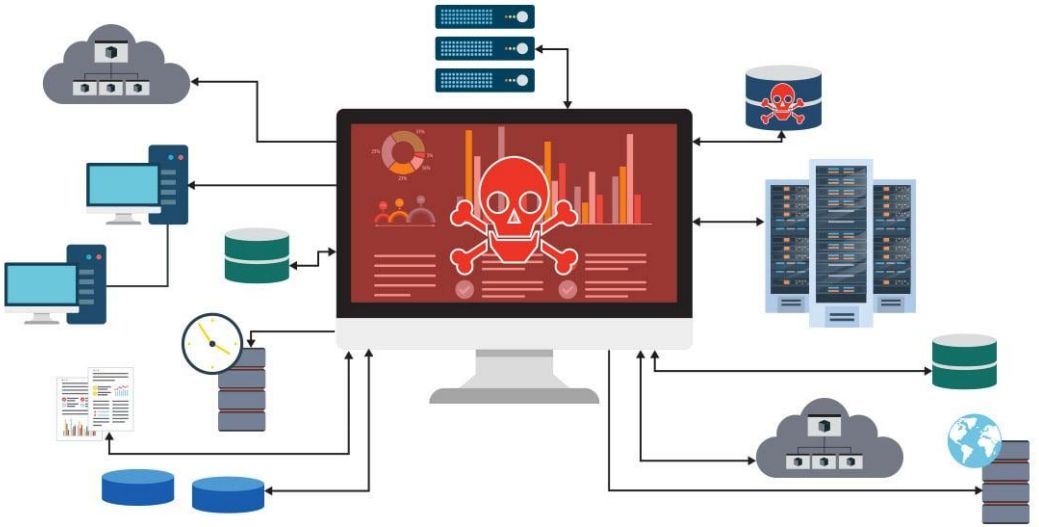
Active Cyber Defense:

From Ransomware Detection to Autonomous Containment



Organized By
Cyber Security Department,
IT Directorate,
National Centre for Physics,
Islamabad.

WELCOME

WE WARMLY WELCOME ALL THE MEMBERS

Workshop Agenda & Objectives

🎯 Goals

Understand **ransomware behavior** and attack methods

Learn **hands-on detection and response** techniques

Gain practical experience with **SIEM monitoring and alerts**

Identify phishing as an initial access vector for ransomware attacks

💼 Agenda Overview

Ransomware fundamentals and lifecycle

Phishing attack simulation (GoPhish demo)

SIEM concepts, setup, and log monitoring

Lab walkthrough and agent deployment

Ransomware simulation and detection exercises (YARA Rules)

Content

Cyber security

Cyber security is the practice by which individuals and organisations reduce the risk of cyber attacks.

Its core purpose is to protect the devices we use every day, including:

- Smartphones
- Laptops
- Tablets
- Desktop computers

Cyber security also safeguards the services we rely on, both online and within the workplace, from theft, disruption, or damage.

In addition, it focuses on preventing unauthorised access to the vast amounts of personal and organisational data stored on devices and across digital platforms.

Cyber security (cont.)

2FA	Password	GDPR-General Data Protection Regulation	Malware	Software	Hardware
Router	DDOS	Breach	Hacker	Ransomware	Firewall
	Social Engineering	Antivirus	Phishing	Cloud	

Cyber security: Myths and reality

Myths	Reality
We are not a target	Every connected system is a target
Antivirus is enough	Modern attacks bypass traditional antivirus
Firewalls will stop all attacks	Firewalls don’t stop phishing or insider threats
Cyber attacks are rare events	Attacks are continuous and automated
If something happens, IT will fix it	Late response = major damage
Backups mean we’re safe	Backups don’t prevent downtime or data leaks

Cyber security as a board-level responsibility

- **Digital dependence:**

Nearly all organisations rely on digital systems and technology to deliver core services and maintain daily operations.

- **Financial impact:**

The cost of responding to and recovering from a cyber incident can be significant, including downtime, recovery, legal, and regulatory expenses.

- **Reputational risk:**

Cyber incidents can severely damage an organisation’s reputation, eroding customer trust and stakeholder confidence.

Cyber security is therefore essential and needs to be understood as an enabler.

Who is Responsible for Cyber security?

- Board & Senior Management

Set strategy, risk appetite, and accountability

- IT & Security Teams

Implement controls, monitoring, and response

- Employees & Users

Follow security practices and report suspicious activity

- Third Parties & Vendors

Maintain secure systems and access controls

Everyone has a role.

Current State of Cybersecurity

- Phishing attacks are still the number one threat.
- Social engineering continues to be the primary method in scams
- Exploitation of zero-day and unpatched vulnerabilities is increasing.
- Ransomware attacks are becoming more frequent and sophisticated.
- AI-driven attacks, including deepfake-based social engineering, are emerging.

Cost of Cybersecurity Attacks

Metric	2024 Value (Ref: IBM Report)
Global average cost of a data breach	$4.88 million (10% increase from prior year)
Avg. cost with multi-environment data visibility gaps	> $5 million
Cost savings with security AI & automation	~ $2.2 million less per breach
Cost impact of staffing shortages	+$1.76 million for severe shortages

Why Ransomware Matters Today

- **Widespread & Growing Threat**

Attacks target **governments, healthcare, education, and enterprises**

Rise of **Ransomware-as-a-Service (RaaS)** lowers entry barriers

- **Severe Financial Impact**

Ransom payments, operational downtime, and recovery costs

Long-term revenue loss and increased cybersecurity spending

- **Data Breaches & Extortion**

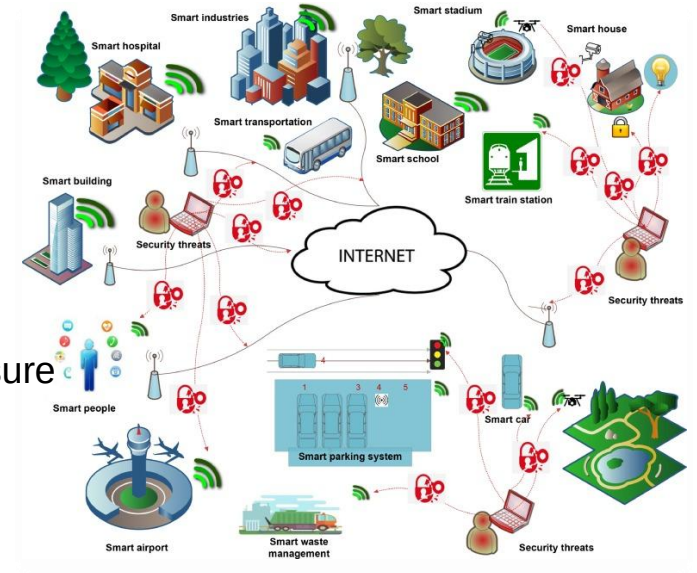
Double and triple extortion: encryption + data theft + public pressure

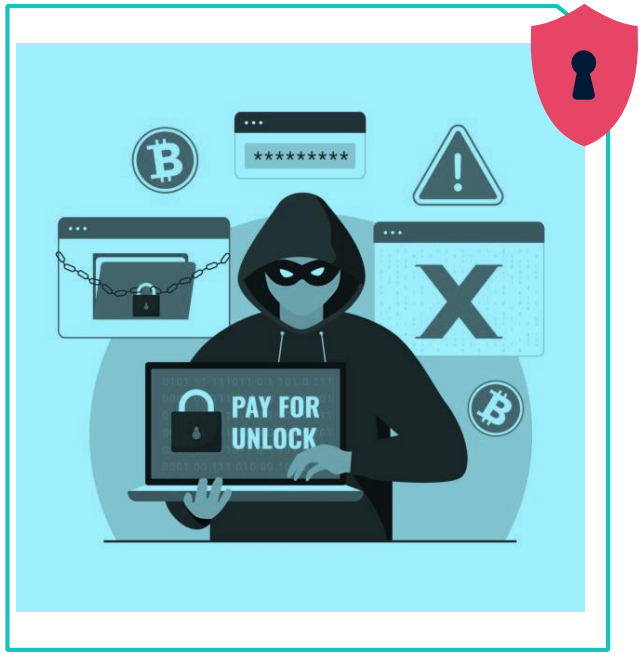
Leads to legal penalties and reputational damage

- **Operational Disruption**

Critical services halted (hospitals, pipelines, power systems)

Supply chains and business continuity affected





OVERVIEW

RANSOMWARE

Understanding how ransomware works, spreads, and impacts modern organizations.

Ransomware

A ransomware attack is a malicious cyber-incident in which malware locks or encrypts data or systems, then demands a ransom payment (often in cryptocurrency) from the victim, promising to restore access or avoid data leakage.

Ransomware is sometimes used to hide the true intent of an attacker:

- They encrypt the files and you think their objective is for you to pay them
- They probably stole your data before encrypting and placed it on the web for sale

How Ransomware Operates

- Executes as a user-level or elevated process
- Performs recursive file system traversal to locate target files
- Uses hybrid encryption (AES for speed + RSA/ECC for key protection)
- Deletes backups and recovery artifacts (Shadow Copies, restore points)
- Generates high-volume file I/O activity during mass encryption

These actions enable attackers to quickly encrypt data, prevent recovery, and increase pressure on victims to pay.

Ransomware Attack Lifecycle

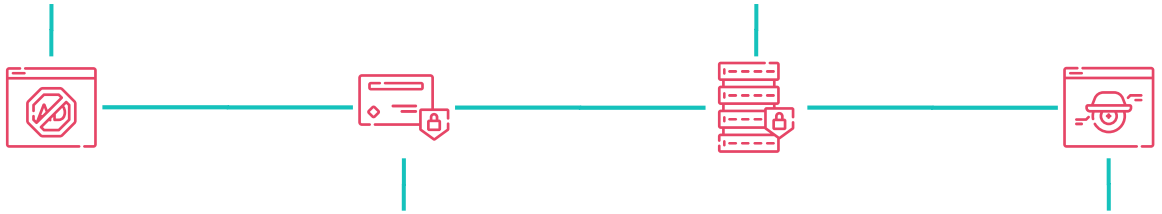
Origins of Ransomware

First known ransomware: AIDS Trojan (1989)

