Different Team

Different IT Teams in a Company

- Systems Team
- Network Team
- Endpoint Security Team
- Network Security Team
- Information Security Team
- Security Operations Center
- Application Development Team
- Database Team
- IT Helpdesk

- **Cloud**
- **Virtualization**
- **Vulnerability Assessment**
- **Identity and Access Management**

Systems Team/Server Team

Providing System (Desktops/Laptops)

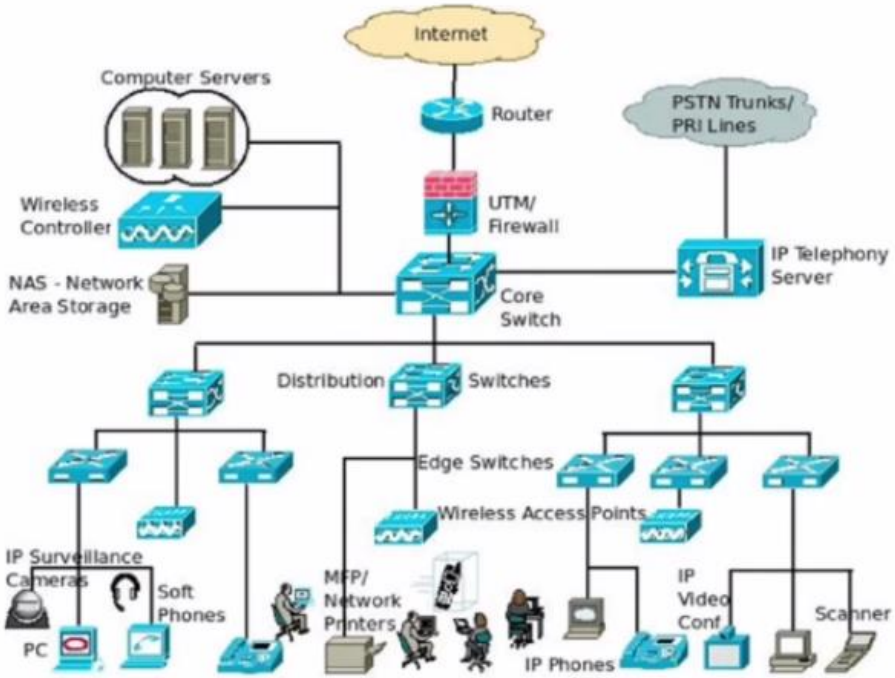
Installing and Maintaining Operating Systems

Installing necessary applications for employees

Installing, configuring and managing servers

Network Team

Planning and Designing Network Architecture



Installing and Maintaining Network Devices

Routers

Switches

Access Points

Network Cables

Endpoint Security Team

Protecting endpoints in the network. (User machines, Servers etc.)

Installing, Configuring and Maintaining Endpoint Security Solutions

Antivirus

Host Firewall

Host Intrusion Prevention system

Disk Encryption

Data Loss Prevention

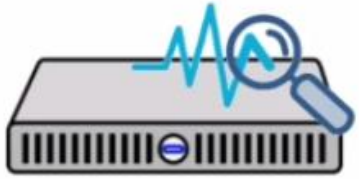
Endpoint Detection & Response

Network Security Team

Protecting the over all network.

