Open-Source Tools for Defending Against Cyber-Attacks

Hong Kong Institute of Information Technology
香 港 資 訊 科 技 學 院
Member of VTC Group VTC 機構成員

Overview

- Common Attack Factors, especially in the Education Field
- Introduction to Cybersecurity-Related Open-Source Tools

Common Cyber Threats Related to Schools

Threat	Impact
The AI Trap: Deepfake Fake voice/video call from well-known people, **ask for money** transfer or provide information	Financial Loss, Reputation Impact
Using Risky Free Apps and Websites Free online **unknown resource** like AI tools, online file convertors (e.g. PDF to word)	**Data leakage -** Upload sensitive data to unknown parties

Common Cyber threat related to School

Threat	Impact
Phishing email/QR code Hacker send email that looks legitimate and it urges you to click a link, download an attachment, or verify your account	Malware Infection, Credential Loss (e.g., password), Financial Loss
Ransomware Malware come from phishing email, risky app/website, unknown USB storage	Operational Outage, Financial Loss if pay for the ransom (Don't do that)

Deepfakes aren't far away

Hong Kong Computer Emergency Response Team Coordination Centre
HKCERT 香港網絡安全事故協調中心

ENG 事故報告/求助

網絡安全的新威脅

儘管深度偽造技術在娛樂和醫療領域中有著積極的應用，例如數位化重現已故演員的影像，或重現因疾病或意外失去聲音的人的聲音。然而深度偽造最廣為人知的用途卻是製作虛假的名人視頻或音頻，以傳播虛假或誤導性訊息。除此之外，人們也可能濫用這項技術來製作色情影像或進行詐騙。因此，深度偽造技術的危險性不容忽視，這種危險性在一些真實案例中得到了充分證實。

最近真實案例

1. 2023年8月，一個犯罪集團因爲使用深度偽造技術偽造身分以申請貸款而被抓捕。

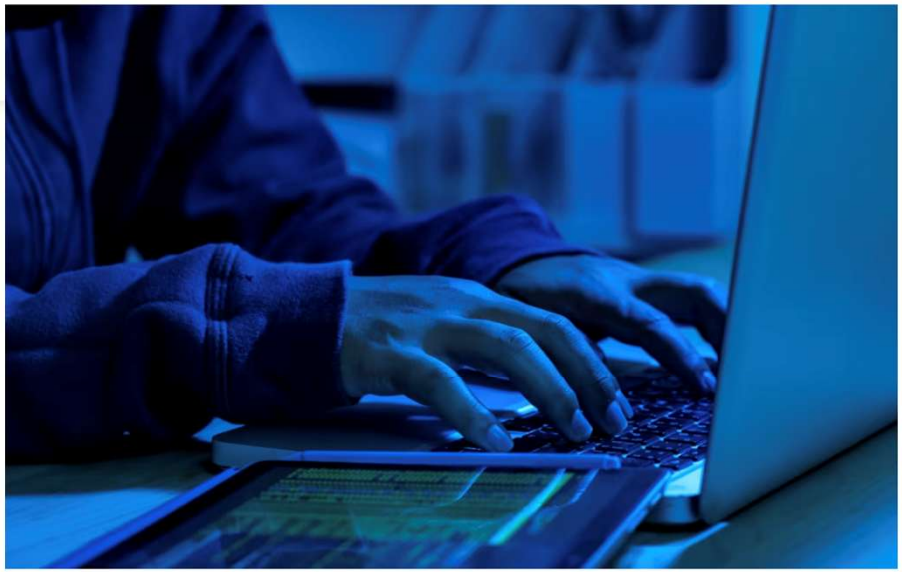
來源：明報

CNN World Africa Americas Asia Australia China Europe India Middle East United Kingdom

World / Asia

Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

By Heather Chen and Kathleen Magramo, CNN
2 min read · Published 2:31 AM EST, Sun February 4, 2024



Authorities are increasingly concerned at the damaging potential posed by artificial intelligence technology. boonchai wedmakawand/Moment RF/Getty Images

(CNN) — A finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company's chief financial officer in a video conference call, according to Hong Kong police.

HKiiT

Source: https://www.hkcert.org/tc/blog/deepfake-where-images-don-t-always-speak-truth

Fake ChatGPT Apps and Phishing Websites

- Attackers exploit interest by offering fake apps or “free” premium access to spread malware or steal data.
- Hackers create fake websites, social media pages, and mobile apps mimicking official ChatGPT.
- Over 50 counterfeit/malicious apps using the ChatGPT logo identified (Cyble report).