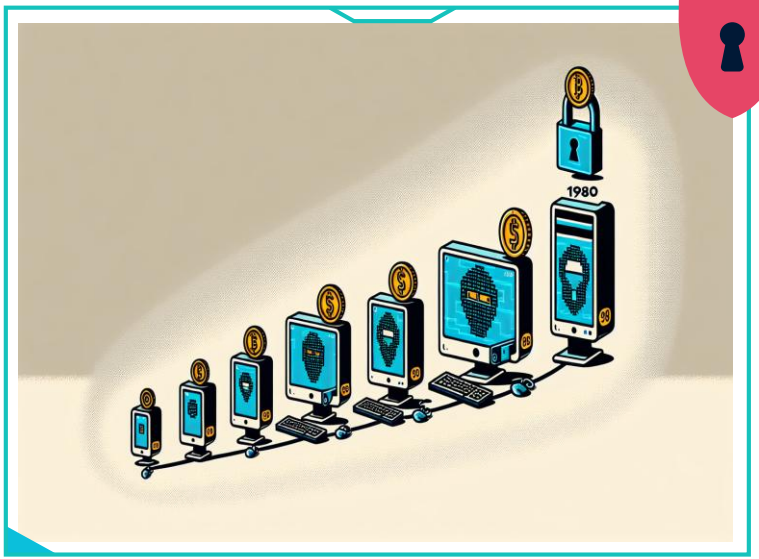
Distributed via infected floppy disks

Used simple symmetric encryption

Payment demanded via postal mail

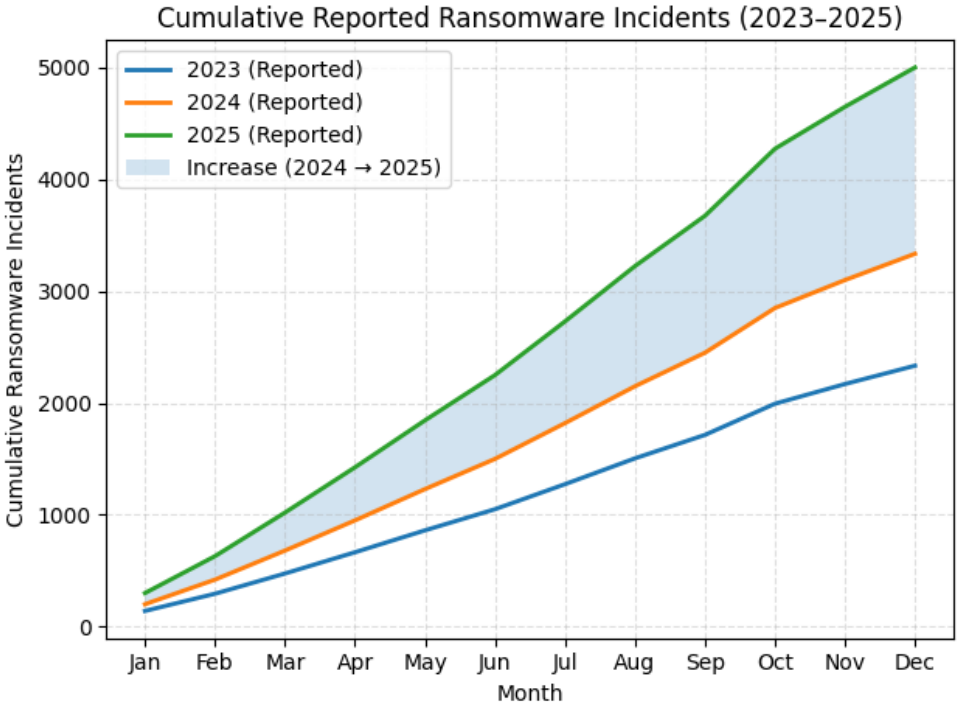


Early ransomware was primitive, limited in scale, and easy to detect.



Ransomware History & Evolution

Ransomware Trends in 2025

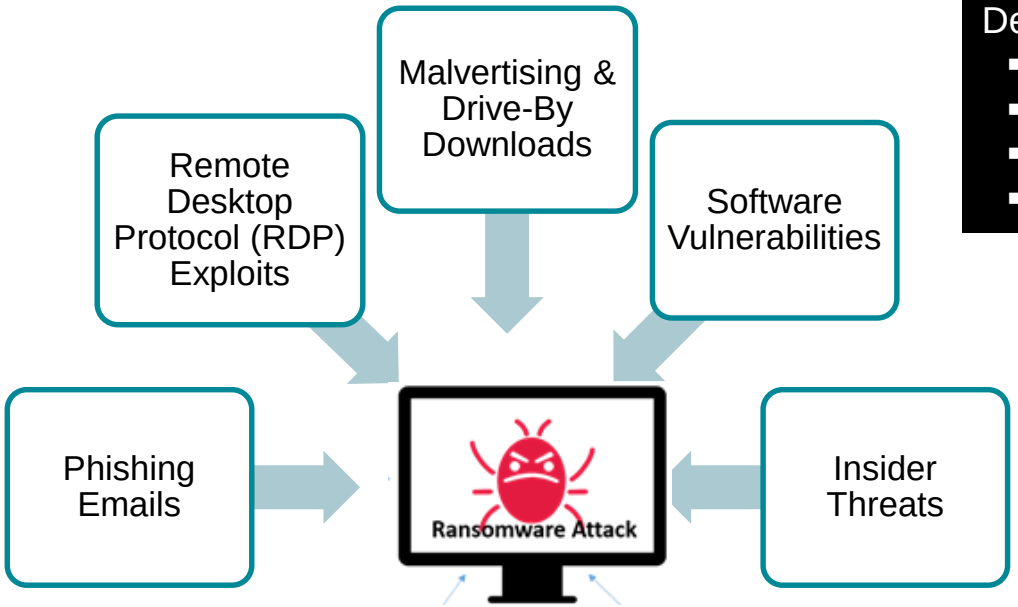


Types of Ransomware

Ransomware can be broadly classified into the following types:

Type	Core Behavior	Examples	Active Period
Crypto Ransomware	Encrypts files and backups using strong cryptography.	WannaCry, Ryuk, LockBit, REvil	2017–Present
Locker Ransomware	Locks users out of systems without file encryption.	Police-themed variants	2012–2016
Double Extortion	Encrypts data and threatens data leaks.	Maze, Conti	2019–Present
Triple Extortion	Adds DDoS or third-party pressure to double extortion.	LockBit 3.0	2021–Present
RaaS	Ransomware-as-a-service model enabling affiliates.	REvil, DarkSide	2018–Present

Ransomware Attack Vectors



Detection Telemetry
- Email gateway logs
- Failed RDP attempts
- IDS exploit alerts
- Authentication anomalies

Attackers often combine multiple vectors for maximum impact.
Network segmentation, patching, and monitoring help prevent infections.

The Three-step Ransomware Attack Playbook

- Phishing emails or malicious attachments
- Exploiting unpatched vulnerabilities
- Weak or stolen credentials (RDP, SSH)

- Executes the ransomware payload
  Disables security tools and backups
  Moves laterally across the network to reach critical systems

- Files and systems are encrypted
  Ransom note is displayed
  Payment is demanded in cryptocurrency to restore access

Ransomware Attack: What Defenders See

- Email logs
- Process creation
- PowerShell execution

- Event ID 4672
- Sudo logs
- SMB auth logs
- PsExec execution

- File modification spikes
- Rename storms
- Ransom note creation

Ransomware Attack: Initial Access

Why Initial Access Matters?

- Most ransomware attacks begin with phishing
- User interaction provides first foothold

Attackers move from **email** → **endpoint** → **network**

Ransomware Attack: Initial Access (GoPhish)

What is GoPhish?

- An Open-source framework to **create, launch, and track phishing emails**
- Simulates real-world phishing campaigns
- Mimics attacker email delivery & user interaction
- Generates realistic initial access events

What This Demonstrates

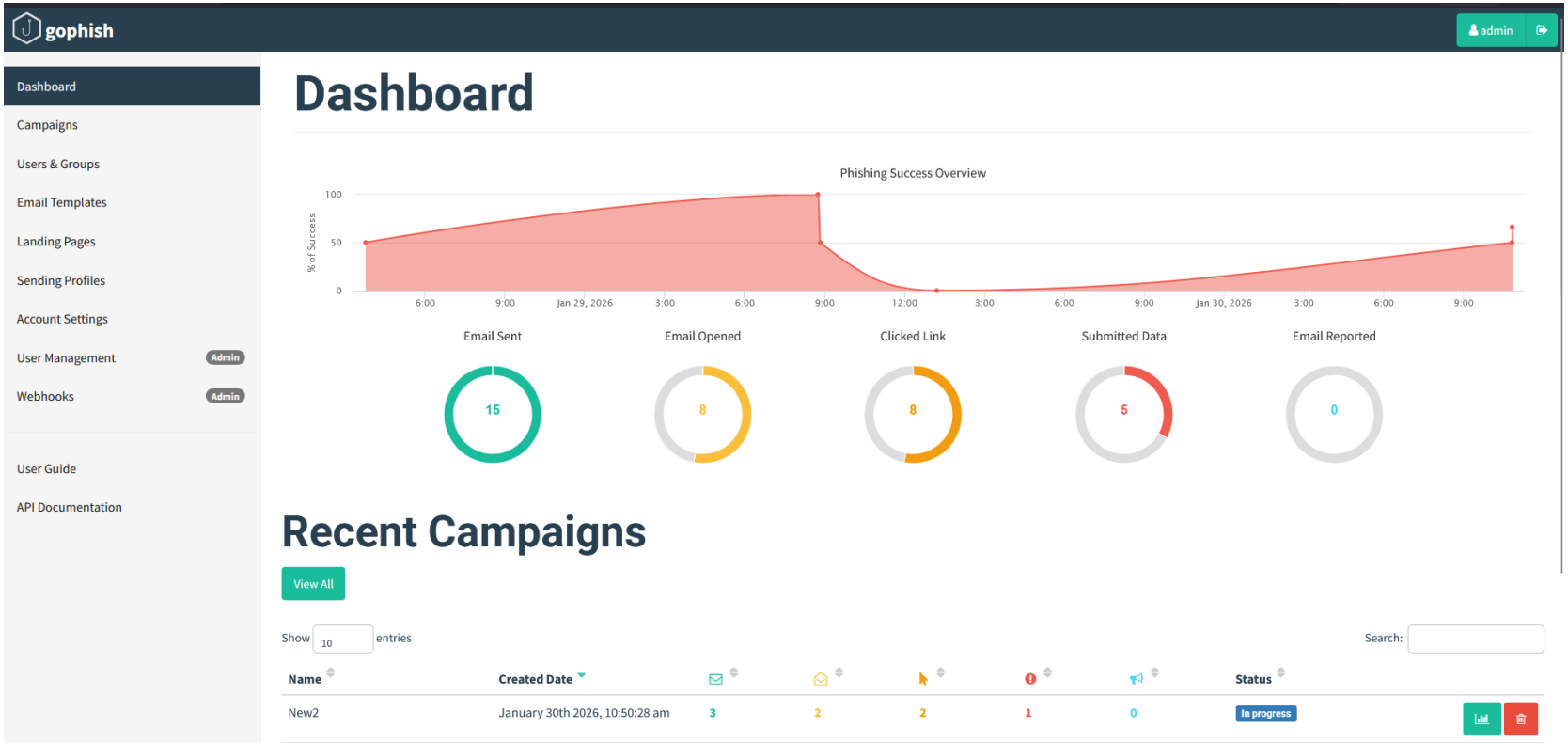
- How ransomware gains entry without exploits
- Visibility of phishing activity in SIEM logs
- Importance of early detection before encryption