Installing, Configuring and Maintaining Network Security Solutions

Firewall



Intrusion Prevention system

Web Gateway

Email Gateway

Wireless Security

Web Application Firewall

Infosec Security Team

Conduct Regular Audits

Drafting Security Policies

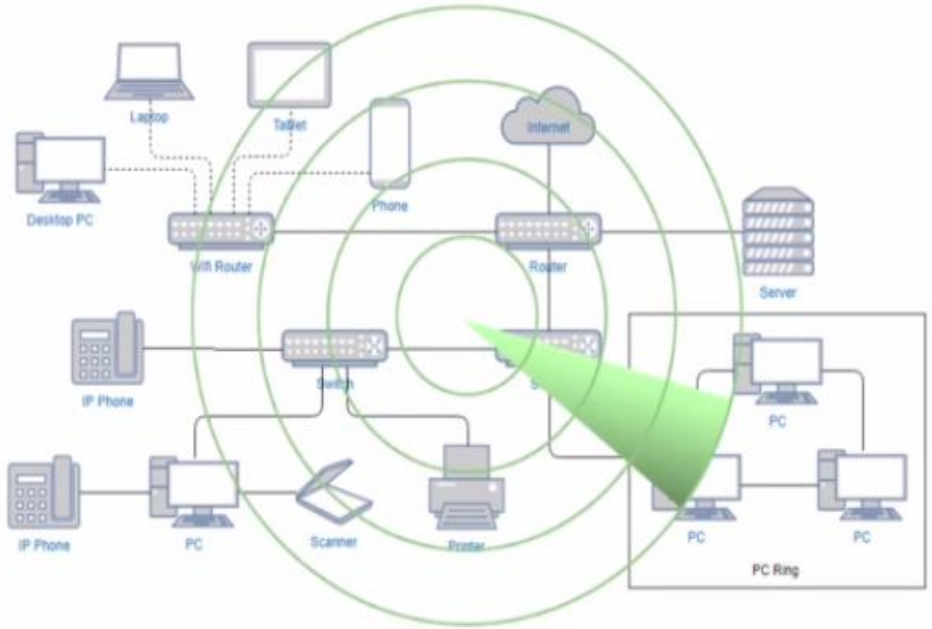
Conduct User Awareness Training

Adherence to Regulatory Compliance

ehackerworld.com
info@ehackerworld.com

Vulnerability Assessment Team

Use automated tools to scan the network to identify the vulnerabilities in applications and systems.



Vulnerability Scanners

Analyse the report and work with various teams for fixing the vulnerabilities.

Patching

Identity and access Management Team

Create and manage Identities and Access rights of people (employees and customers)

IAM – Identity and Access Management Tool

User Accounts

Password Resets

Granting Access

Security Operation Center

- Monitor, detect, investigate, and respond to cyberthreats
- Work with SME of other teams to remediate the security incident

