Syntax: Commands like superstar, punch, and style replace traditional programming keywords.
- Case Insensitivity: Since "Rajinikanth doesn’t follow rules, rules follow him."
- Humorous Execution: Some commands execute in unexpected ways, adding fun elements.
- No Compilation Errors: Because "Rajinikanth’s code never fails!"

6. CYBERSECURITY HISTORY

Cybersecurity is the practice of protecting computers, networks, systems, and data from cyber threats such as hacking, malware, ransomware, phishing, and data breaches. It ensures the confidentiality, integrity, and availability of digital assets.

Why is Cybersecurity Important?

- Prevents Cyber Attacks – Defends against hackers, viruses, and malware.
- Protects Personal & Business Data – Prevents identity theft and financial fraud.
- Ensures National Security – Safeguards government and critical infrastructure.
- Maintains Trust & Compliance – Helps businesses follow laws like GDPR & HIPAA.

Evolution of Cybersecurity:-

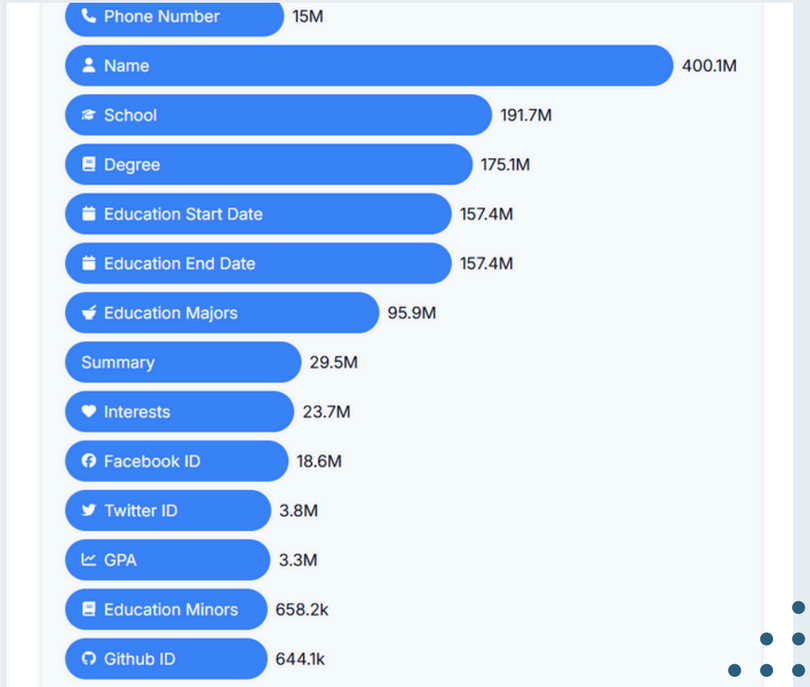
1. 1970s – The Birth of Cybersecurity
   - First computer worm ("Creeper") spreads on ARPANET.
   - "Reaper" created as the first antivirus program.
2. 1980s – Rise of Cyber Threats
   - Morris Worm (1988) spreads across the early internet.
   - First antivirus software (McAfee, Norton) is developed.
3. 1990s – Internet Expansion & Hacking
   - Firewalls and encryption methods improve security.
   - Hacking groups like Anonymous emerge.
4. 2000s – Cybercrime Becomes Global
   - Rise of phishing, ransomware, and identity theft.
   - Governments introduce cybersecurity regulations.
5. 2010s – Cloud, AI & Data Breaches
   - AI enhances threat detection & response.
   - Large-scale breaches affect millions (Yahoo, Facebook, Equifax).
6. 2020s – Zero Trust & Future Threats
   - 5G, IoT, and quantum computing pose new risks.
   - Cyber warfare and nation-state attacks increase.

7. REAL WORLD AUTHENTICATION BREACHES

An authentication breach happens when attackers bypass or compromise a system's login mechanisms to gain unauthorized access to sensitive data, accounts, or systems. These breaches often occur due to weak passwords, phishing attacks, stolen credentials, or security flaws.

1.Linkedin Data Breach (2021)

The LinkedIn data breach of 2021 was one of the largest data leaks, affecting 700 million users—which accounted for nearly 93% of LinkedIn's total user base at the time. The breach raised concerns about data privacy, as it exposed sensitive user information.



Overview of the LinkedIn 2021 Breach:

- Date of Breach: June 2021
- Affected Users: 700 million
- Type of Data Compromised: Public and private data
- Source of Breach: Scraping, not hacking

2.Facebook Credentials Leak (2021)

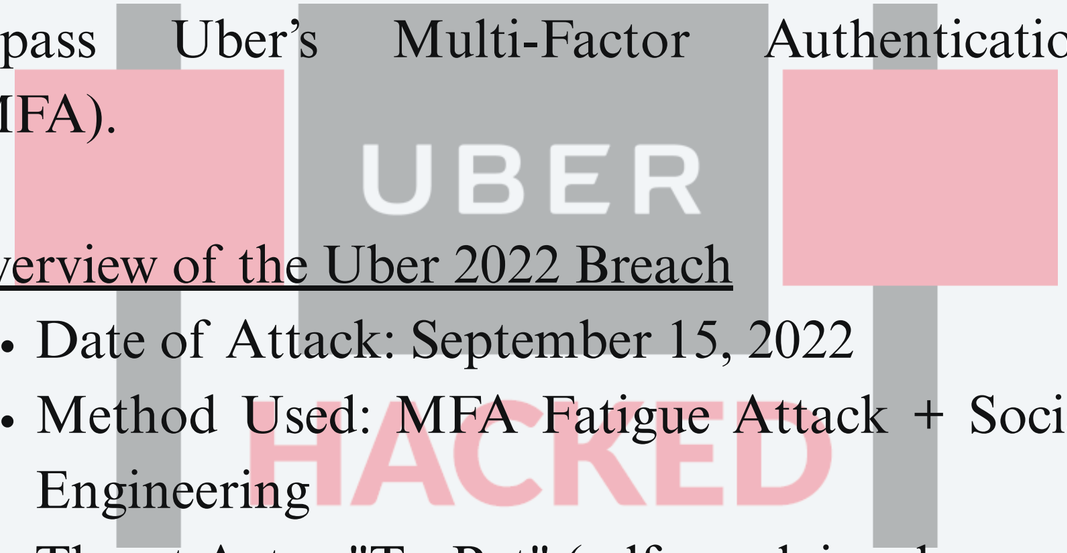
The Facebook data leak of 2021 was a major security incident in which 533 million users' personal data was exposed online for free. This included phone numbers, email addresses, and other sensitive information.

Overview of the Leak

- Date of Leak: First reported in April 2021
- Affected Users: 533 million Facebook users from 106 countries
- Source of Breach: Scraping via a vulnerability in Facebook's contact importer feature
- Nature of Data Exposed: Personal data, but not passwords

3. Uber 2022 MFA bypass via Social Engineering

The Uber security breach in 2022 was a major cyberattack that exposed internal systems, source code, security tools, and sensitive company data. The attack was carried out by a single hacker (allegedly 18 years old) using social engineering to bypass Uber's Multi-Factor Authentication (MFA).