How GoPhish Works

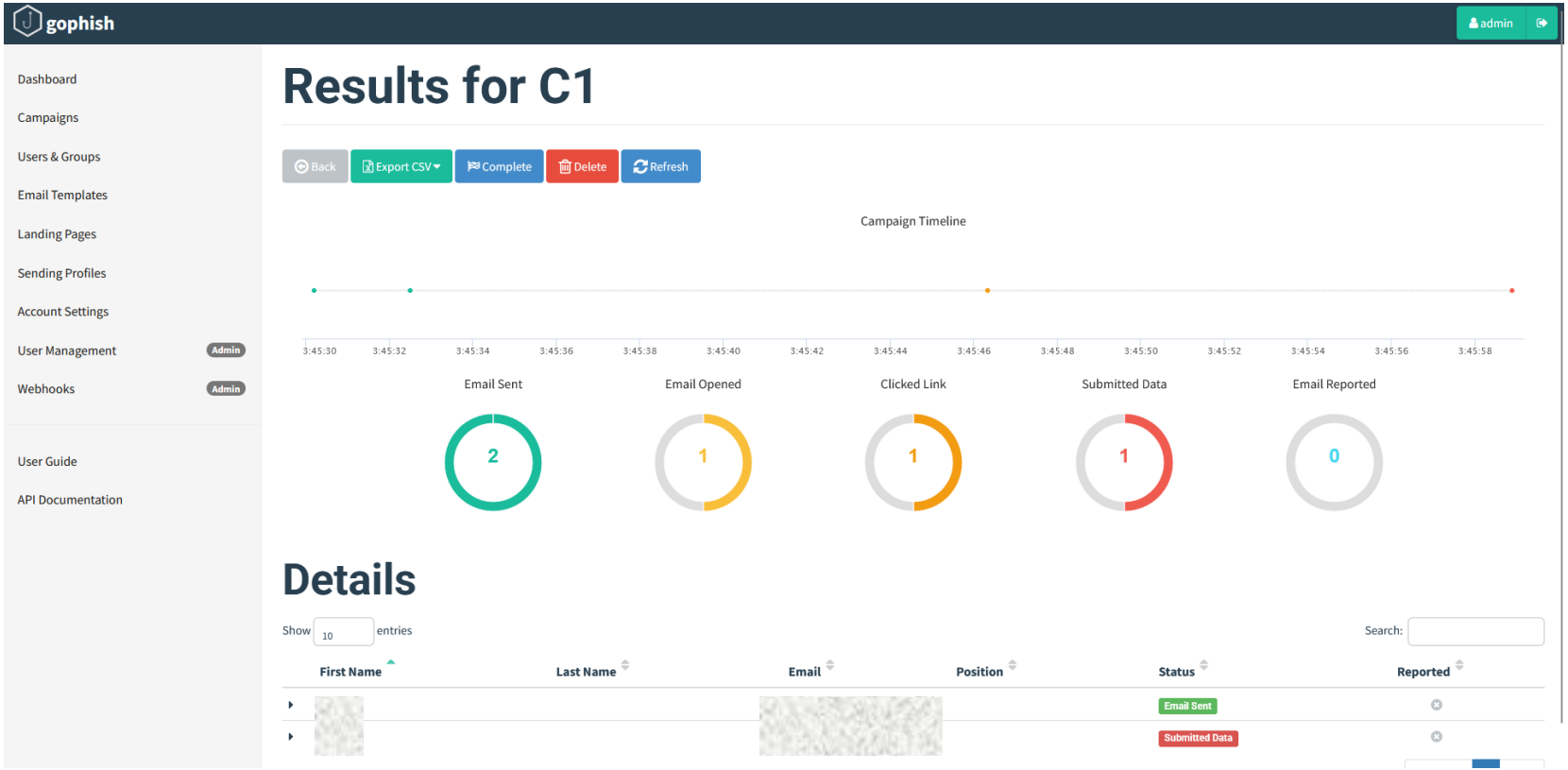
GoPhish simulates real phishing attacks in a controlled lab environment

- Campaign Creation: Attacker-like email templates and target users are defined
- Email Delivery: Phishing emails sent to selected users
- User Interaction: Victim clicks link or opens attachment
- Payload / Landing Page: Malicious script or fake page is triggered
- Initial Access Gained: System becomes entry point for ransomware
- Logging & Monitoring: Events are captured for SIEM analysis

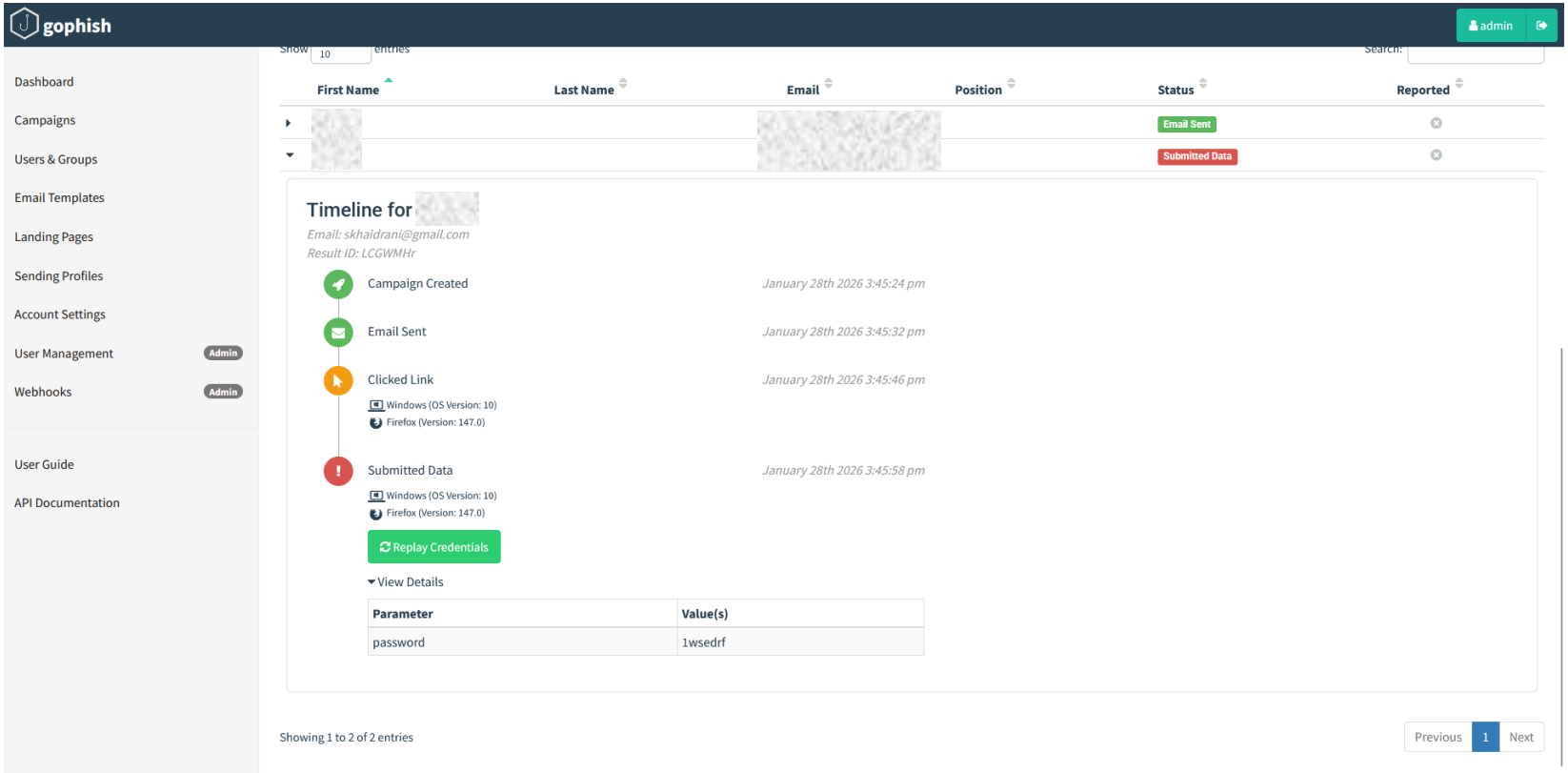
GoPhish


gophish
admin
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Sending Profiles
Account Settings
User Management
Admin
Webhooks
Admin
User Guide
API Documentation
Dashboard
Phishing Success Overview
% of Success
100
50
0
6:00
9:00
Jan 29, 2026
3:00
6:00
9:00
12:00
3:00
6:00
9:00
Jan 30, 2026
3:00
6:00
9:00
Email Sent
15
Email Opened
8
Clicked Link
8
Submitted Data
5
Email Reported
0
Recent Campaigns
View All
Show 10 entries
Search:
Name
Created Date
Status
New2
January 30th 2026, 10:50:28 am
3
2
2
1
0
In progress

GoPhish Cont..



GoPhish


gophish
admin
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Sending Profiles
Account Settings
User Management
Admin
Webhooks
Admin
User Guide
API Documentation
Show 10 entries
Search:
First Name
Last Name
Email
Position
Status
Reported
Email Sent
Submitted Data
Timeline for
Email: skhaidrani@gmail.com
Result ID: LCGWMHr
Campaign Created
January 28th 2026 3:45:24 pm
Email Sent
January 28th 2026 3:45:32 pm
Clicked Link
January 28th 2026 3:45:46 pm
Windows (OS Version: 10)
Firefox (Version: 147.0)
Submitted Data
January 28th 2026 3:45:58 pm
Windows (OS Version: 10)
Firefox (Version: 147.0)
Replay Credentials
View Details
Parameter
Value(s)
password
1wsedrf
Showing 1 to 2 of 2 entries
Previous
1
Next

Lateral Movement in Ransomware

Definition:

Lateral movement is when attackers move **inside a network** after initial access to **spread ransomware**, escalate privileges, and target critical systems.

- Attackers **explore network resources** and identify high-value targets (servers, databases, backups).
- Use techniques like **credential dumping**, **pass-the-hash**, or **RDP exploitation** to move across systems.
- Enables **full-scale ransomware deployment**, maximizing impact across an organization.
- **Defensive Focus:** Monitor unusual internal activity, enforce least-privilege access, segment networks, and log authentication events.

Lateral movement creates abnormal internal traffic patterns detectable by SIEM.

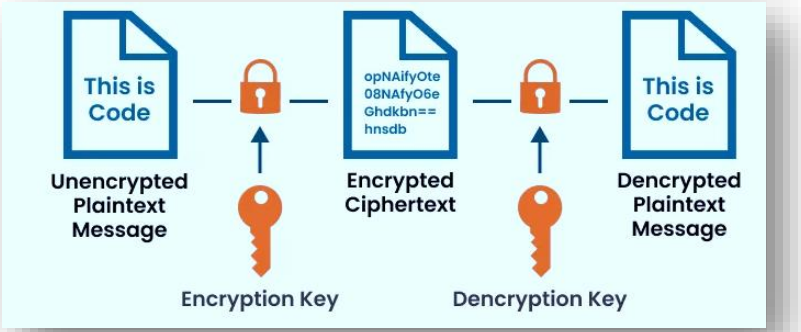
Ransomware Encryption Mechanisms

Encryption overview

Encryption is a security technique used to protect data by converting it into an unreadable format called ciphertext. Only authorized users with the correct decryption key can convert it back into readable form

Why Encryption is Important

- 🔒 Protects sensitive information (passwords, files, messages)
- 🚫 Prevents unauthorized access and data breaches
- 📜 Ensures data confidentiality and privacy
- 🌐 Secures data during storage and transmission



Ransomware Encryption Mechanisms Cont..

