

Malware Analysis and Prevention Strategy

Team Presentation by : **Breach Blockers 2025**

Overview of our four-week cybersecurity project on malware analysis, SIEM, and prevention.






Meet the Team

Team Members


- Ahmed Elkamash
- Naira Abdelsalam
- Saif Reda
- Mohamed Saad
- Aya Mohamed El-araj
- Mostafa Ezzat
- Rawan Hossam

Project Timeline

| | | |
|--------|---------------------------------|-------------------------|
| Week 1 | Malware Analysis | Report + Presentation |
| Week 2 | SIEM Configuration & Monitoring | Config Docs + Alerts |
| Week 3 | Prevention Strategy & Training | Strategy + Materials |
| Week 4 | Final Report & Presentation | Report + Slides + Notes |

 Google Drive

DEPI Project Deliverables – Google Drive



Types of Malware

Malware is a software that is designed to attack, control and



Week 1 – Malware Analysis

Malware Types

Viruses, Worms, Trojans, Ransomware, Rootkits, Spyware

Focus Areas

- Infection vectors
- Payload behavior
- Detection & impact

Tools Used

VirusTotal, Any.Run, Wireshark, Process Monitor

Deliverables

Analysis report + presentation

Week 2 – SIEM Configuration & Monitoring

SIEM Tool

IBM Qradar

Log Sources

- Windows Machine logs

Configurations

- Custom dashboards
- Real-time alerts

Alert Types

- Unusual process behavior
- Suspicious IP connections
- Failed logins

Deliverables

Config document and monitoring report



Week 3 – Prevention Strategy & Awareness Training

Defense Strategy

Multi-layered with endpoint protection

Best Practices

- Least privilege
- Network segmentation

Training Topics

- Phishing detection
- Safe browsing
- USB device policy

Deliverables

Strategy document and training materials

Week 4 – Final Report & Presentation

Compiled Deliverables

All previous work integrated

Organized Sections

- Malware analysis
- SIEM configuration
- Prevention strategy

Prepared Presentation

Summary slides and notes



Project Outcomes



Malware Analysis

Successfully analyzed malicious script

SIEM Deployment

Configured alerts and monitoring



Training

Designed and shared awareness content

Final Report

Delivered actionable recommendations



Q&A

Thank you! We welcome any questions you have about our approach or findings.



Thank You for Your Attention

We appreciate your time and interest in our cybersecurity project.