Overview of the Uber 2022 Breach

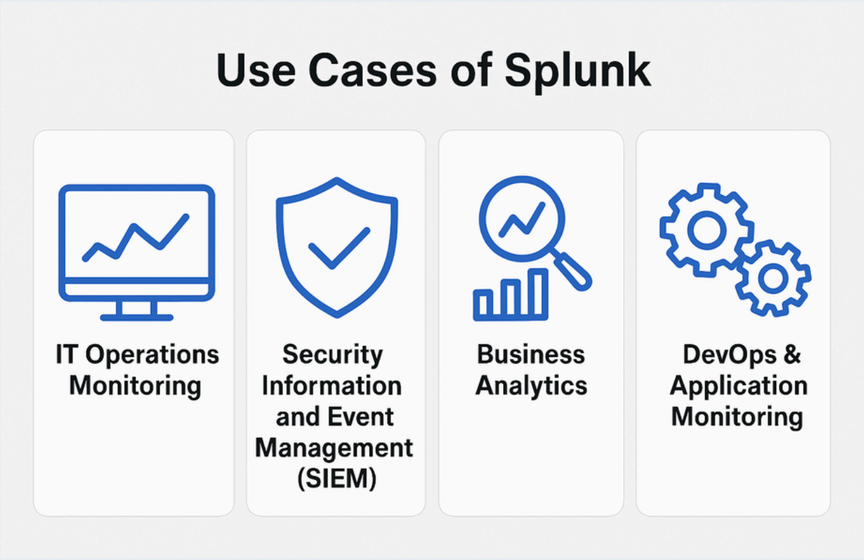
- Date of Attack: September 15, 2022
- Method Used: MFA Fatigue Attack + Social Engineering
- Threat Actor:"TeaPot" (self-proclaimed hacker, allegedly affiliated with LAPSUS$ hacking group)
- Target: Uber's internal corporate network.

8. SIEM TOOLS

SIEM tools, or Security Information and Event Management tools, are software solutions that collect, analyze, and manage security data from various sources within an organization. They help detect and respond to potential security threats in real-time by aggregating data from applications, devices, and networks.

1. **SPLUNK:-** A powerful platform for searching, monitoring, and analyzing machine-generated data in real time.

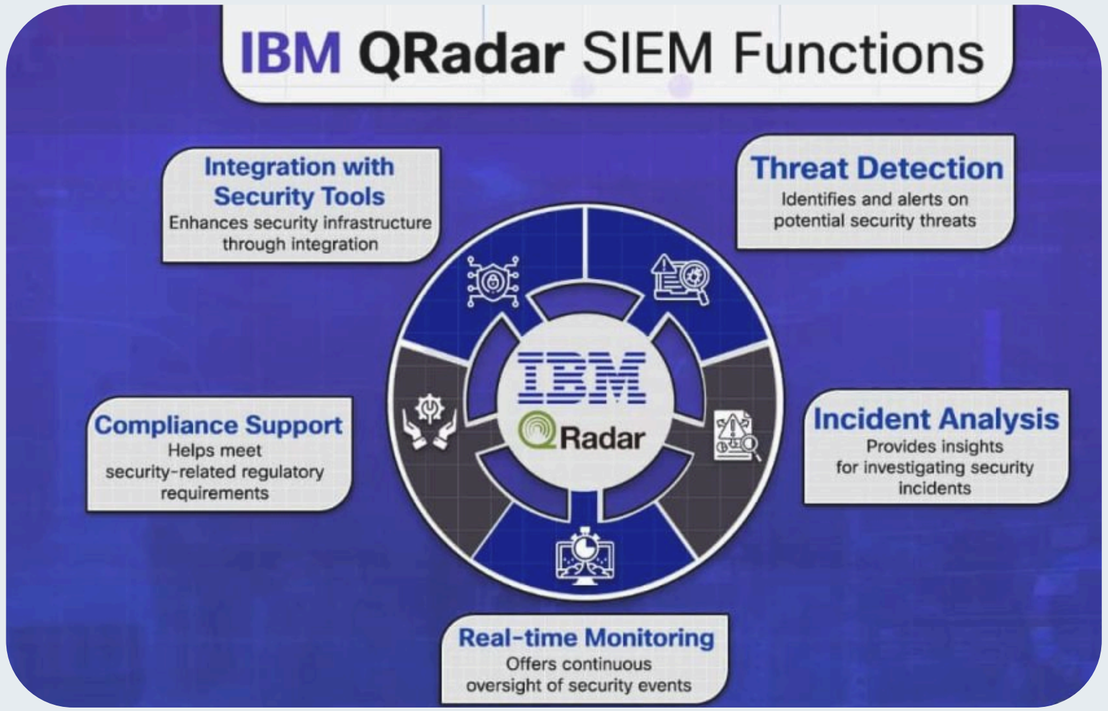
How Splunk Works



2. IBM QRADAR:- A powerful SIEM tool that helps organizations detect, analyze, and respond to cybersecurity threats in real-time.

How It Works:

1. Data Ingestion – Collects security logs & network data
2. Correlation & Analysis – Uses AI & threat intelligence for detection
3. Incident Prioritization – Reduces alert fatigue with risk-based insights
4. Response & Remediation – Automates incident response with SOAR integration

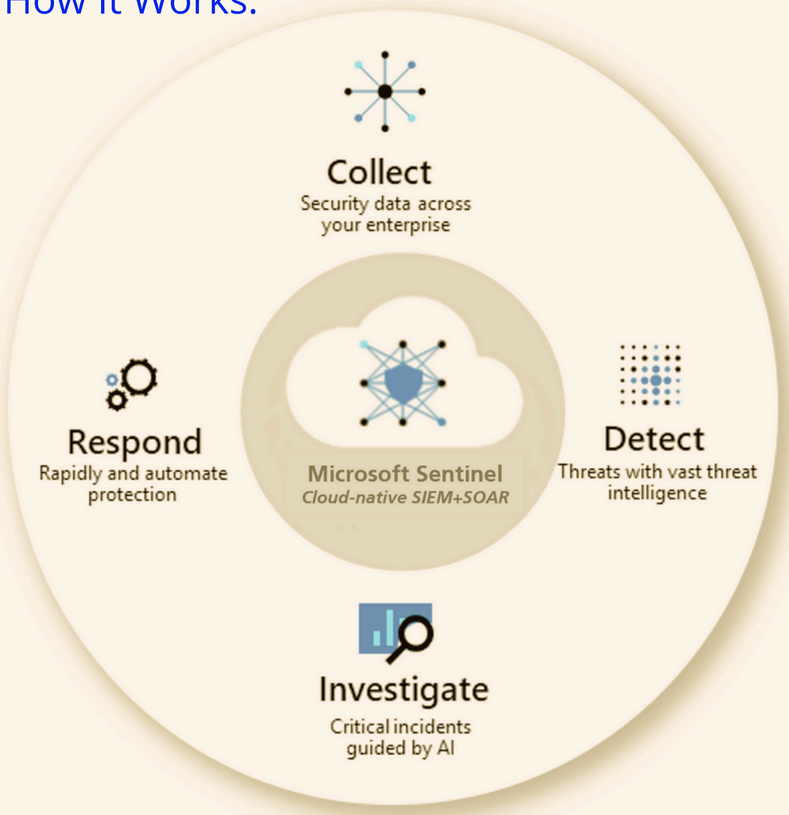


USE CASES

- Cyber Threat Detection & Response
- Insider Threat Monitoring
- Security Compliance Auditing
- Cloud Security & Hybrid IT Protection

3. SENTINEL:- A cloud-native SIEM and SOAR platform that helps organizations detect, investigate, and respond to security threats using AI and automation.