- Ransomware uses legitimate cryptographic algorithms
- Relies on hybrid encryption for speed and control
- No custom crypto, abuses standard OS libraries
- Encryption is performed at mass scale, not secrecy

Ransomware Encryption Workflow

File Discovery

- Scans system for valuable files (documents, databases, backups)

Key Generation

- Creates a unique symmetric encryption key

File Encryption

- Encrypts files using fast algorithms (AES)

Key Protection & Exfiltration

- AES key encrypted with attacker's public key (RSA/ECC) and sent to C2

Ransom Note Creation

- Displays payment instructions to victim

🔐 **Why Decryption Is Difficult**

- Uses **strong, industry-grade cryptography**
- Private decryption key is **never stored locally**
- Brute-force recovery is **computationally infeasible**

Hybrid Encryption Model Used by Ransomware

01

AES encrypts victim files

02

RSA / ECC encrypts the AES key

03

Private decryption key never exists on victim system

Why Encryption is Hard to Detect Directly

- AES/RSA operations are legitimate
- Encrypted data appears as random noise
- Crypto API usage is normal behavior

Used by: LockBit, REvil, Conti, DarkSide

Ransomware Encryption Techniques (Modern Methods)

Full File Encryption

- Entire file encrypted
- High security, slower speed

Partial / Chunk Encryption

- Encrypts file headers or random blocks
- Faster, still renders file unusable
- Common in modern ransomware

Multithreaded Encryption

- Uses multiple CPU cores
- Extremely rapid file encryption

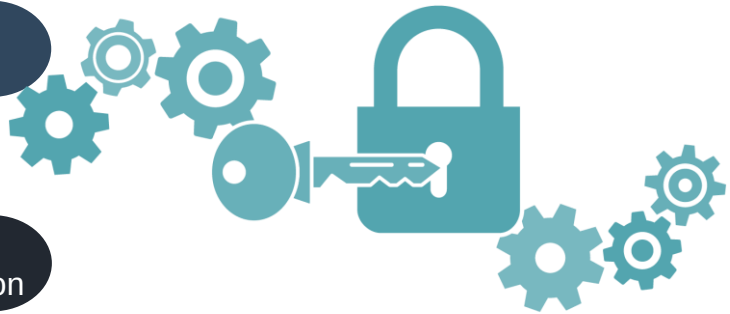
Advanced Encryption Evasion Techniques

Memory-only cryptography
Crypto routines exist only in RAM

OS Crypto API Abuse
Uses legitimate system encryption APIs

Network-dependent key handling
Encryption keys sent to C2 servers

Anti-recovery actions
Shadow copy deletion, Backup service termination



Ransomware does not break encryption; it abuses encryption at a speed and scale no legitimate software ever would

Indicators of Active Ransomware Encryption

As ransomware encrypts files, its activity produces distinct system-level behaviors that can be monitored for detection.

- Rapid overwrite of existing files with encrypted versions
- High-entropy data written to disk (characteristic of encryption output)
- A single process modifying hundreds or thousands of files
- Correlated spikes in CPU usage and disk I/O activity

Ransom and demands

- Hackers request payment settlements via Western Union or text message to conceal their identity.
- Some demand Bitcoin payments for anonymity and to avoid intermediaries.
- Once payment is made, attackers may decrypt files and restore system access.
- Attackers sometimes masquerade as U.S. law enforcement or government officials.
- Common scam: claim the victim’s computer is being shut down due to illegal content or pirated software.
- They demand a “fine” to release control of the system.

Double & Triple Extortion Models

Advanced ransomware tactics used to maximize pressure on victims

- Double Extortion

Step 1: Encrypts victim's files (traditional ransomware)

Step 2: Steals sensitive data and threatens to publish or leak it if ransom isn't paid

Purpose: Forces payment even if backups exist

- Triple Extortion

Step 1 & 2: Same as double extortion

Step 3: Adds external pressure on partners, customers, or public (e.g., DDoS, public shaming)

Purpose: Amplifies coercion and damages reputation

- Relation to Ransomware

Both are evolution of traditional ransomware

Focus on extortion beyond simple encryption

Make attacks more profitable and impactful

Technical Indicators
Large outbound data transfers
Unusual archive creation
Long-running HTTPS sessions

AI-Enhanced Ransomware

AI-enhanced ransomware leverages artificial intelligence and machine learning to adapt, evade, and optimize attacks.

- Smarter targeting: AI identifies the most critical files and systems to encrypt first.
- Evasion of defences: Learns from endpoint detection responses to bypass antivirus and EDR.
- Automated decision-making: Can choose whether to encrypt, steal, or exfiltrate data depending on system behaviour.
- Predictive timing: Executes attacks at optimal times to maximize disruption.
- Defensive Focus: Deploy AI-driven detection tools, anomaly monitoring, and behaviour-based response systems.

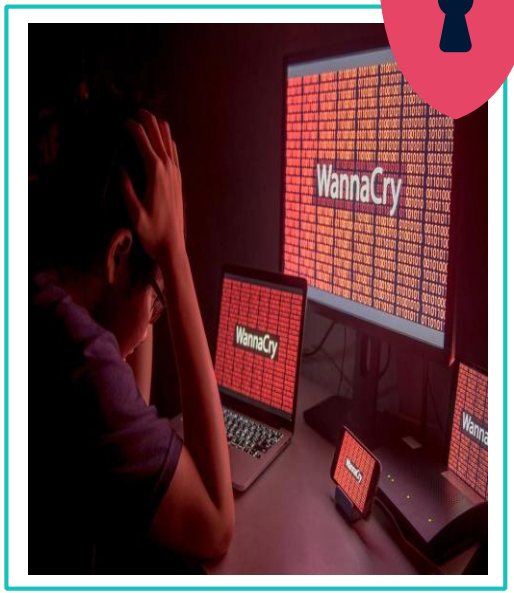
How AI is Changing Ransomware Attacks

- AI scans networks to identify high-value files and weak points
- Malware can bypass antivirus and security tools using AI-driven techniques
- AI optimizes propagation within networks
- AI generates realistic emails/messages to trick users
- AI estimates ransom based on victim profile and ability to pay
- AI creates unique variants to evade detection

Famous Ransomware Attacks

Ransomware Attack	Attack Characteristics	Consequences
WannaCry (2017)	Exploited SMB vulnerability (EternalBlue); self-propagating worm; rapid network spread	Affected over 200,000 systems across 150+ countries; disrupted healthcare, enterprises, and public services
NotPetya (2017)	Disguised as ransomware; destructive wiper malware; leveraged lateral movement techniques	Estimated Financial Impact: 300 million USD Infected Systems: 45,000 PCs and 4,000 servers Affected Facilities: 76 global port terminals shut down
Colonial Pipeline (2021)	Ransomware attack on critical infrastructure; forced operational shutdown	Led to fuel shortages, panic buying, and significant economic disruption across the United States
LockBit (2022–2024)	Ransomware-as-a-Service model; automated propagation; lateral movement and double extortion	Targeted enterprises worldwide; caused major financial losses, data breaches, and operational downtime

Parameter	Details
Attack Name	WannaCry (WanaCrypt0r)
Year	May 2017
Type	Crypto-ransomware with worm capabilities
Target	Windows systems
Exploited Vulnerability	SMBv1 (MS17-010)
Tool Used	EternalBlue (leaked NSA exploit)
Impact	230,000+ systems affected across 150+ countries



Wannacry

WannaCry Outbreak – What Happened

Spread rapidly, infecting thousands of computers within hours

Propagated automatically across networks without user action

Victims discovered the attack only when files were encrypted

Critical services went offline, causing widespread disruption

Contained temporarily via a “kill switch,” highlighting the importance of patching and cyber hygiene

~200,000+

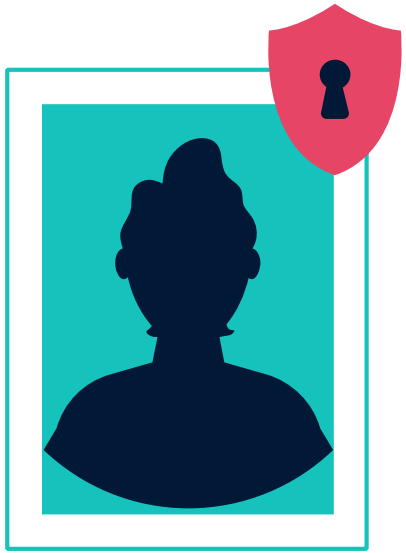
Computers infected worldwide during the outbreak