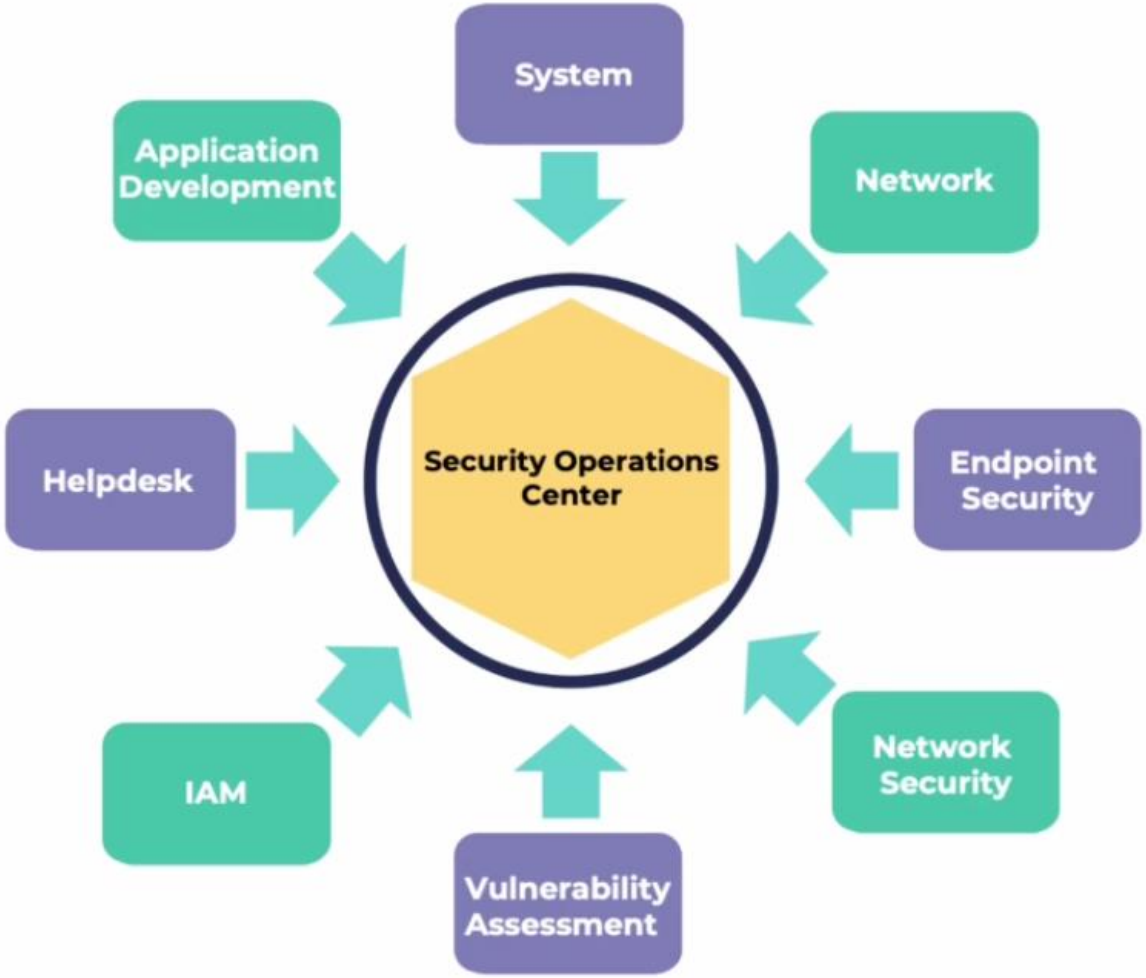
SIEM

SOAR

Threat Intelligence

Analysis Tools

SOC – Central to organization Security



Evolution of SOC

Year 2008 - 2010

Stuxnet

First cyber weapon

Designed to bring down
Iran's Nuclear Power Plant

Major Cyber Attacks in the past

SONY

In 2014, a hacker group which identified itself by the name "Guardians of Peace" leaked a release of confidential data from the film studio Sony Pictures.

yahoo!

In 2012, hackers posted login credentials for more than 453,000 user accounts. Again in January 2013 and in January 2014.

MasterCard VISA

In 2012, they warned card-issuing banks that a third-party payments processor suffered a security breach, affecting up to 10 million credit cards.

SUBWAY

In 2012, two Romanian men admitted to participating in an international conspiracy that hacked into credit-card payment terminals at more than 150 Subway restaurant franchises and stole data for more than 146,000 accounts.

TARGET

In 2013, approximately 40 million credit and debit card accounts were impacted in a credit card breach. According to another estimate, it compromised as many as 110 million Target customers.

Who is safe in the Internet?