How It Works:



Key Features:

✅ Scalable Cloud-Native SIEM – Built on Microsoft Azure for global scalability

✅ AI-Powered Threat Detection – Uses machine learning & threat intelligence

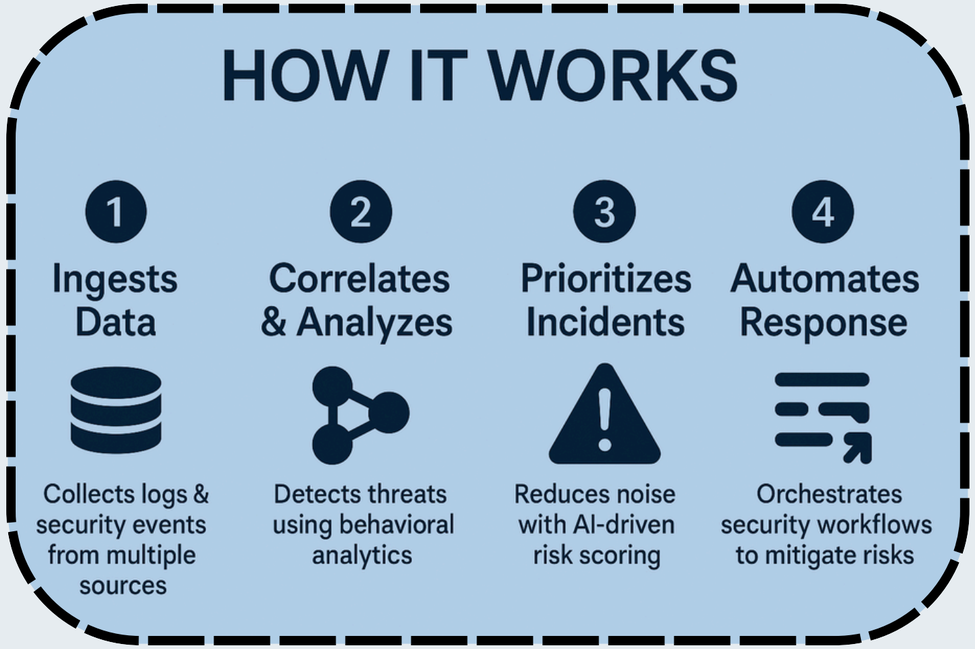
✅ Automated Incident Response (SOAR) – Reduces response time with automation

✅ Security Analytics & Log Management – Centralized visibility across environments

✅ Integration with Microsoft & Third-Party Tools – Works with Office 365, Azure, AWS, and more

4. ARCSIGHT:-

ArcSight is an advanced SIEM solution designed for threat detection, compliance, and security analytics across enterprise environments.



Key Features

- ✅ Real-time Threat Detection
- ✅ Log Management & Security Analytics
- ✅ Scalable & High Performance
- ✅ User & Entity Behavior Analytics (UEBA)
- ✅ Automated Incident Response
- ✅ Compliance & Reporting

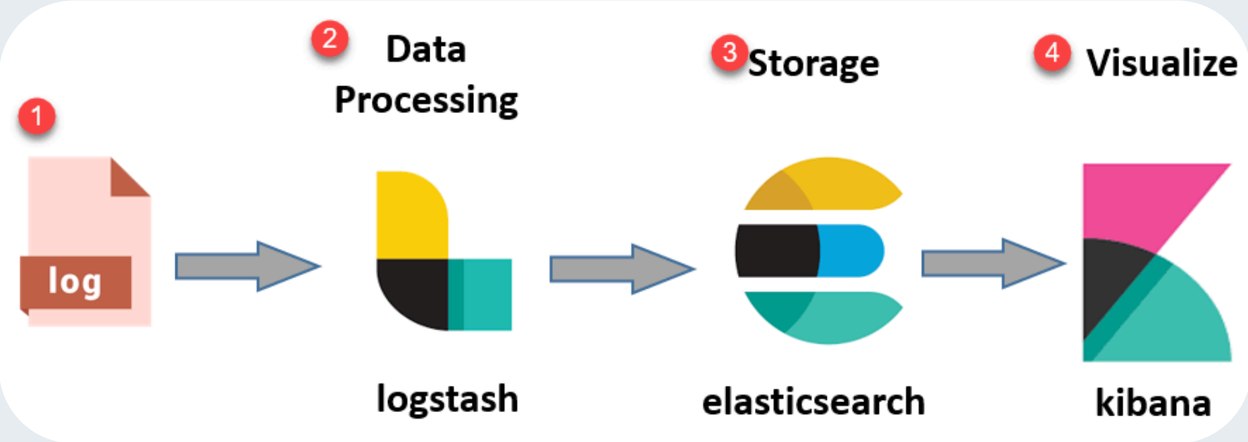
Use Cases:-

- Enterprise Threat Detection & Response
- Security Operations Center (SOC) Optimization
- Compliance & Risk Management
- Cloud & Hybrid Security Monitoring

5. ELK STACK:-

The ELK Stack (Elasticsearch, Logstash, Kibana) is a powerful open-source log management, search, and analytics platform used for real-time monitoring, visualization, and security analytics.

How it Works-



Use Cases:

- IT Operations Monitoring
- Security & Threat Detection
- Application Performance Management
- Business Intelligence & Log Analytics

Key Features

Centralized Log Management
Collects and processes logs from multiple sources

Real-time Search & Analytics
Fast querying and filtering of massive datasets

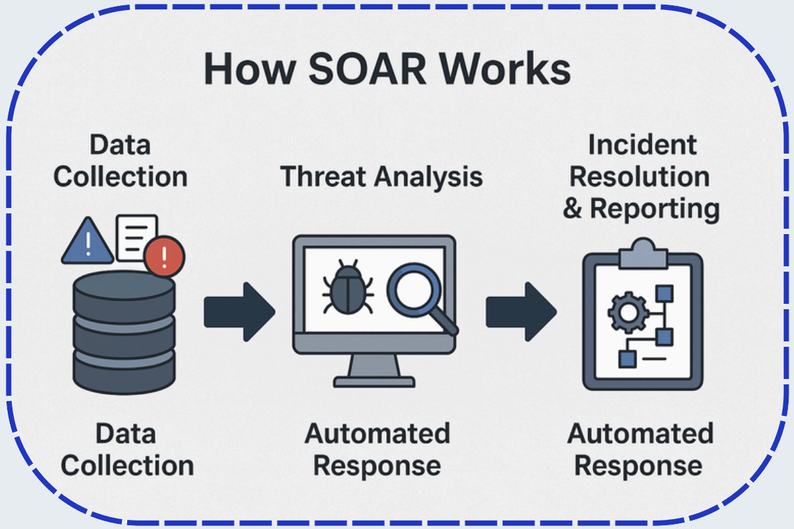
Customizable Dashboards
Interactive visualizations for monitoring trends

Security & Compliance
Detects anomalies and helps with audits

9. SOAR

SOAR stands for Security Orchestration, Automation, and Response. It is a set of tools and processes that help security teams automate incident response, streamline workflows, and improve overall cybersecurity efficiency.

SOAR = SOA+SIRP+TIA



Use Cases:

- Automated Phishing Analysis & Response
- Endpoint Threat Detection & Remediation
- Insider Threat Identification
- Vulnerability & Patch Management

10. NETWORK SECURITY MONITORING TOOLS

For Network security monitoring we are using; Intrusion Detection Systems; Network Packet Analysis.

1.Intrusion Detection System (SNORT)

Snort is a powerful, open-source Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) developed by Cisco. It monitors network traffic in real time to detect and prevent security threats.