150+

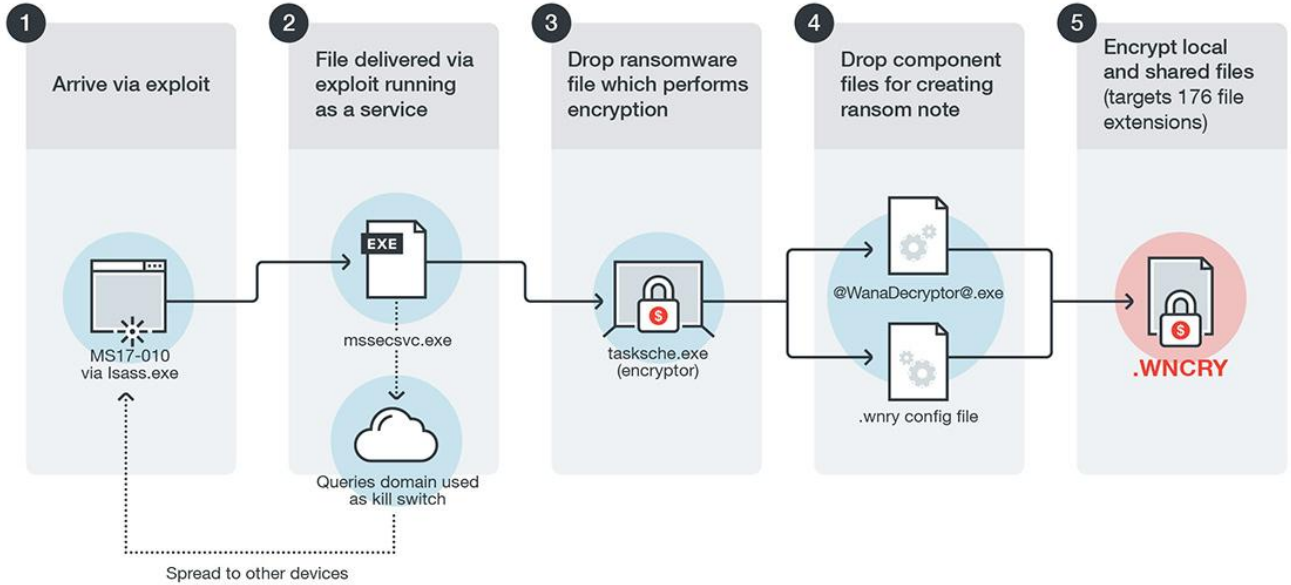
Countries affected globally

230,000+

Systems reported as impacted in some reports



Massive WannaCry



Lessons Learned from WannaCry

- **Global Impact**

Rapid spread across **150+ countries** in hours

Affected **hospitals, businesses, and governments**

- **Importance of Patch Management**

Exploited **unpatched SMB vulnerability (EternalBlue)**

Reinforces need for **regular updates & vulnerability management**

- **Backups Are Critical**

Organizations without backups suffered **irreversible data loss**

Reliable backups reduce ransom leverage

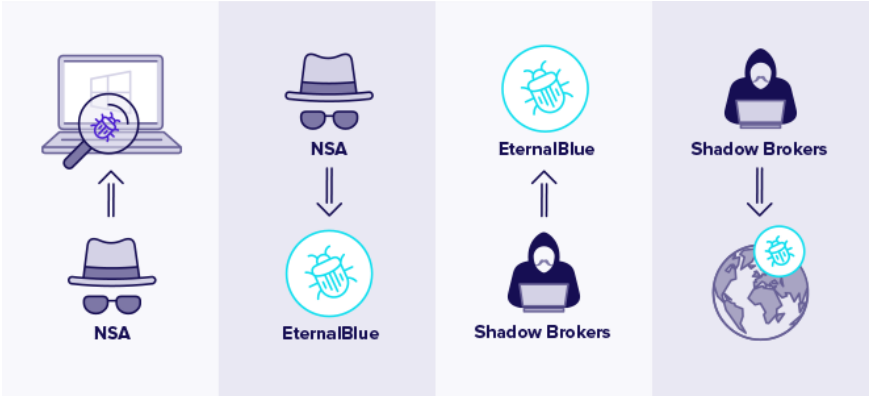
- **User Awareness Matters**

Phishing and careless clicks contributed to infection

Cyber hygiene and training are essential

WannaCry – Detection Opportunities

- SMB exploit traffic (Eternal Blue)
- Sudden file encryption burst
- Worm-like lateral movement
- Kill-switch DNS domain



This shows what could have been detected.

Ransomware Attack Examples and Notable Virus Variants

Ransomware	Type / Platform	Key Characteristics	Targets / Geography	Notes / Timeline
RansomHub	RaaS	Fast encryption, evades EDR	Organizations in US & Brazil	Affiliates: ALPHV, LockBit; ceased April 2025
Akira	Multi-platform (Windows & Linux)	ChaCha2008 encryption, intermittent file encryption, data theft, uses phishing & VPN exploits, LOLBins, credential dumping	Education, Finance, Manufacturing, Healthcare	Flexible attack pattern (encrypts or steals)
Play / Playcrypt	RaaS	Double extortion, intermittent encryption, exploits FortiOS & exposed RDP	High-profile organizations globally	Active since 2022
Qilin	Rust-based RaaS	Double extortion, customized attacks, proprietary leak site	Variable (new affiliates post-RansomHub)	Started 2025; targets high-value victims
Other key variants	RaaS / ransomware families	File encryption, data theft, high-profile targets	Global	Includes LockBit, DearCry, Maze, Lapsus$

Ransomware Attack Case Studies

Costa Rica (2022)Type: Conti ransomware

Targets: Government ministries and institutions

Impact:

Declared national emergency due to shutdown of public services

Payment demands disrupted tax, health, and customs operations

Lesson Learned:

Critical infrastructure requires sector-specific backup strategies

Employee awareness and network segmentation are vital

Ransomware Attack Case Studies Cont..

Portugal (2023)Type: LockBit ransomware

Targets: Healthcare and municipal services

Impact:

Hospitals and local authorities experienced system outages

Patient care and municipal services were temporarily halted

Lesson Learned:

Healthcare organizations must implement continuous monitoring

Importance of offline backups and rapid incident response

Ransomware Attack Case Studies Cont..

Colonial Pipeline (USA, 2021)

Type: DarkSide ransomware

Targets: Pipeline operations and fuel distribution

Impact:

Shutdown of fuel pipeline for several days

Panic buying and supply chain disruption across the eastern US

Company paid ransom (~$4.4 million in Bitcoin) to restore operations

Lesson Learned:

Critical energy infrastructure needs **robust segmentation** and **incident response planning**

Supply chain resilience and threat intelligence sharing are key

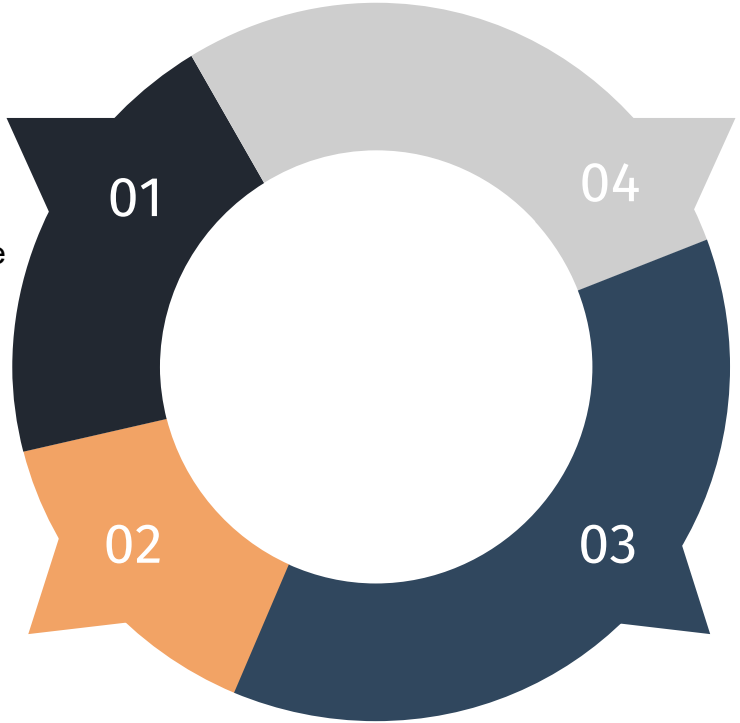
Business Impact of Ransomware Attack

Legal Impact

Unauthorized access to sensitive data → lawsuits, fines, compliance violations (e.g., GDPR, HIPAA) → loss of customer trust

Financial Impact

Revenue loss during downtime, ransom payments, legal fees, and security upgrades → especially severe for SMEs



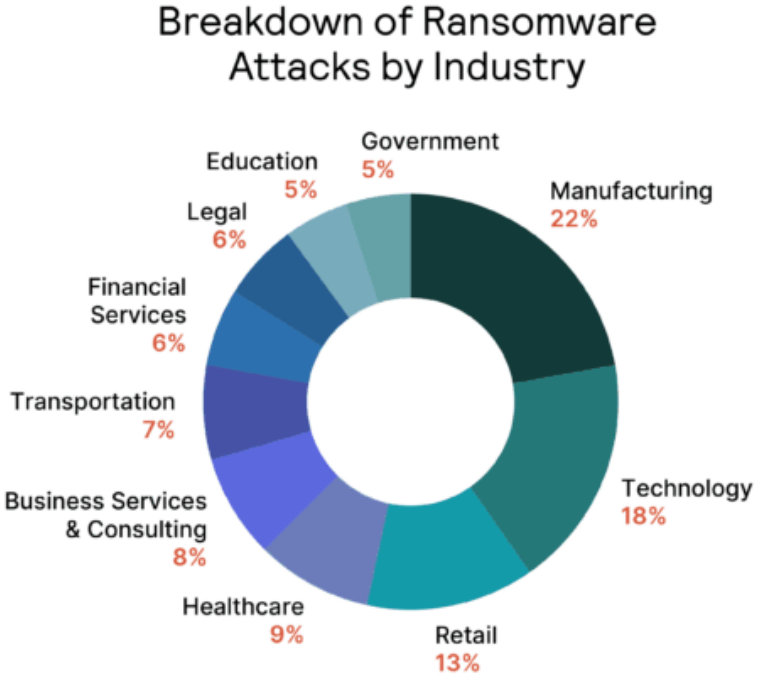
Reputational Impact

Brand damage from public disclosure and negative media coverage → loss of stakeholder confidence and customers

Operational Impact

Disruption of daily operations, delayed services, productivity loss, supply chain delays, and IT strain during recovery

Ransomware Targeted Industries



FLASHPOINT

Ransomware Detection & Response

- Employee Awareness

  Train staff to identify phishing emails, suspicious links, and unsafe attachments.

- Honeypots

  Deploy decoy files to lure and detect ransomware activity.

- Network & Endpoint Monitoring

  Log traffic, scan for anomalies, and establish behavioral baselines.

- Security Tools

  Use antivirus and anti-ransomware solutions with whitelisting and threat alerts.

- Email Protection

  Block malicious emails and risky file types before they reach users.

Early Warning Signs of a Ransomware Attack

- **Process-Level Indicators**
  - Sudden system slowdown or crashes
  - Frequent application errors or freezes
  - Unknown or suspicious processes running
  - High CPU or memory usage from non-standard processes
- **File-System Indicators**
  - Unexpected file extensions appearing
  - Files becoming inaccessible or unreadable
  - High volume of file modifications in short time
  - Ransom note files created in multiple directories
- **Network-Level Indicators**
  - Unusual outbound network connections
  - Repeated beaconing to unknown domains/Ips
  - Large or abnormal data transfers
  - Connections detected by IDS/EDR tools
- **Privilege & Authentication Indicators**
  - Unauthorized login attempts
  - Sudden privilege escalation events
  - Admin actions from non-admin accounts
  - Security controls being disabled

Ransomware Detection & Response (Cont.)

Detection Signals

- Bulk file rename
- File modification spikes
- Privilege escalation
- Shadow copy deletion
- Canary file access

Correlation Logic

Example:

```
Privilege escalation
+ Shadow copy deletion
+ File modification spike
= High confidence ransomware
```

Detecting Advanced Ransomware (Cont.)