Some findings

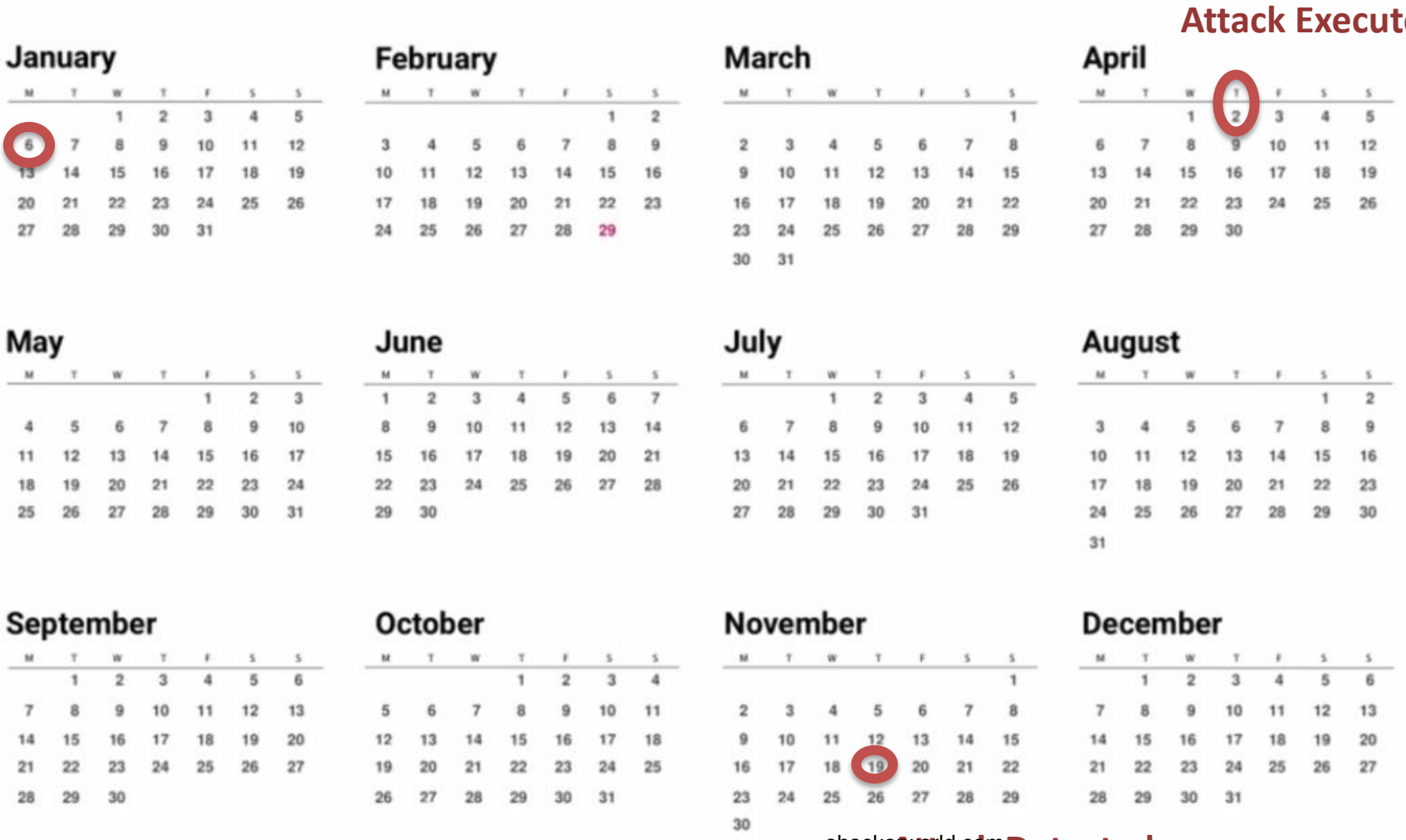
It took **205** days for companies to detected an attack

80 days before the attack, there were indications that the attack would happen

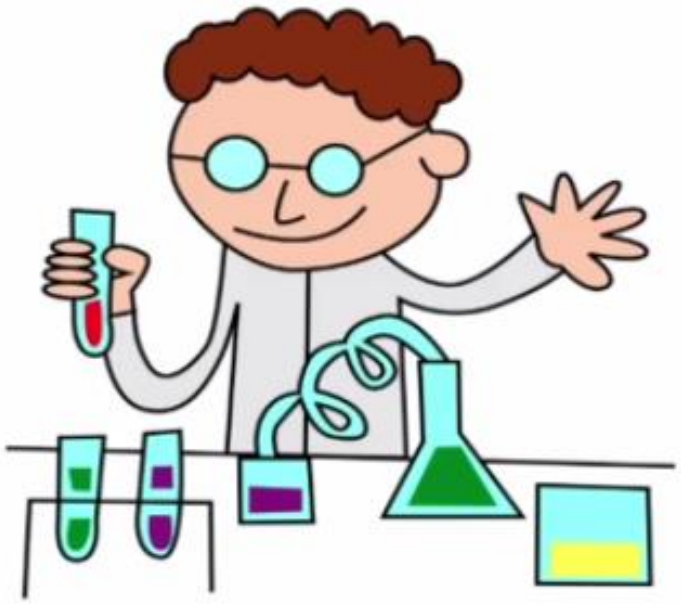
67% of the time the attacks are detected by an external entity