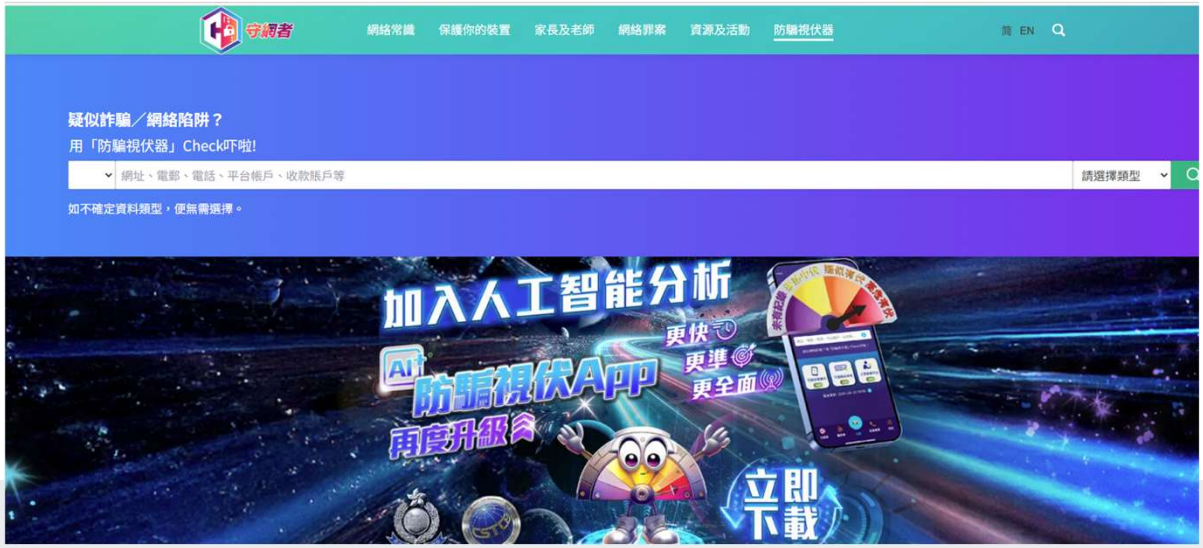
Source: https://www.hkcert.org/blog/hkcert-security-tips-beware-of-fake-chatgpt-apps-and-phishing-websites

HKiiT

Preventing Deepfakes and Fake Apps

- Deepfakes
  - Verify identity using secret questions or a “face-hand” test (ask the person to perform a specific action on camera).
  - Stop sharing information if authenticity is uncertain.

- Malicious Apps/Websites
  - Use apps and web resources only from trusted, official sources.
  - Verify using CyberDefender’s Scameter (防騙視伏器): https://cyberdefender.hk/scameter/



HKiiT

Example : **Locky**

Locky was heavily distributed by large criminal enterprises that used phishing messages. The one below claims that the victim made a payment on an account. The victim can view the payment confirmation in the attached zip file. Unfortunately for victims, the zip contained fake transaction information and a Locky ransomware loader.

From: John Long
Date: Monday, March 7, 2016 at 2:37 PM
To: Victim
Subject: Payment ACCEPTED A-122974
Attachment: payment_document_122974.zip

Dear sir,

Please check the payment confirmation attached to this email. The transaction should appear on your band in 2 days.

Thank you.