Behavioral Anomaly Detection (EDR / XDR)

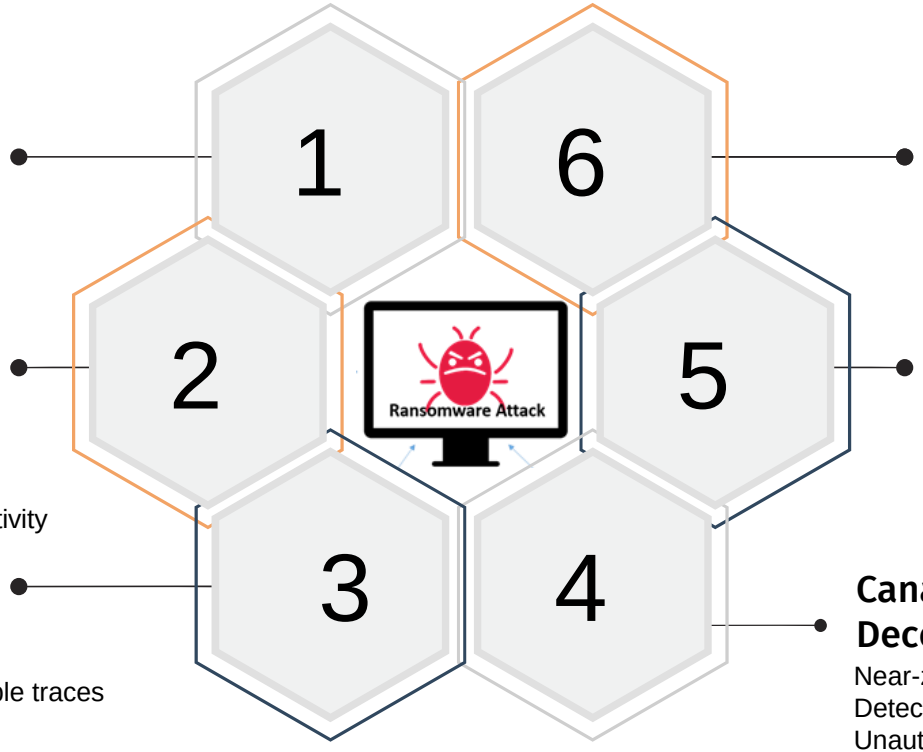
AI ransomware evades signatures
Behavior cannot be hidden
Abnormal file write storms
CPU & disk I/O spikes
Suspicious process execution

SIEM Correlation & Kill-Chain Detection

Single alerts ≠ attack
Correlated events = confidence
Privilege escalation + file modification
Backup deletion + encryption activity
Multi-host ransomware spread

File System Activity Monitoring

Encryption leaves unavoidable traces
Bulk file modifications
Rapid file renaming
High-entropy file writes



YARA-Based Malware Identification

Identifies ransomware families
Works even with polymorphic malware
Ransom note strings
Binary artifacts
In-memory malware patterns

Memory & Runtime Analysis (YARA + EDR)

AI ransomware hides on disk
Memory reveals real intent
In-memory encryption routines
Process injection
Unpacked ransomware code

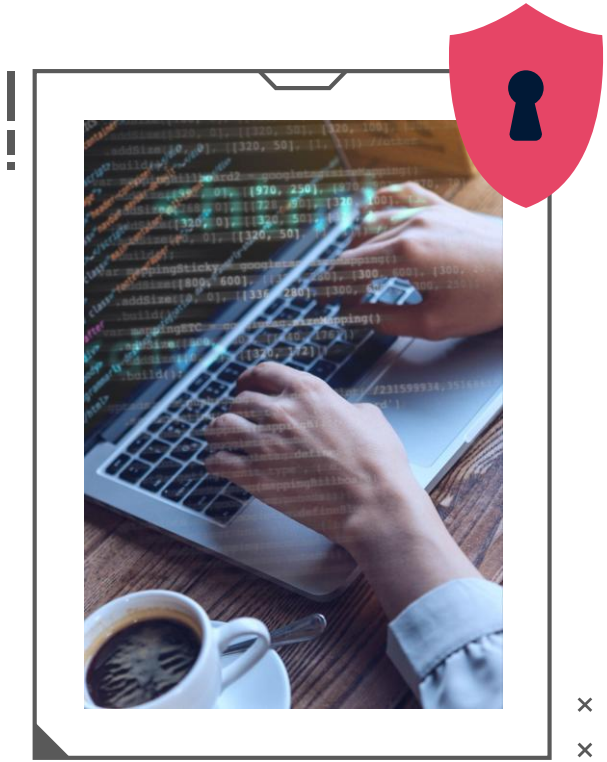
Canary Files & Deception Techniques

Near-zero false positives
Detects encryption early
Unauthorized access to decoy files
Early ransomware execution

SIEM Correlation & Kill-Chain

Cyber Kill Chain Stage	Ransomware Detection Method
Reconnaissance	• Threat intel, scanning alerts
Weaponization	• YARA, sandboxing
Delivery	• Email security, phishing detection
Exploitation	• EDR behavior analysis
Installation	• File/registry monitoring, YARA
C2	• DNS & network anomaly detection
Actions on Objectives	• Encryption behavior detection

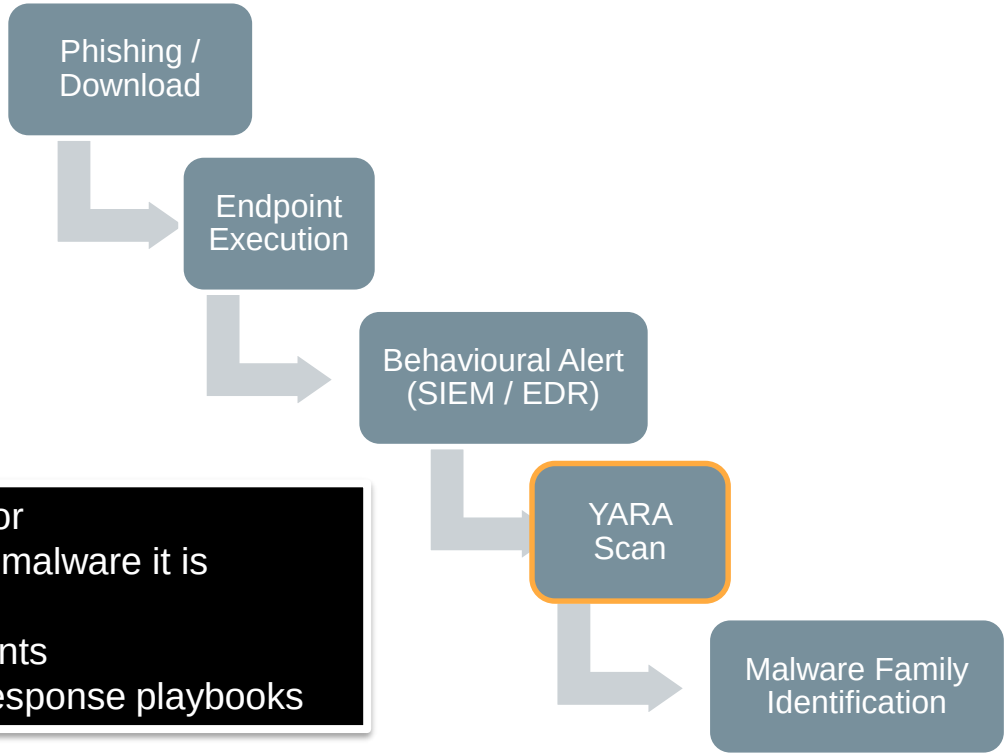
YARA – Malware Detection & Classification



What is YARA & Why Blue Teams Use It

- Pattern-matching tool for malware identification
- Used by SOCs, DFIR, threat hunters
- Detects
  - Known ransomware families
  - Variants with reused code
- Complements SIEM & EDR
- YARA detects malware artifacts, not encryption activity itself.
- Widely used for **security testing and awareness**
- Mimics real attacker phishing campaigns in a controlled lab

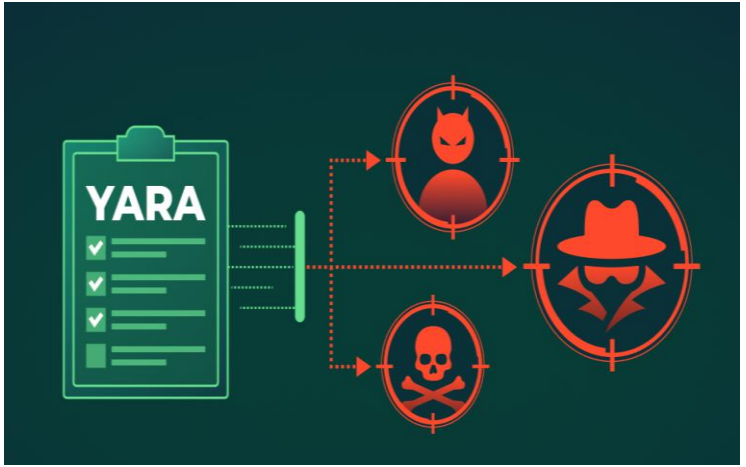
YARA in the Ransomware Detection Workflow



- SIEM detects behavior
- YARA confirms what malware it is
- Helps analysts
  - Prioritize incidents
  - Apply correct response playbooks

Where YARA Detects Ransomware

Layer	What YARA Scans
Files	Ransomware binaries
Memory	Injected code
Disk	Dropped payloads
Email	Attachments



Anatomy of a YARA Rule

Rule Structure

- Meta: rule description & author
- Strings: malware indicators
- Condition: logic for detection

Detection Logic

- String matching
- Hex patterns
- Boolean conditions

Visual

Rule blocks highlighted (meta / strings / condition)

Example

```
rule Simple_Suspicious_Strings
{
    meta:
        description = "Detects basic suspicious
                       indicators"
        author = “Team A"
        date = "2026-01-19"

    strings:
        $cmd        = "cmd.exe"
        $powershell = "powershell"
        $url        = "http://"

    condition:
        any of them
}
```

Ransomware Artifacts in YARA Rules

Detects

- Ransom note phrases
- File extension patterns
- Encryption library strings
- Mutex and API references

String Examples

"Your files have been encrypted"
.locked, .encrypted
CryptEncrypt
AES_set_encrypt_key

Shows Indicators mapped to ransomware stages

Ransomware Example

```
rule Simple_Ransomware_Indicator
{
  meta:
    description = "ransomware Indicator"
    author = "Blue Team"
    reference = "Internal Detection"

  strings:
    $s1 = "Your files have been encrypted"
    $s2 = "encrypted"
    $s3 = ".locked"

  condition:
    2 of them
}
```

In-Memory Ransomware Detection with YARA

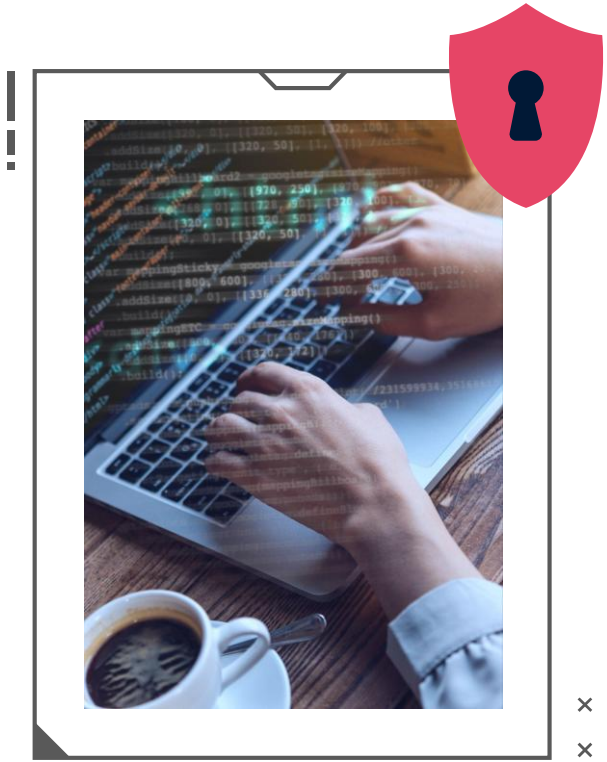
Why Memory Matters?