Snort

Operating Modes

- Sniffer Mode - Read IP packets and prompt them in the console application.
- Packet Logger Mode - Log all IP packets (inbound and outbound) that visit the network.
- NIDS and NIPS Modes: Log/drop the packets that are deemed as malicious according to the user-defined rules

KEY FEATURES

- Real-time Traffic Analysis
- Signature & Behavior-Based Detection
- Packet Logging & Analysis
- Flexible Rule-Based System

USE CASES

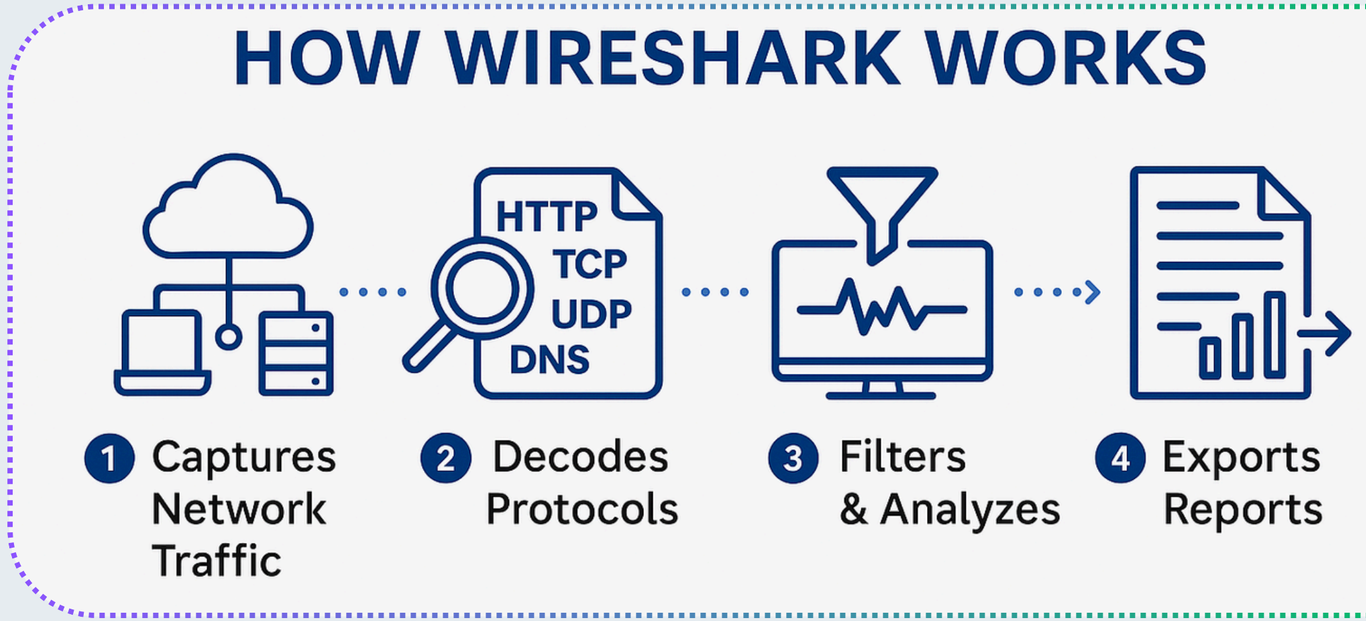
- Intrusion Detection & Prevention
- Network Security Monitoring
- Malware & Exploit Detection
- Threat Hunting & Forensics

2. Network Packet Analysis (WIRESHARK)

Wireshark is a free and open-source network packet analyzer that allows users to capture, inspect, and analyze network traffic in real time. It is widely used for troubleshooting, network monitoring, security analysis, and forensic investigations.

Key Features

- ✅ **Packet Capture & Analysis**
- ✅ **Deep Packet Inspection (DPI)**
- ✅ **Real-Time & Offline Analysis**
- ✅ **Color-Coded Filters & Views**
- ✅ **Cross-Platform Support**



11. CLOUD VENDORS

Cloud vendors are companies that provide cloud computing services, including infrastructure, platforms, and software, to businesses and individuals over the internet. These services allow users to access computing resources such as servers, storage, databases, networking, and analytics without having to maintain physical hardware.

Cloud Service Providers :-

Services they are providing-

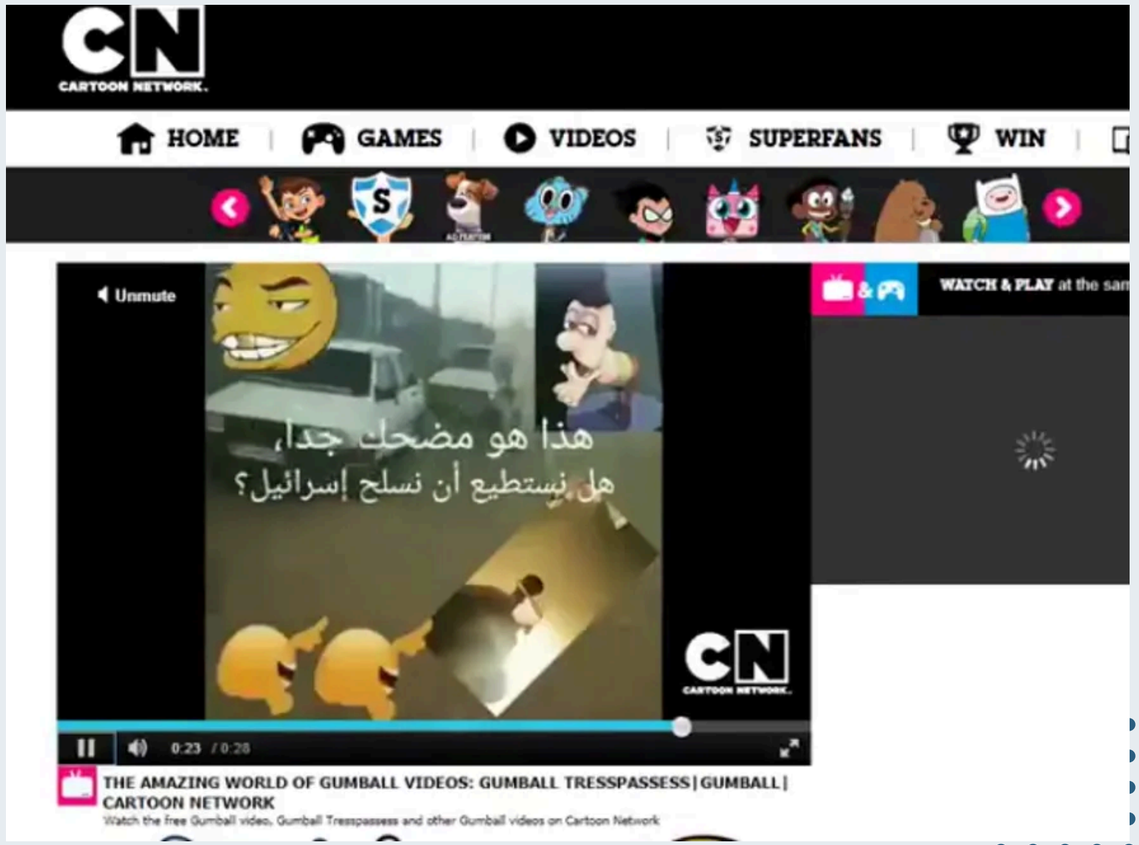
GOOGLE CLOUD SERVICES	MICROSOFT AZURE	AMAZON WEB SERVICES (AWS)	WHAT IT DOES
Google Compute Engine	Azure Virtual Machines	Elastic Compute Cloud (EC2)	Infrastructure as a Service (IaaS)
Google App Engine	Azure Cloud Services	AWS Elastic Beanstalk	Platform as a Service (PaaS)
Google Cloud SQL	Azure SQL Database	Amazon Relational Database Service	Database as a Service (DaaS)
Google Cloud Bigtable	Azure Table Storage	Amazon Dynamo DB	Scalable SQL database services
Google BigQuery	Azure SQL Database	Amazon Redshift	Relational Databases
Google Cloud Functions	Azure Functions	AWS Lambda	Serverless Applications
Google Cloud Datastore	Azure Cosmos DB	Amazon Simple DB	Highly Scalable NoSQL Database Services
Google Storage	Azure Storage	Amazon Simple Storage Service (S3)	Storage of object, blocks and files. Also for cool and cold storage of data.

12. CARTOON NETWORK ATTACK

In April 2019, multiple regional websites of Cartoon Network were hacked by two Brazilian hackers. The breach resulted in unauthorized content being displayed, including Arabic memes, Brazilian hip-hop music, and videos featuring Brazilian male stripper Ricardo Milos. The attack lasted for approximately three days before the websites were restored.