John Long, CMA
Corporate Comptroller

- Ransonware by n Day Attack
- **What is a n-Day Attack?**
  - A cyberattack exploiting discovered vulnerabilities

```
Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

Example
WannaCry (2017):

- Exploited a vulnerability in Windows systems (EternalBlue).
- Spread globally within hours, affecting over 200,000 computers.

What to Do When Infected by Ransomware

- Isolate and disconnect the infected machine; do NOT pay the ransom.
- Seek assistance:
  - HK Police / CyberDefender
  - HKCERT (Hong Kong Computer Emergency Response Team)
- Investigate potential data theft:
  - Review firewall logs for file uploads and anomalous outbound traffic.
  - Use SIEM to correlate events and identify exfiltration indicators.

Prevention Is Better Than Cure

Prevention with monitoring is far more effective than trying to fix a hack after it happens. Here are three layers of defense you can apply:

1. The Human Firewall — User Training
2. The Digital Bodyguard — Endpoint Security
3. Monitoring — Review Your Security Status

1. The Human firewall – User training

A. Adopt a “**Verify First**” mindset: validate unexpected requests, regardless of who they appear to come from.

B. Don’t click: avoid QR codes and links unless you can verify the source.

C. Protect sensitive data: keep student and school information **off public** platforms.

2. The Digital Bodyguard – Endpoint Security

A. The **“Invisible Shield”**: Install a security agent to help prevent ransomware.