- Modern ransomware executes directly in RAM
- Binaries are often packed, encrypted, or fileless
- Malware may delete itself from disk after execution
- Disk-based antivirus may see nothing suspicious
- Decrypted ransomware code

YARA Detects in Memory:

- Decrypted ransomware payloads after unpacking
- Encryption routines loaded at runtime (AES, RSA APIs)
- Injected code inside legitimate processes
- Reflective DLL and shellcode patterns

Ransomware Simulation & SIEM Setup



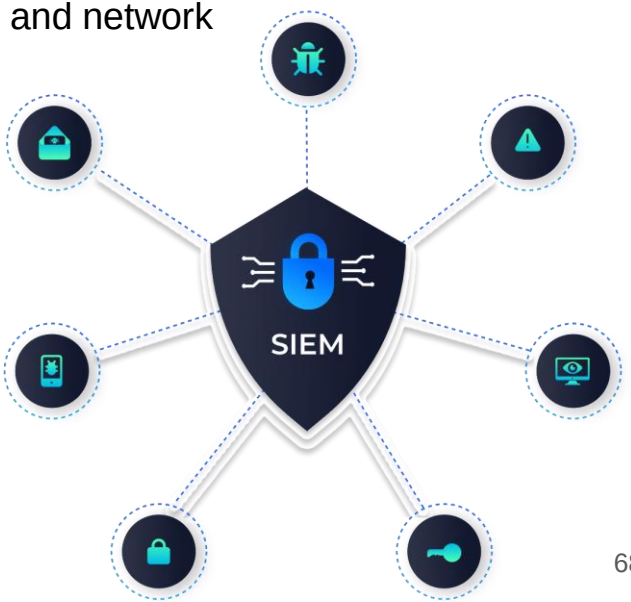
SIEM Overview

What is SIEM?

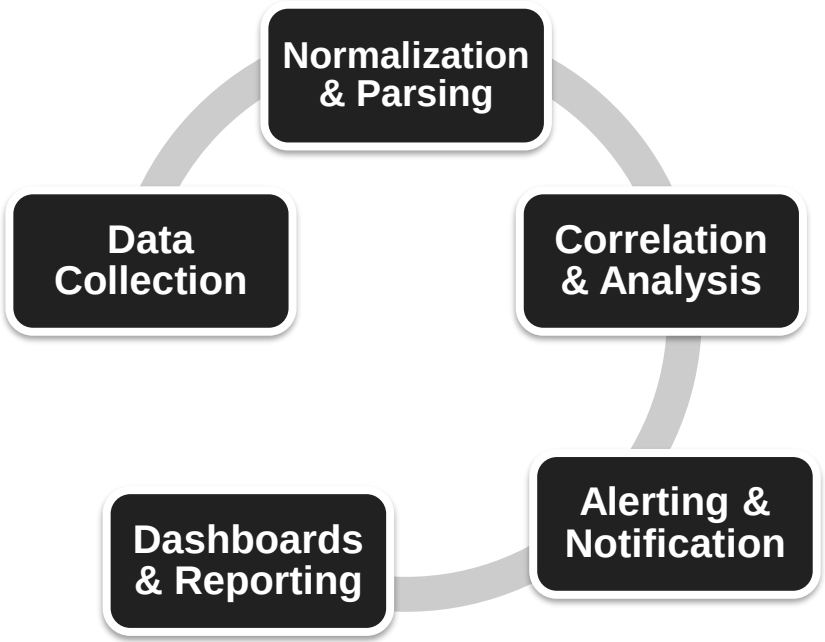
SIEM = Security Information & Event Management
Centralized platform to monitor, detect, and respond to security threats
Provides visibility across endpoints, servers, and network

Key Benefits

Detect anomalies and suspicious activity
Correlate events from multiple sources
Enable faster incident response



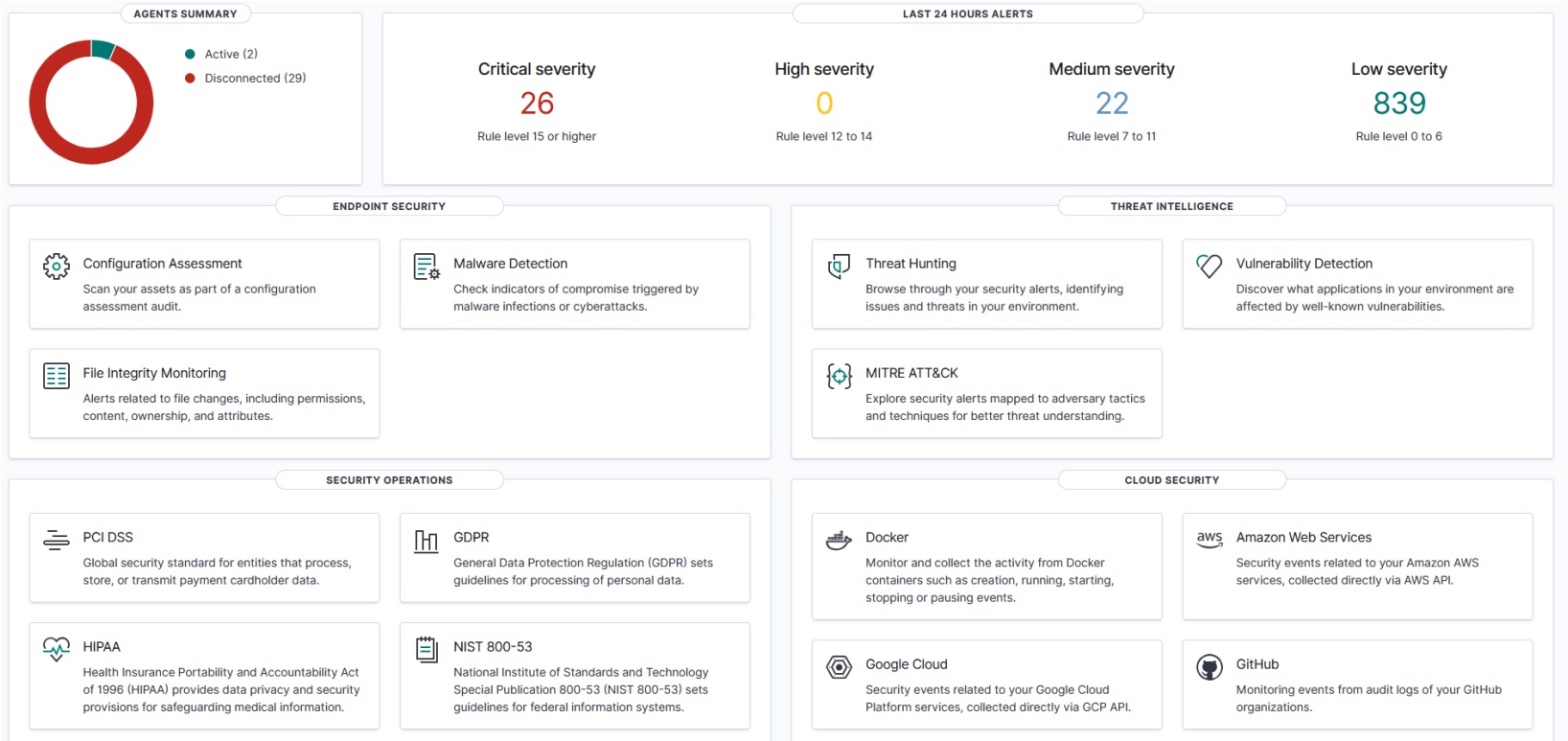
How SIEM Works



Key SIEM Components

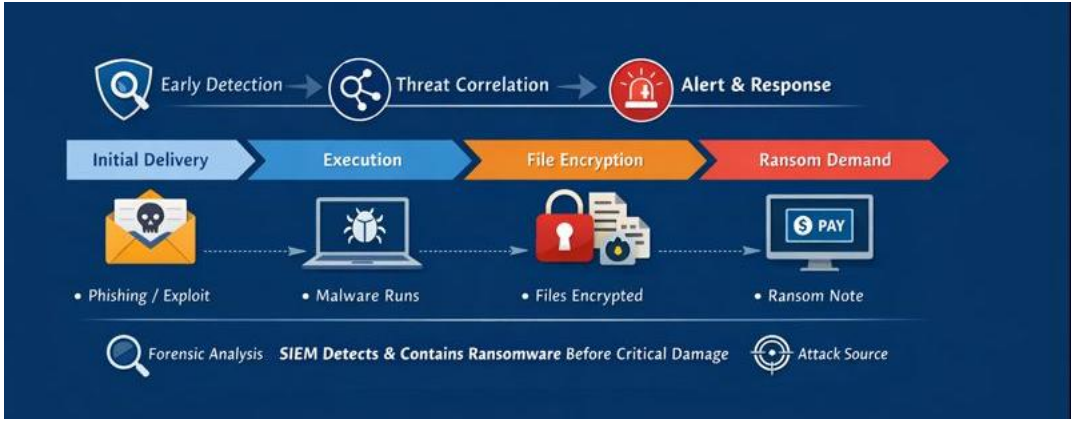
Component	Purpose / Function	Example / Notes
Log Collection	Collects logs from servers, endpoints, network devices, and applications	Syslog, API-based collection
Normalization	Converts collected data into a **standard format** for analysis	Removes inconsistencies across sources
Correlation Engine	Detects patterns and relationships across events	Identifies suspicious behavior, e.g., multiple failed logins followed by a file access
Alerting & Notification	Generates alerts for potential threats	Email, SMS, or SIEM dashboard notifications
Dashboards & Reporting	Provides **visual summaries** of security posture	Trend graphs, compliance reports, incident summaries
Threat Intelligence Integration	Uses external feeds to enrich detection	IOC feeds, malware signatures, MITRE ATT&CK references
Incident Response Automation	Automates responses to detected threats	Blocking IPs, isolating hosts, triggering scripts

SIEM dashboard



Why SIEM Is Important

- Detects ransomware early in the attack lifecycle
- Correlates malicious behavior across multiple endpoints
- Provides actionable alerts to contain attacks before encryption
- Supports forensic analysis to understand attack impact and source



SIEM Use Cases & Detection Scenarios

Unusual Login Activity

Multiple failed attempts, logins from odd locations or hours

Privilege Escalation

Unauthorized role changes or access attempts

Suspicious Processes

Unknown or malicious programs, ransomware behavior

Data Exfiltration

Large or unusual file transfers, sensitive file access

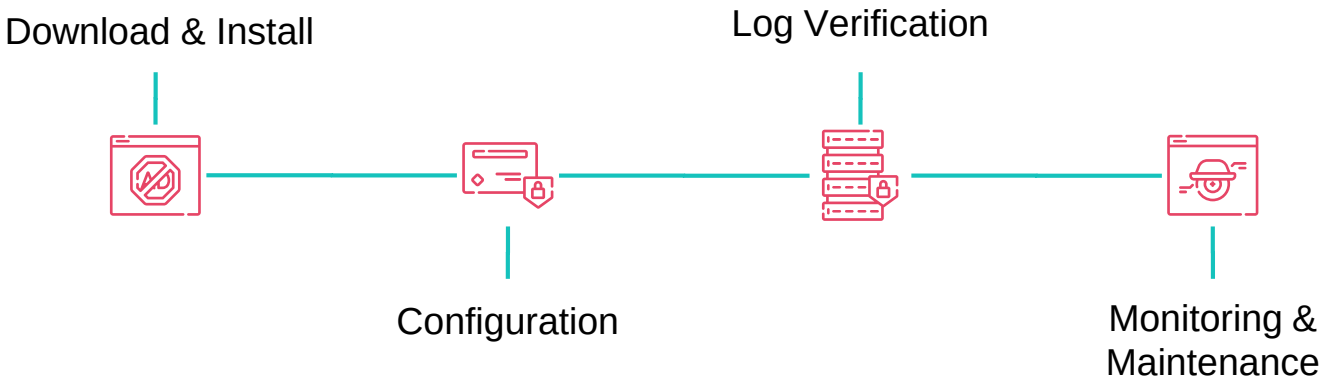
Network Anomalies

Unexpected internal connections, known malicious IPs

Lab Setup & Environment Walkthrough

Component	Purpose	Key Configuration	Expected Activity / Traffic
Attacker VM	Simulates ransomware attack behavior	Kali / Linux-based OS Attack tools enabled Isolated test network	Generates malicious traffic Attempts lateral movement Sends exploit & command traffic
Client VM	Victim system under attack	Windows OS SIEM agent installed User-level access enabled	Receives attack payloads Generates security logs Sends logs to SIEM server
SIEM Server	Centralized monitoring & analysis	Log correlation rules Alerting enabled Dashboard configured	Collects logs from Client VM Correlates suspicious activity Triggers security alerts
Network Overview	Defines communication paths	Isolated lab VLAN Controlled routing No internet exposure	Attacker → Client traffic Client → SIEM log forwarding Monitoring-only traffic