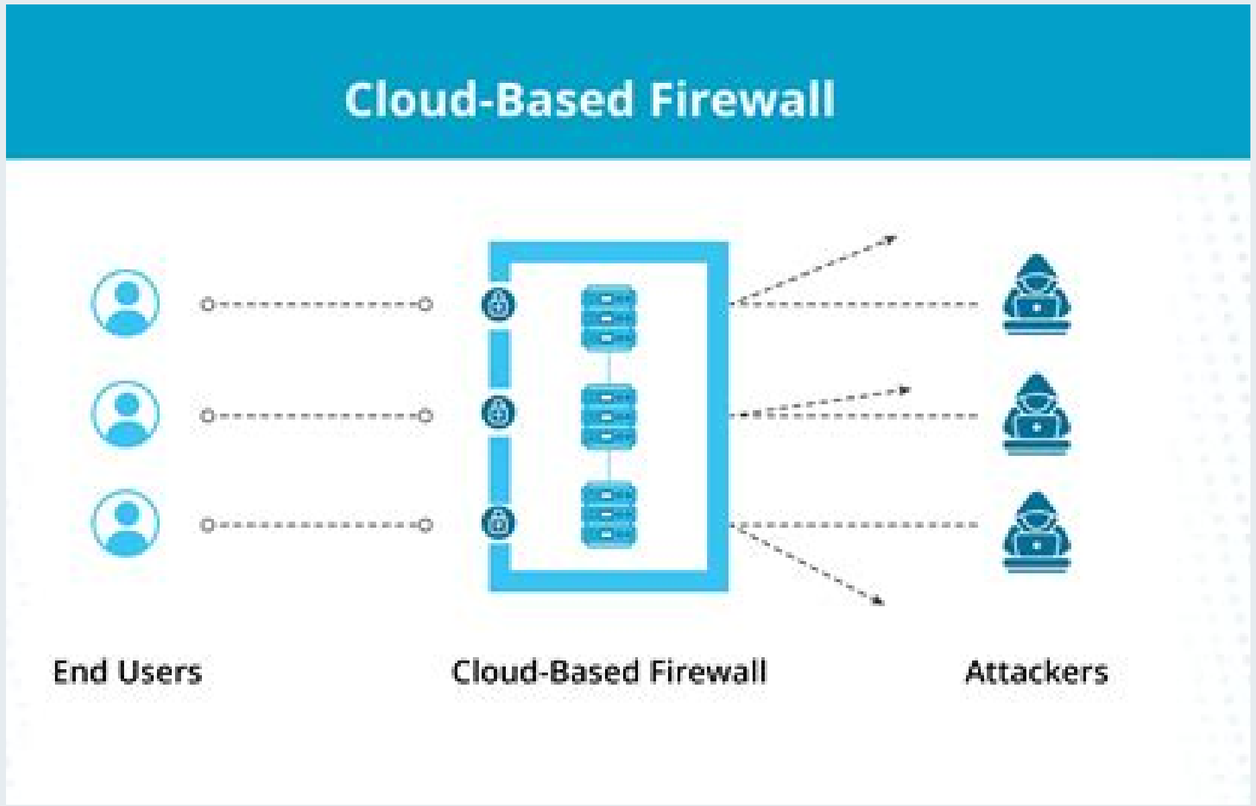
Nature of the Attack

- The hackers exploited vulnerabilities in Cartoon Network's content management system.
- Instead of the usual Cartoon Network shows, visitors saw memes, music, and explicit videos.
- Some pages redirected users to unrelated content, including adult-themed media.



13.CLOUD FIREWALLS

Cloud firewalls are security solutions designed to protect cloud environments from unauthorized access, cyber threats, and data breaches. They function similarly to traditional firewalls but are optimized for cloud-based infrastructure.



Types of Cloud Firewalls:-

1. Network-Based Cloud Firewalls
2. Host-Based Cloud Firewalls
3. Web Application Firewalls
4. Next-Generation Firewalls (NGFWs) in the Cloud

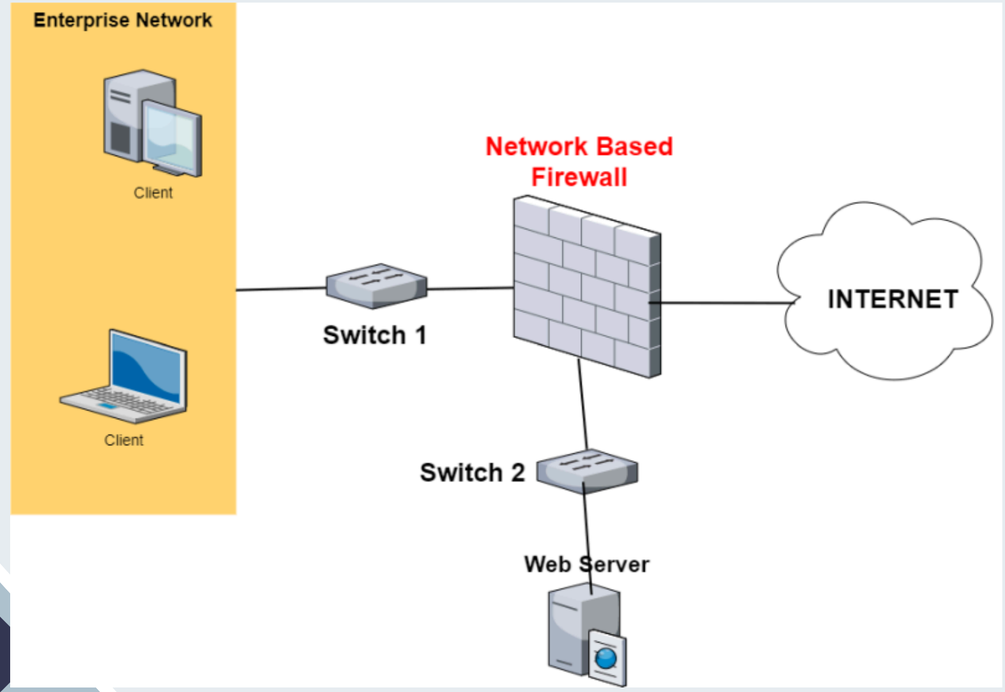
1 Network-Based Cloud Firewalls

🔹 Protects an entire cloud network by monitoring and filtering traffic between cloud instances, virtual networks, and the internet.

🔹 Typically implemented as cloud security groups or virtual network firewalls.

🔹 Examples: AWS Security Groups, Azure Firewall, Google Cloud Firewall.

✅ Best for: Organizations needing to secure multiple cloud resources at a network level.



2 Host-Based Cloud Firewalls

🔹 Installed directly on individual cloud servers (virtual machines or instances).

🔹 Provides authorization esecurity control for each server.

🔹 Can block specific IP addresses, ports, or applications at the instance level.

✅ Best for: Businesses running critical applications on virtual machines requiring custom security configurations.