B. Never disable it, even if it slows down a specific task. Real-time monitoring is critical.

3. Monitoring — Review Your Security Status

A. SIEM serves as a **central** system, acting like CCTV for your network.

B. It provides 24/7 monitoring and alerts the team when **abnormal activity** occurs.

C. SIEM can **detect** it and **alert** the team to stop the attack before it spreads.

IT Security Guidelines [G3]

- Providing detailed implementation standards and guidance for protecting government information assets, covering risk management, incident handling, and secure system design
- Logging and monitoring is required

14.4 Logging

(a) Log Collection and Retention

An audit trail shows how the system is being used from day to day. Depending upon the configuration of the audit log system, audit log files may show a range of access attempts from which abnormal system usage can be derived.

More complicated applications should have their own auditing or tracing functions in order to give more information on individual use or misuse of the application. This mechanism is virtually essential for highly secure applications, as the tracing functionality of the operating system may not have a fine enough granularity to record critical functions of the application.

There is virtually no limit to the recording of access to records by individual users and the actual updates made. However, logging routine use can result in a waste of resources and may even obscure irregularities because of the volume generated. Therefore, self-developed audit trails should focus on failed transactions and attempts by users to access objects for which they do not have authorisation.

(iv) Log analysis

- Roles and responsibilities.
- Type of events to trigger alerts to responsible parties.
- Type of events to be analysed.
- Log review frequency.
- Handling procedures for suspicious and abnormal activities.

Pillars of Cybersecurity: What We're Trying to Accomplish

Confidentiality - Protection of information from disclosure to unauthorized individuals, systems, or entities. Confidentiality is **data** oriented.

Integrity - Protection of information, systems, and services from unauthorized modification or destruction. Integrity is **data** oriented.

Availability - Timely, reliable access to data and information services by authorized users. Availability is **service** oriented.

Non-repudiation - The ability to correlate, with high certainty, a recorded action with its originating individual or entity. Non-repudiation is **entity** oriented.

Authentication - The ability to verify the identity of an individual or entity. Authentication is **entity** oriented.

HKiiT

Cyber Defense Principles: How we're trying to accomplish it

Least Privilege

- Know who has access to systems and data, and minimize the level of access to only what is required

Defense in Depth

- Know what your critical assets are, and protect them with multiple overlapping security controls

Management and Monitoring