Deploying SIEM Agents



Detection in SIEM – Anomaly & Threat Detection

How SIEM Detects Anomalies

- Event Correlation: Links related events from multiple sources
- Baselining: Compares activity against normal behavior patterns
- Anomaly Detection: Flags deviations from normal trends

Threat Detection Use Cases

- Unusual login attempts or brute-force attacks
- Privilege escalation activities
- Suspicious processes or malware execution
- Abnormal file access or exfiltration

Threat Hunting

- What is Threat Hunting?

Proactive process of searching for hidden threats in the network before they trigger alerts.

- Why it Matters:

Detect advanced threats early

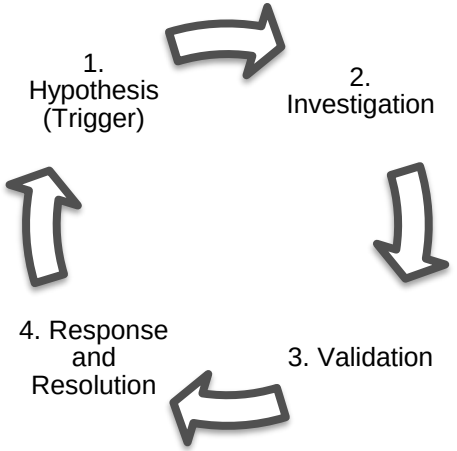
Reduce dwell time of attackers

Complement SIEM detection and automated alerts

- Approaches:

Proactive: Analysts actively search for threats using hypotheses

Reactive: Investigate alerts generated by SIEM or security tools



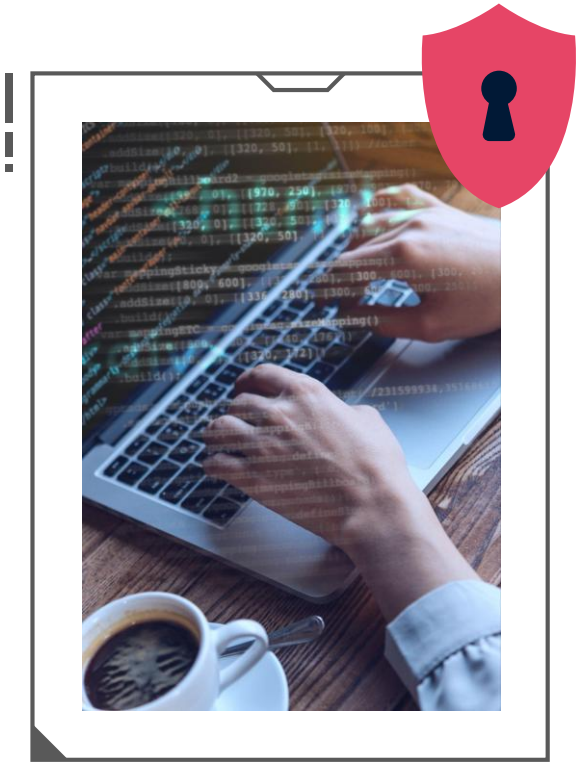
Threat Hunting – Practical Techniques

Icon	Technique	Description
🔍	**Queries**	Search SIEM logs for unusual patterns and anomalies.
□	**Indicators of Compromise (IOCs)**	Use known malicious IPs, hashes, domains to identify threats.
📈	**Behavioral Patterns**	Monitor for abnormal user or system behaviors (e.g., unusual processes, lateral movement).

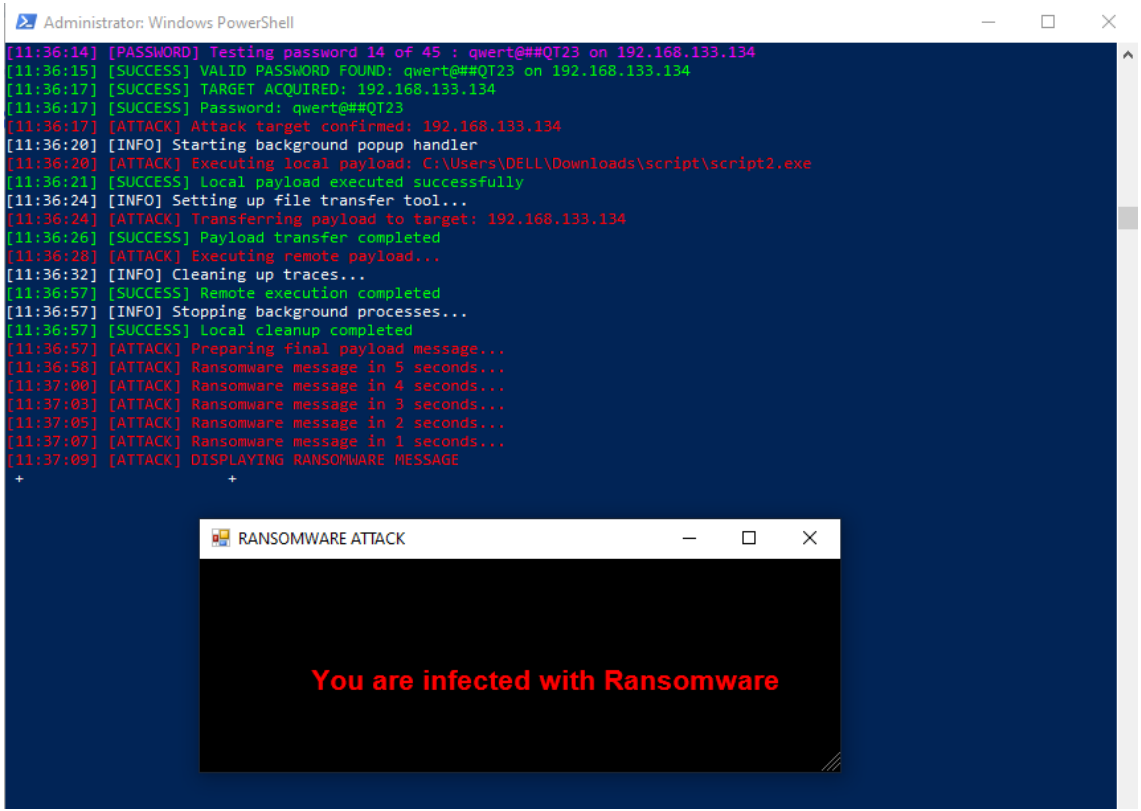
Threat Detection Use Cases

Icon	Step	Description
	Log Collection	Aggregates data from endpoints, servers, and network devices.
	Correlation	Connects related events to detect anomalies.
	Alert Generation	Flags suspicious activity for investigation.
	Investigation	Analysts review alerts and take action.

Hands-On: Ransomware Simulation



Ransomware Attack in Action



Automated Network Isolation & Containment

Purpose:

Prevent the spread of malware/ransomware within a network

How it Works:

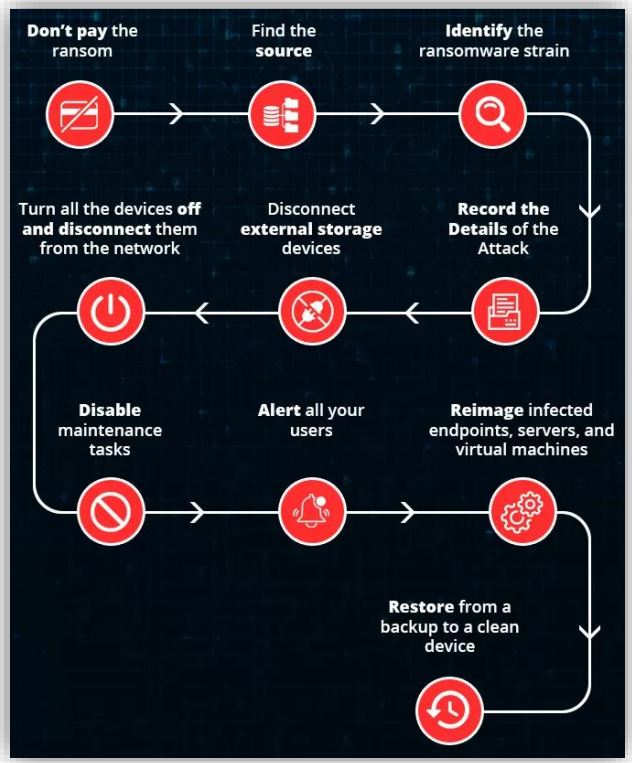
- SIEM detects suspicious or malicious activity
- Automated system or SOAR triggers isolation of the affected host(s)
- Stops lateral movement and limits impact

Practical Demo / Implementation

- SIEM generates an alert on ransomware or anomaly
- Predefined playbook triggers network isolation
- Affected VM or endpoint is automatically segregated
- Security team investigates safely without risk to others

Responding to A Ransomware Attack

- Isolate infected systems immediately
- Disconnect network, Wi-Fi, and external drives
- Do not pay the ransom
- Identify ransomware type & attack vector
- Notify IT/security team and management
- Preserve logs and evidence



What to Expect After a Ransomware Attack

- Significant slowdown in business operations and productivity loss
- Upgrade antivirus and security systems to prevent future attacks
- Employee training on ransomware awareness and prevention
- File recovery, including decryption of targeted files like Microsoft Office documents
- Operational frustration among staff and management due to disruptions

How to Prevent Ransomware Attacks: 8 Key Strategies


Cybersecurity isn’t just IT’s problem — it can shut down hospitals, factories, and governments overnight

Conclusion

- Ransomware is a high-impact, rapidly evolving threat across all industries.
- Modern attacks combine encryption, data theft, and multi-layer extortion.
- AI-driven techniques have increased the speed and sophistication of attacks.
- Early detection using SIEM and proactive threat hunting is critical.
- Real-world incidents highlight the cost of weak security controls and delayed response.
- Hands-on, practical training bridges the gap between theory and real-world defense.
- Live simulations and labs build confidence in detection, response, and recovery.
- A layered security approach significantly reduces ransomware risk and impact.

THANKS!

Do you have any Questions?