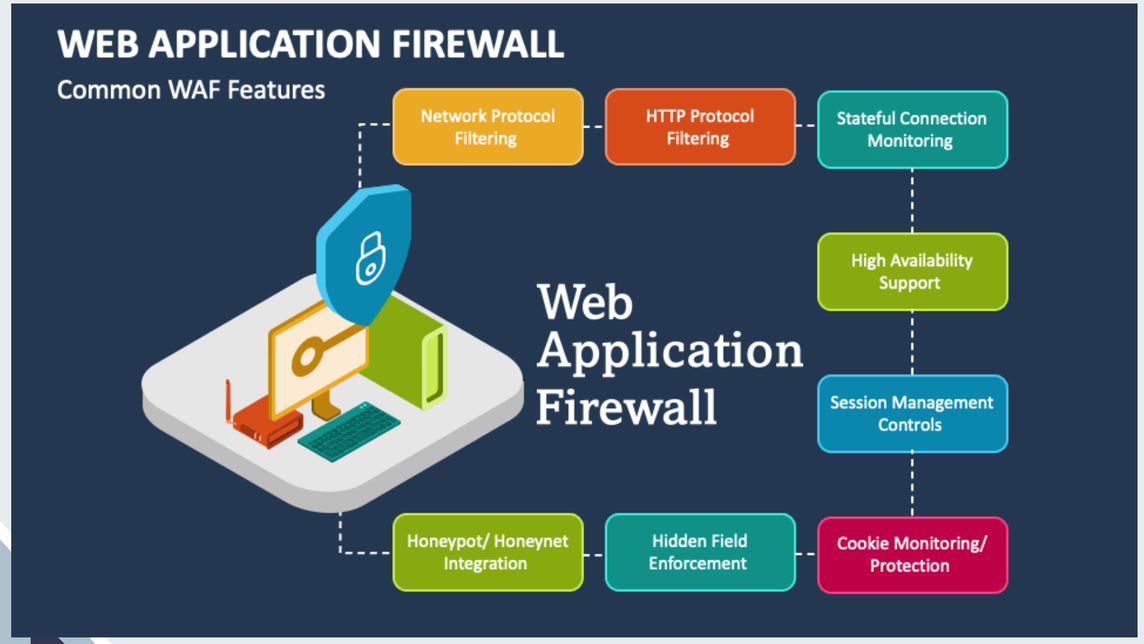
3 Web Application Firewalls

🔹 Protects specific web applications from HTTP/S-based attacks like SQL injection, cross-site scripting (XSS), and DDoS attacks.

🔹 Analyzes web traffic and filters out malicious requests before they reach the application.

🔹 Examples: AWS WAF, Cloudflare WAF, Azure WAF.

✅ Best for: Websites, APIs, and web applications needing real-time security from online threats.



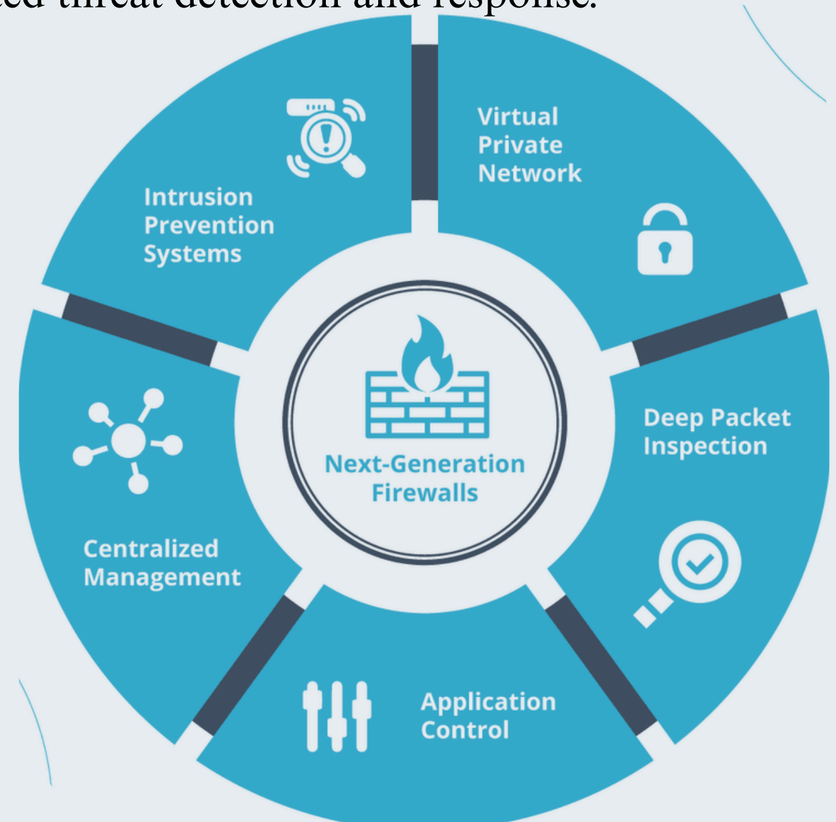
4 Next-Generation Firewalls

🔹 Offers advanced security features such as deep packet inspection, intrusion prevention, malware scanning, and threat intelligence integration.

🔹 Uses AI and machine learning to detect sophisticated threats.

🔹 Examples: Palo Alto Networks Prisma Cloud, Check Point CloudGuard.

✅ Best for: Enterprises requiring high-end security with automated threat detection and response.



14. CLOUD BASED THREAT DETECTION

Cloud-based threat detection is a cybersecurity approach that uses cloud infrastructure to identify and respond to potential threats—like malware, phishing, unauthorized access, or abnormal behavior—in real-time. It's a key part of modern security strategies, especially for businesses operating in cloud environments (like AWS, Azure, or Google Cloud).

1️⃣ Microsoft Defender for Cloud

Microsoft Defender for Cloud is a cloud-native security solution that provides threat protection, security posture management, and compliance monitoring for multi-cloud and hybrid environments. It integrates with **Azure, AWS,** and **Google Cloud** to help detect, prevent, and respond to security threats.

Key Capabilities of Microsoft Defender for Cloud:

1. **Cloud Security Posture Management (CSPM)**
2. **Cloud Workload Protection Platform (CWPP)**
3. **Cloud-Based Threat Detection (Advanced Threat Detection, ATP)**
4. **Regulatory Compliance & Governance**
5. **Multi-Cloud & Hybrid Security**
6. **Integration with Security Tools**

Microsoft Defender for Cloud | Overview

Showing 59 subscriptions

Search (Ctrl+/)

Subscriptions | What's new

General

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Community

Cloud Security

- Secure Score
- Regulatory compliance
- Workload protections
- Firewall Manager

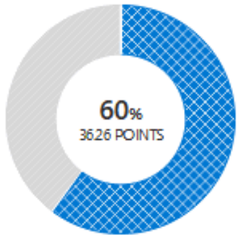
Management

- Environment settings
- Security solutions
- Workflow automation

59	1	4	161	121
Azure subscriptions	AWS accounts	GCP projects	Active recommendations	Security alerts