- Know how your assets should be performing, and how they are performing currently

Prevention Steps:

1. **Risk Identification**
   - Know your assets & identify what's critical
   - Know your network & data
   - Know your applications & application versions
   - Know the common vulnerabilities
2. **Vulnerability Reduction**
   - Secure network endpoints
   - Install asset protection/intrusion detection tools
   - Apply principle of least privilege and defense in depth
   - Apply mitigations to known vulnerabilities
3. **Threat Reduction**
4. **Consequence Mitigation**
5. **Enable Cybersecurity Outcomes**

Where to Start (Cyber Hygiene)

Definition of Open-Source Tools

Open-source tools are software applications whose **source code is publicly available**, allowing anyone to use, study, modify, and distribute them under an open-source license.

Limitations of Open-Source Tools

- May require a certain level of technical expertise to install and maintain
- Some organizations may prefer a cloud-based solution
- Like any security monitoring solution, open-source tools may generate false positives, requiring human expertise to investigate and address.

Network Discovery Tools

Network discovery tools enable you to automatically identify all devices connected to your network.

Finding Hidden Devices in BYOD (Bring Your Own Device) Environments:

- **Shadow IT**: Hidden devices enable the use of unapproved applications or services, creating vulnerabilities.
- **Data Leakage**: Personal devices may store sensitive company data, risking exposure if the device is lost or stolen.

NMAP

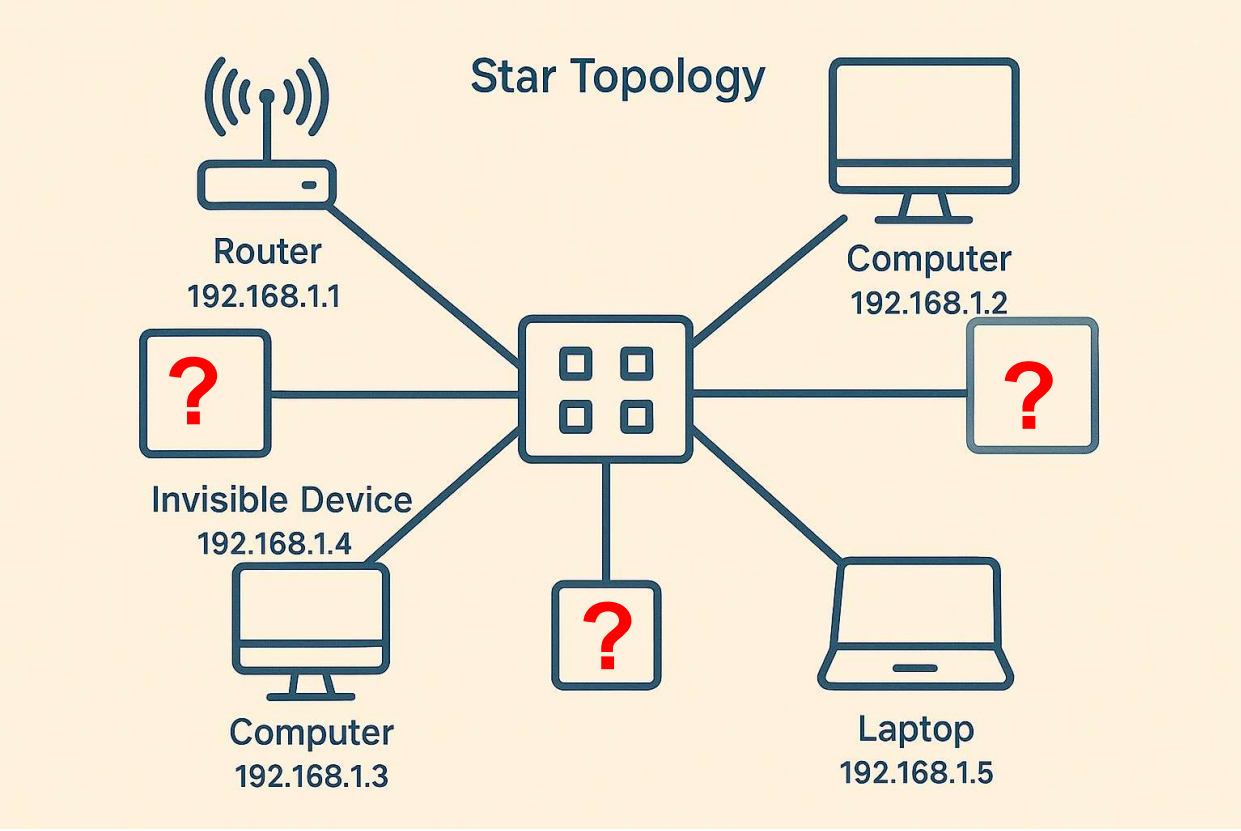
Network Discovery with Nmap Network Discovery with Nmap

Nmap can tell us:

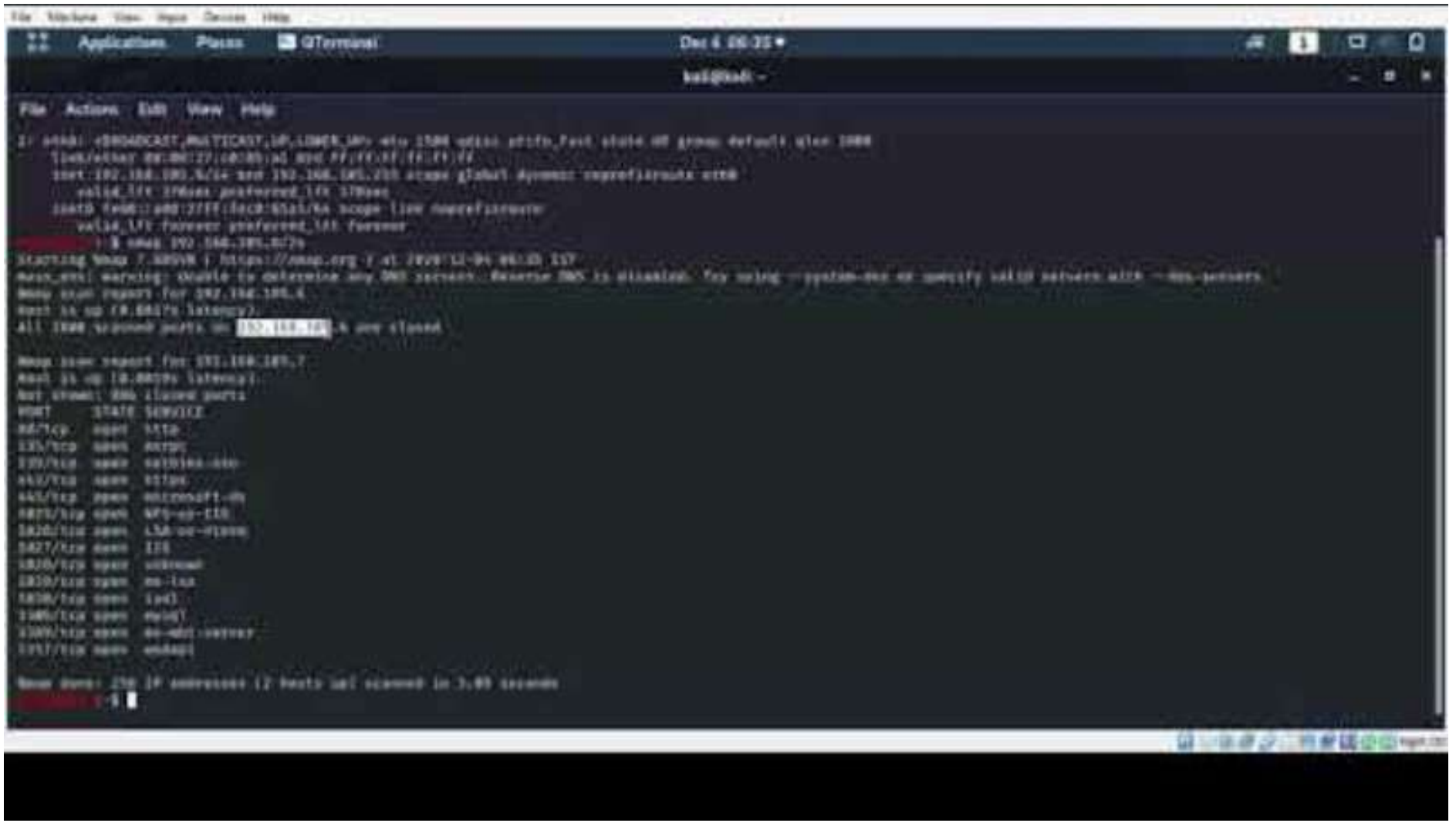
- Hosts on a network
- Services running on hosts
- Operating system versions
- Firewalls
- Network Segmentation
- Fingerprinting

Discovering :

- Possible Vulnerability
- Shaon IT



Nmap Demo


Applications
Places
QTerminal
File
Actions
Edit
View
Help

An intrusion detection system is a device or software application that monitors a network or systems for malicious activity or policy violations.

Malware Discovery

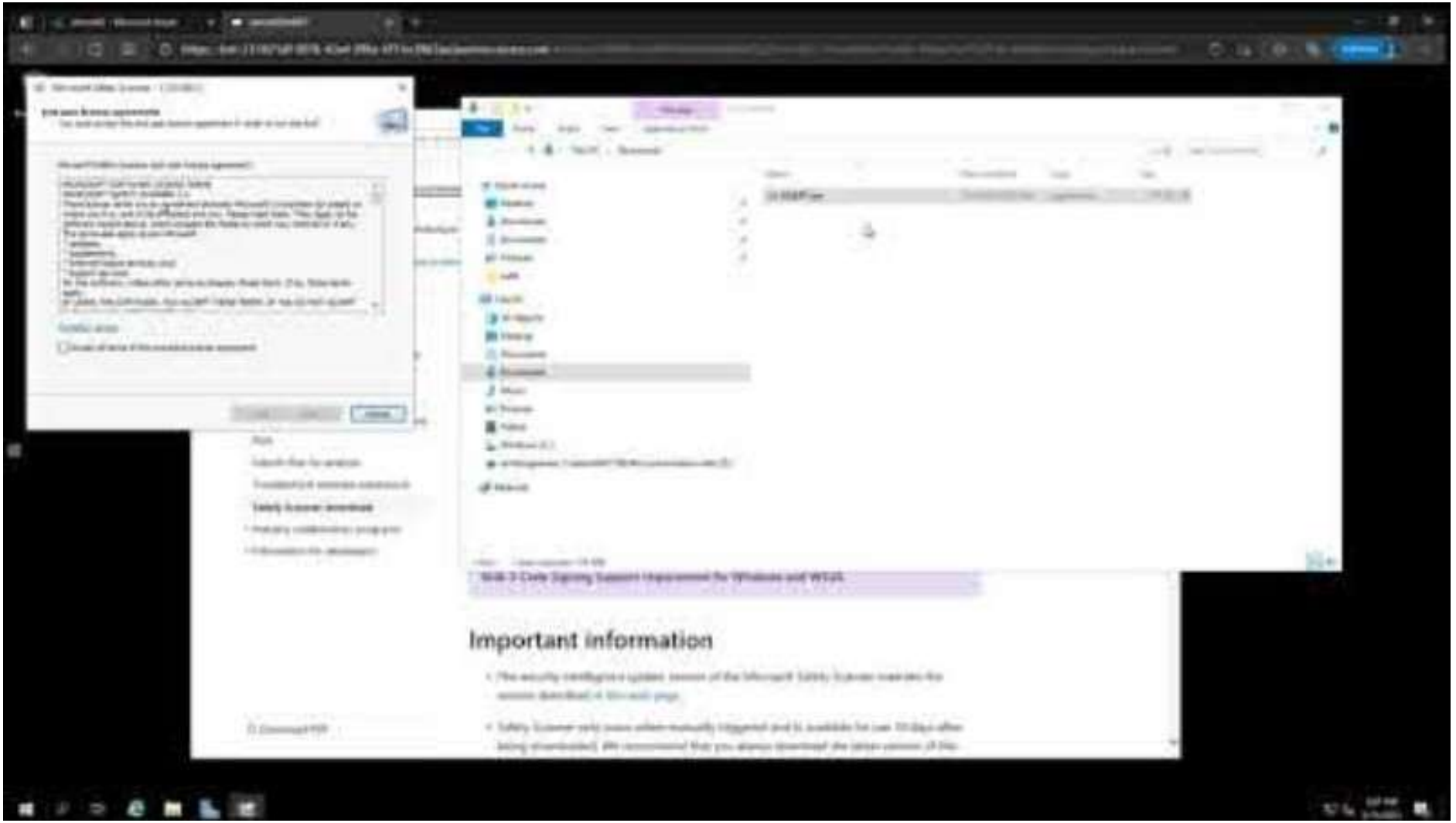
Microsoft Safety Scanner (Free but not Open-Sourced)

- Microsoft Safety Scanner is a scanning tool designed to detect and remove malware from Windows computers.
- After detecting malware during a scan, the tool attempts to reverse the changes made by identified threats.

Microsoft Safety Scanner

- Safety Scanner only scans when manually triggered and is available for use 10 days after being downloaded.
- Microsoft recommends that you always download the latest version of the Safety Scanner tool before each scan.
- Microsoft indicates that this tool does not replace any existing anti-malware product.

Demo



- A software function that consolidates log data from throughout the IT infrastructure into a single centralized platform where it can be reviewed and analyzed.

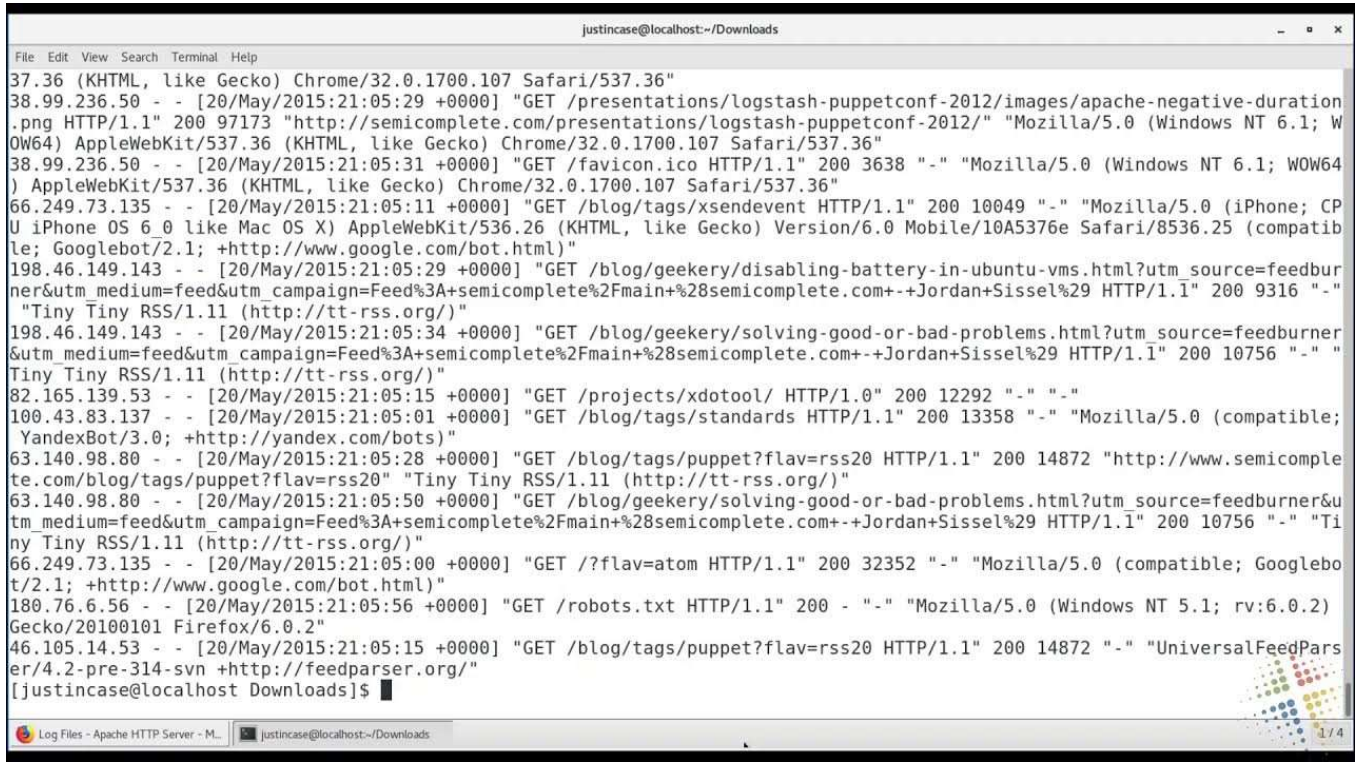