Some findings

Unnoticed Indicators



Root Cause Analysis



Lack of Visibility

Need of Security Monitoring

What should we Monitor

Challenges

There are not easy to read

```
111.111.111.111 - - [08/Jan/2020:11:17:55 -0400] "GET / HTTP/1.1" 200 10801
"http://www.google.com/search?q=log+analyzer&ie=utf-8&oe=utf-8 &aq=t&rls=org.mozilla:en-
US:official&client=firefox-a" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.8.1.7) Gecko/20200108
Firefox/2.0.0.7"
```

NO Standards Followed

Failed Login event - Linux

```
Jun 4 22:14:15 server1 sshd[41458] : Failed password for root from 10.0.
```

Failed Login event - Windows

```
An account failed to log on.
Subject:
   Security ID:  NULL SID
   Account Name:  -
   Account Domain:  -
   Logon ID:  0x0
Logon Type:  3
Account For Which Logon Failed:
   Security ID:  NULL SID
   Account Name:  asdf
   Account Domain:
Failure Information:
   Failure Reason:  Unknown user name or bad pass
ord.
   Status:  0xc000006d
   Sub Status:  0xc0000064
Process Information:
   Caller Process ID: 0x0
   Caller Process Name: -
Network Information:
   Workstation Name: WIN-R9H529RIO4Y
   Source Network Address: 10.42.42.201
   Source Port:  53176
Detailed Authentication Information:
      Logon Process:  NtLmSsp
   Authentication Package: NTLM
   Transited Services: -
   Package Name (NTLM only): -
   Key Length:  0
```

Huge Volume (25 million logs/day) (300 logs/sec)

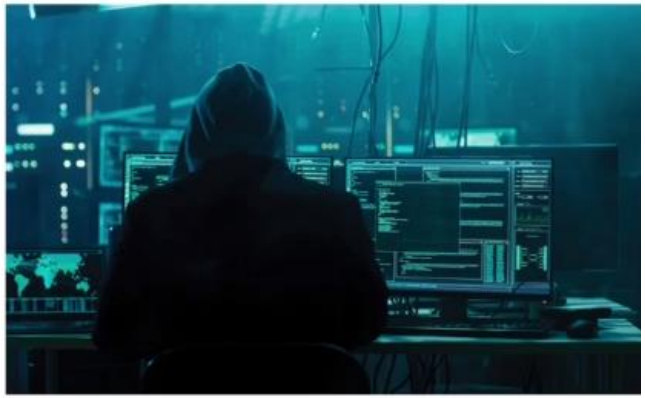
Solution

Security Information & Event Management

what is SIEM?


AD
WWW
DNS
DHCP
WAF
WLAN controller
LOGS
SIEM
Suspicious Activities

Problem



Root Cause

Solution

Real Life Analogy

Problem

Root Cause

Solution

Rule Enforces

- Regional Transport Office (India)
- Department of Motor Vehicle (USA)
- Driver and Vehicle Licensing Agency (UK)

Cyber security Rule Enforcers

- **Regulatory compliances**
- **Industry Best Practices**

PCI Security Standards Council

GDPR

HIPAA Health Insurance Portability & Accountability Act

Security Monitoring

The team that make use of the **SIEM** tool for security monitoring is called

SOC
Security Operations Center

A person who works in SOC is called

Security Analyst
SOC Analyst

Thanks