Secure score

Current secure score



COMPLETED Controls 1/16

COMPLETED Recommendations 29/190

Improve your secure score >

Regulatory compliance

Current compliance by passed controls

UKO and U...	0/7
SOC TSP	1/13
NIST SP 80...	2/23
HIPAA HITR...	2/22
NIST SP 80...	3/29

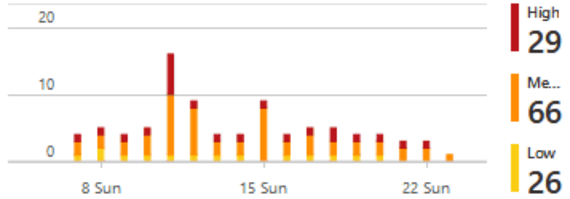
Improve your compliance >

Workload protections

Resource coverage

95% For full protection, enable 10 resource plans

Alerts by severity



Enhance your threat protection capabilities >

Inventory

Unmonitored VMs

60 To better protect your organization, we recommend installing agents

Total Resources

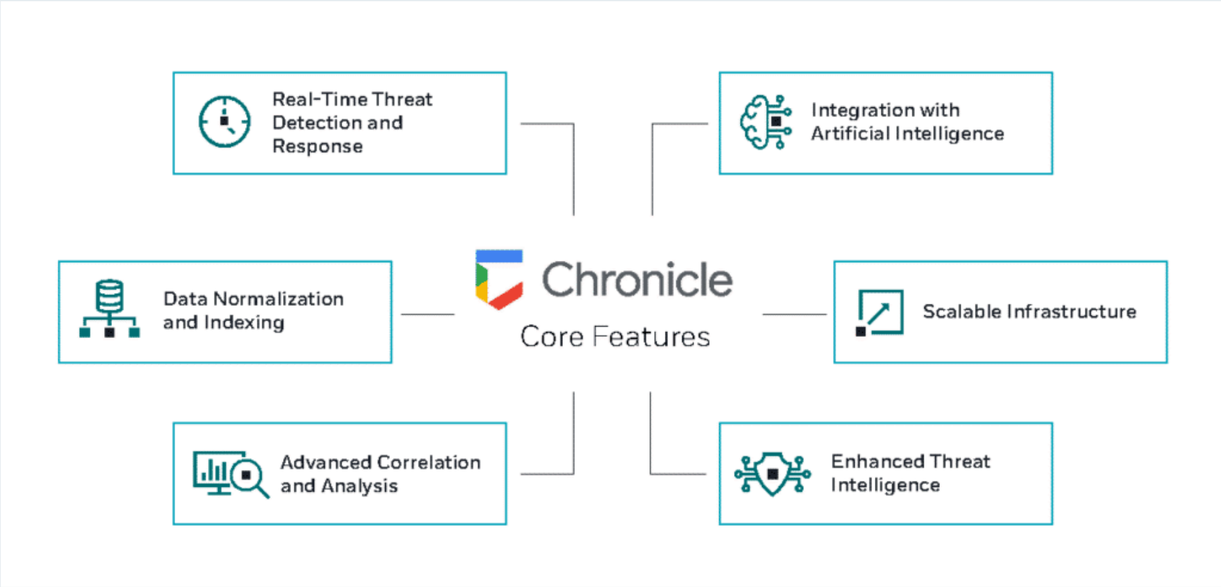
3900

Unhealthy (2936) Healthy (679) Not applicable (285)

Explore your resources >

2️⃣ Google Chronicle

Google Chronicle is a cloud-native security analytics platform used for cloud-based threat detection and security operations. It is designed to detect, investigate, and respond to cyber threats at scale using Google's infrastructure, AI, and big data analytics.



🧠 How Chronicle Works

1. Ingests data from your environment: firewalls, endpoints, network, cloud, identity providers, etc.
2. Normalizes and indexes all that data in a unified timeline view.
3. Correlates with threat intelligence and behavioral analytics.
4. Surfaces detections for investigation in an easy-to-navigate interface.
5. Enables automated or manual response using integrations (e.g., SOAR tools, tickets, alerts).

15. OWASP TOP 10

The OWASP Top 10 is a list of the most critical security risks for web applications, published by the Open Web Application Security Project (OWASP).

The OWASP Top 10 list is typically updated every 3 to 4 years, based on industry trends, new threats, and community feedback. Here's the update timeline so far:

- **2003 – First OWASP Top 10 release**
- **2004 – Second edition**
- **2007 – Third edition (3 years later)**
- **2010 – Fourth edition (3 years later)**
- **2013 – Fifth edition (3 years later)**
- **2017 – Sixth edition (4 years later)**
- **2021 – Seventh edition (4 years later)**

OWASP Top 10 (A1 to A10) are a mix of **attacks, threats and vulnerabilities.**

A1, A3, A8 are **attacks,** and A2, A4, A5, A7, A9, A10 are **vulnerabilities** and A6 is **threat**

The Most Persistent OWASP Top 10 Risks (2003-2021)

The following vulnerabilities have been present in multiple OWASP editions and continue to be major threats:

🚨**Injection (SQLi, Command Injection)** – 2003 to 2021

🔐**Broken Authentication** – 2003 to 2021

🛡️**Broken Access Control** – 2003 to 2021 (Ranked #1 in 2021)

⚙️**Security Misconfiguration** – 2010 to 2021

🔑**Sensitive Data Exposure (Renamed Cryptographic Failures in 2021)** – 2013 to 2021

Owasp Top 10 Vulnerabilities (Published from 2003 - 2017)		
OWASP Top 10 - 2017	**OWASP Top 10 - 2013**	**OWASP Top 10 - 2010**
A1. Injection	A1. Injection	A1. Injection
A2. Broken Authentication	A2. Broken Authentication and Session Management	A2. Cross Site Scripting (XSS)
A3. Sensitive Data Exposure	A3. Cross-Site Scripting (XSS)	A3. Broken Authentication and Session Management
A4. XML External Entities (XXE)	A4. Insecure Direct Object References	A4. Insecure Direct Object References
A5. Broken Access Control	A5. Security Misconfiguration	A5. Cross Site Request Forgery (CSRF)
A6. Security Misconfiguration	A6. Sensitive Data Exposure	A6. Security Misconfiguration
A7. Cross-Site Scripting (XSS)	A7. Missing Function Level Access Control	A7. Insecure Cryptographic Storage
A8. Insecure Deserialization	A8. Cross-Site Request Forgery (CSRF)	A8. Failure to Restrict URL Access
A9. Using Components with Known Vulnerabilities	A9. Using Components with Known Vulnerabilities	A9. Insufficient Transport Layer Protection
A10. Insufficient Logging&Monitoring	A10. Unvalidated Redirects and Forwards	A10. Unvalidated Redirects and Forwards
OWASP Top 10 - 2007	**OWASP Top 10 - 2004**	**OWASP Top 10 - 2003**
A1. Cross Site Scripting (XSS)	A1. Unvalidated Input	A1. Unvalidated Input
A2. Injection Flaws	A2. Broken Access Control	A2. Broken Access Control
A3. Malicious File Execution	A3. Broken Authentication and Session Management	A3. Broken Authentication and Session Management
A4. Insecure Direct Object Reference	A4. Cross Site Scripting	A4. Cross Site Scripting
A5. Cross Site Request Forgery (CSRF)	A5. Buffer Overflow	A5. Buffer Overflow
A6. Information Leakage and Improper Error Handling	A6. Injection Flaws	A6. Injection Flaws
A7. Broken Authentication and Session Management	A7. Improper Error Handling	A7. Improper Error Handling
A8. Insecure Cryptographic Storage	A8. Insecure Storage	A8. Insecure Storage
A9. Insecure Communications	A9. Application Denial of Service	A9. Remote Administration Flaws
A10. Failure to Restrict URL Access	A10. Insecure Configuration Management	A10. Security Misconfiguration

For interactive graphical details, [Click here]

16.ENCRYPTION TECHNIQUES FOR CLOUD

- Encryption in cloud security is the process of converting data into a secure format so that only authorized users can access it.
- This ensures that sensitive data remains confidential and protected from unauthorized access, even if intercepted by attackers.
- Cloud security relies heavily on encryption to protect **data at rest, in transit, and in use**.

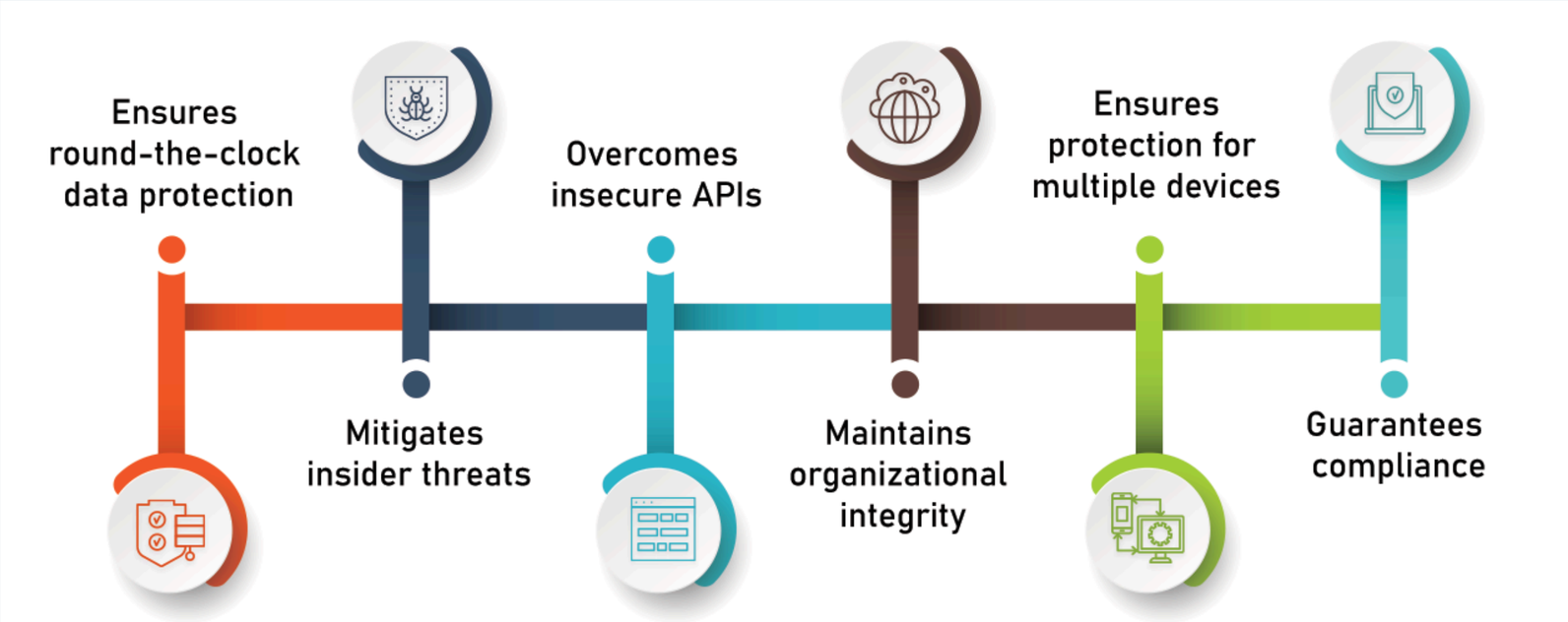


fig. Importance of Cloud Encryption

1 AES-256 (Advanced Encryption Standard) :-

What it is?

AES-256 is a symmetric encryption algorithm that encrypts and decrypts data using the same 256-bit key. It is one of the most secure encryption methods used for cloud storage, databases, and secure communications.

How it works?

1. Encrypts data in 14 rounds of transformations (substitution, shifting, mixing, and key addition).
2. Fast and efficient for encrypting large volumes of data.
3. Used for data encryption at rest (e.g., AWS S3, Google Cloud Storage).

🔐 AES-256 in Action

1. HTTPS (TLS) for secure web browsing
2. VPN encryption for secure tunneling (e.g., OpenVPN, IPsec)
3. File encryption tools (e.g., 7-Zip, VeraCrypt)
4. Cloud storage encryption (e.g., Google Drive, AWS S3 encryption)
5. Disk encryption (BitLocker, FileVault)

2 TLS/SSL (Transport Layer Security & Secure Sockets Layer) :-

What it is?

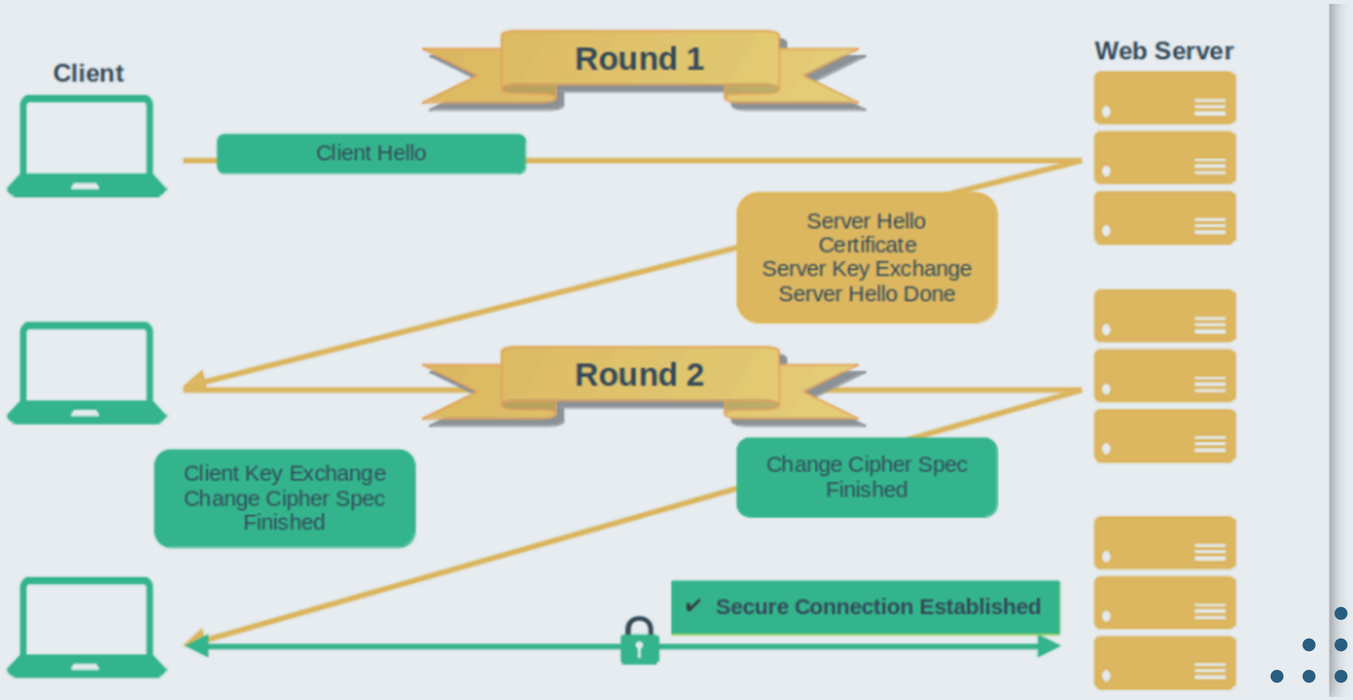
TLS (modern version of SSL) is a cryptographic protocol that secures data in transit over networks. It ensures secure web browsing, API communications, and VPNs.

How it works?

1. Uses asymmetric encryption (RSA, ECC) for key exchange and symmetric encryption (AES) for data transmission.
2. Establishes a secure connection (HTTPS, VPNs) between client and server.

🌐 Where TLS/SSL is Used

1. HTTPS (web browsing)
2. Email encryption (SMTP, IMAP, POP with TLS)
3. VPNs
4. VoIP
5. Cloud services
6. Online transactions



3 Homomorphic Encryption :-

🔹 What it is?

1. Homomorphic Encryption is a form of encryption that allows computation on encrypted data without needing to decrypt it first.
2. In simple terms: You can run operations on data while it's still encrypted, and when you decrypt the result, it's the same as if you'd performed those operations on the original plaintext.
3. This is a game-changer for data privacy—especially for sensitive applications in finance, healthcare, and cloud computing.

🧠 Why It Matters?

Normally, to perform analysis on encrypted data, you'd have to:

1. Decrypt it 🔓
2. Process it 🧮
3. Re-encrypt it 🔐

This exposes the data in step 2. But with homomorphic encryption, data stays encrypted throughout.

🔍 Example Use Cases:-

🏥 Healthcare: Run statistical models on encrypted patient records without exposing personal data

💳 Finance: Perform fraud detection on encrypted transactions

☁️ Cloud Computing: Cloud providers can compute over encrypted client data without seeing it

🧠 Machine Learning: Train models on private data securely

THANK YOU

FOR YOUR ATTENTION