Log Aggregation and Analysis

What is Event Log?

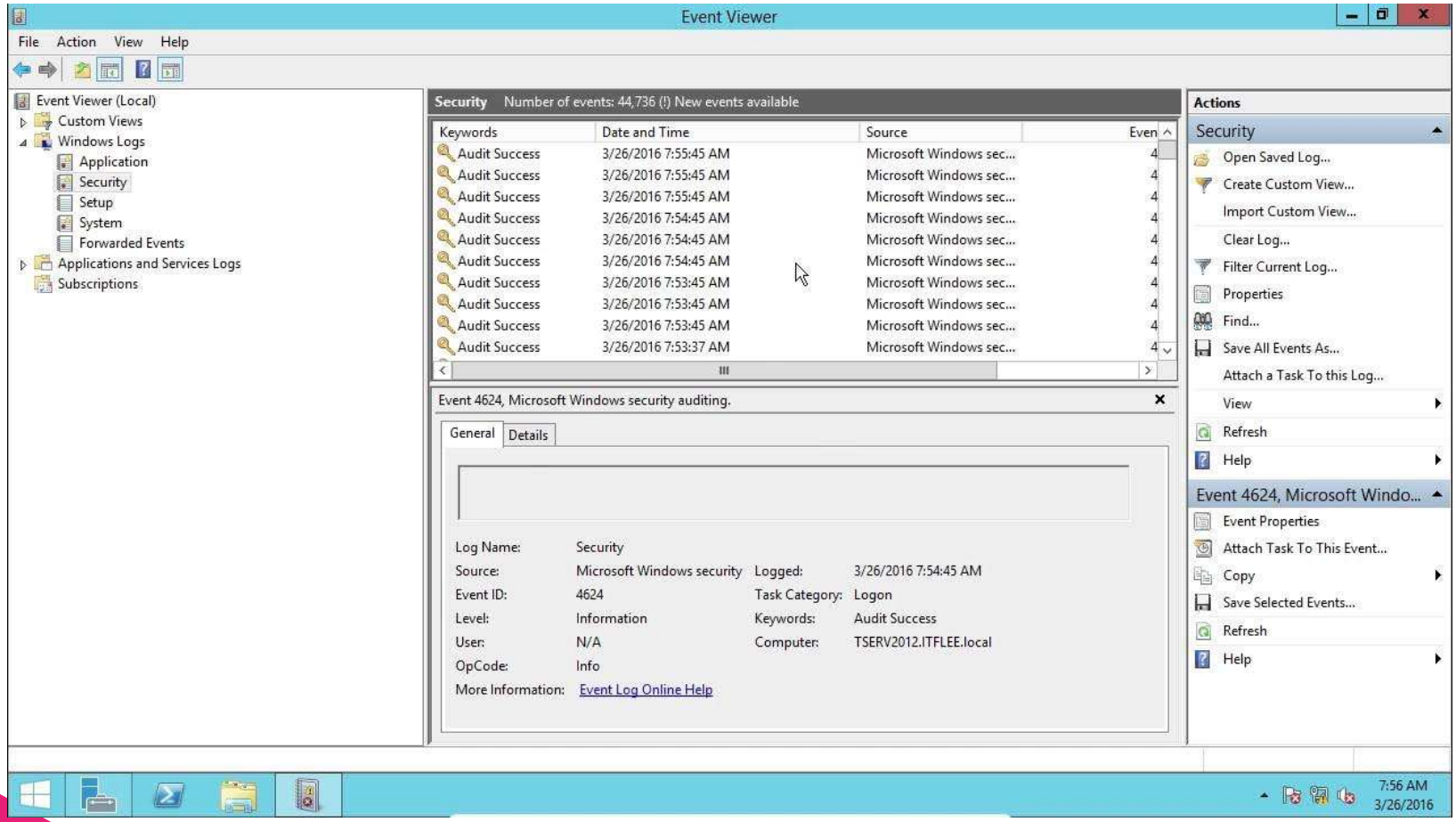
An event log is a structured file containing records of event data.

- System: OS and hardware events (startup, driver errors)
- Application: App-specific errors and warnings
- Security: Authentications, access attempts, policy changes
- Network/Firewall: Connections, blocks, intrusion alerts

Example 1: Web Logs



Example 2: Windows Log



HKiiT

Elastic Security

- Open-source solution with both endpoint security and SIEM features
- Strong performance in antivirus detection tests
- All-in-one platform: deploy endpoint security and SIEM together

Features included in Elastic’s open-source version

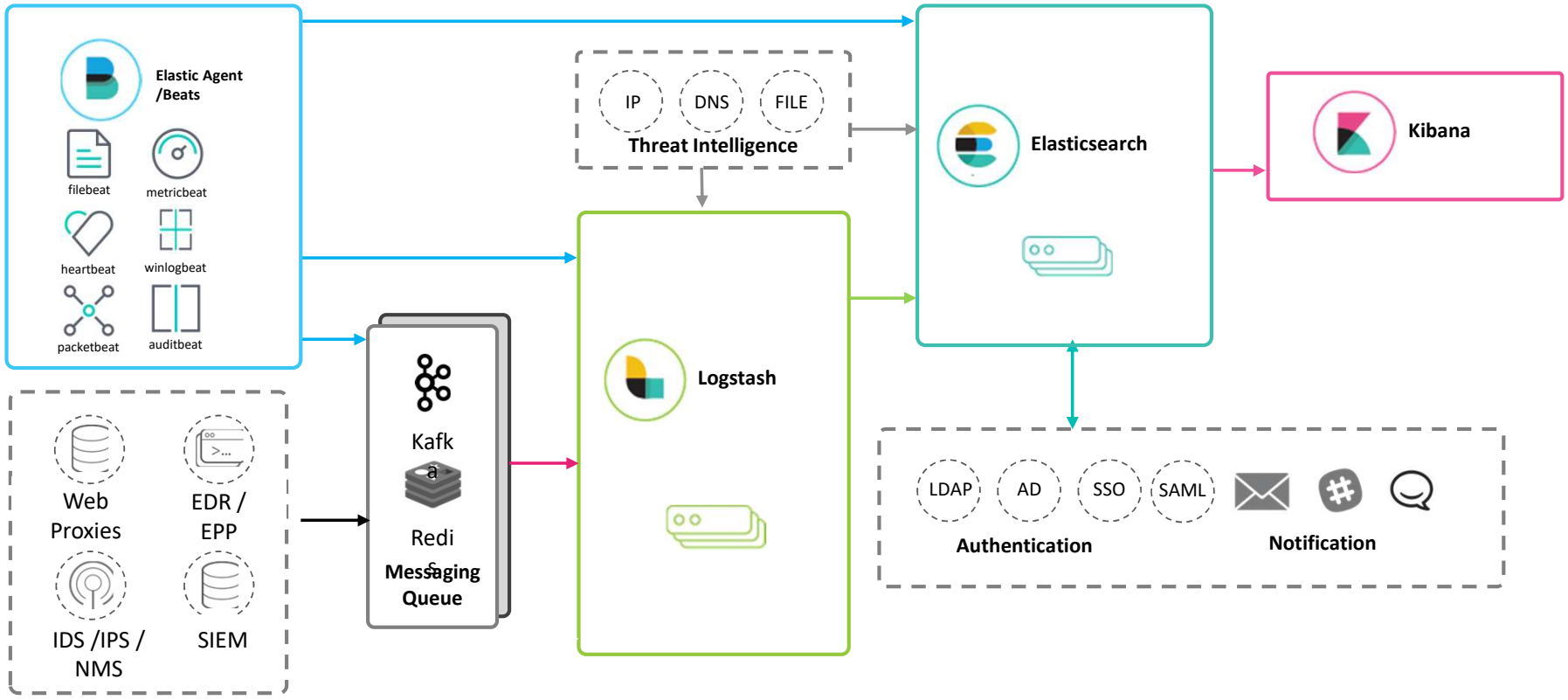
Endpoint Security

1. Malware prevention
2. Admin-defined endpoint blocklists

SIEM

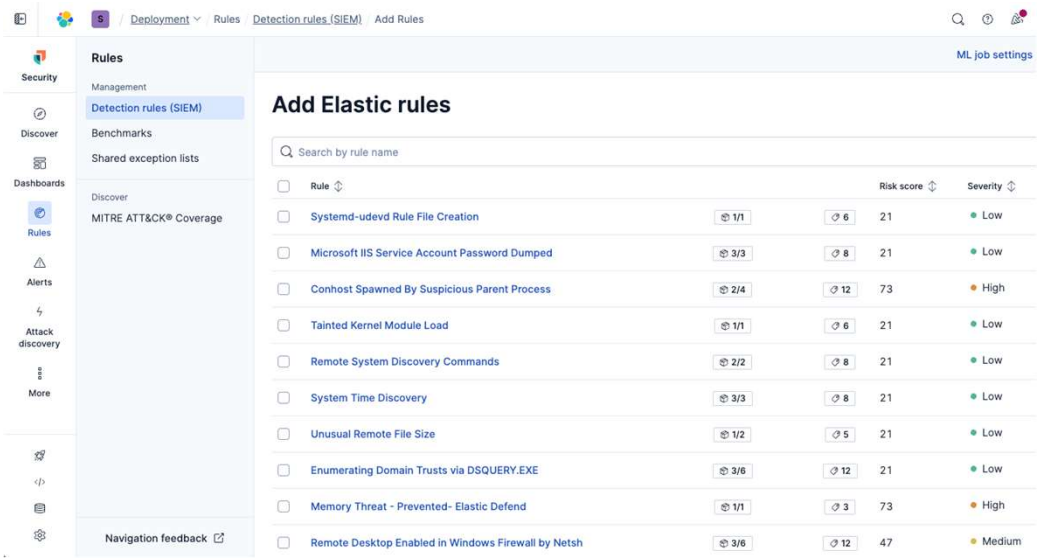
1. Over 1,000 prebuilt detection rules
2. Host, network, and user security analytics
3. Case management
4. Threat intelligence integration

High Level SIEM architecture

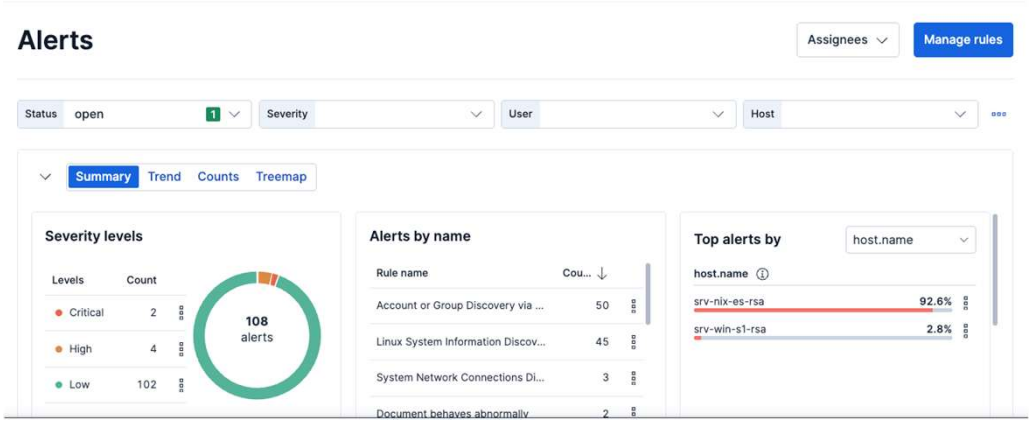


HKiiT

- Built-in detection rules for endpoint security and SIEM

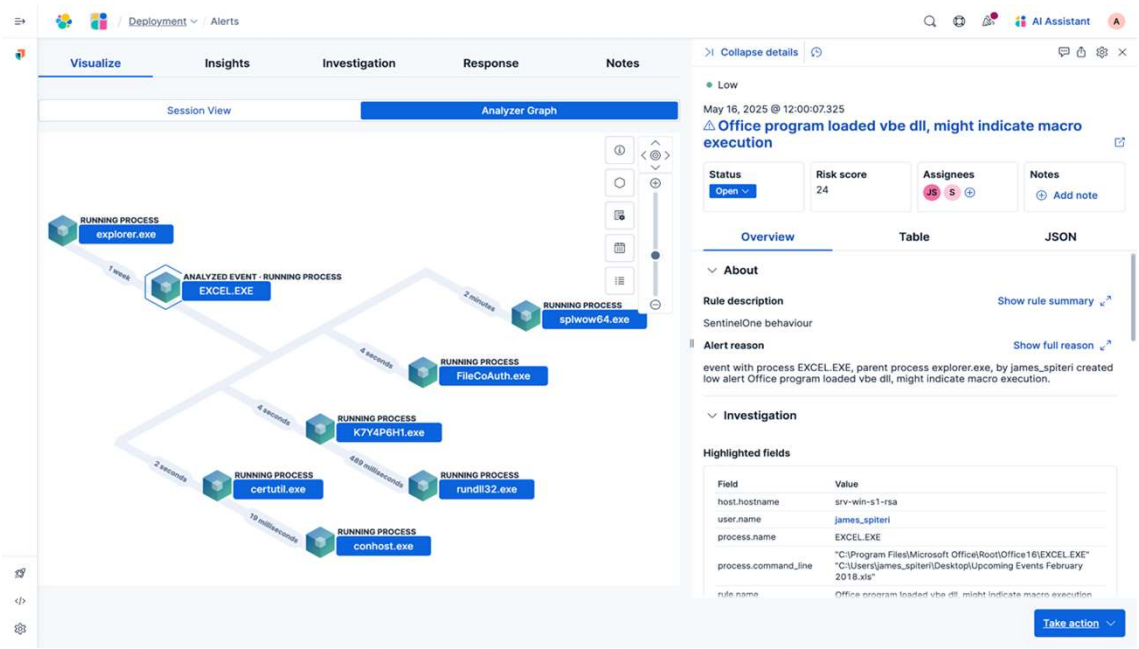


- Predefined dashboards for monitoring



HKiiT

- Combine endpoint security and SIEM in a unified platform
  - Endpoint alerts are visible within SIEM
  - SIEM displays detailed event information
  - The full process execution path is captured



- ELK Demo On Detecting Attack

- Elastic offers an enterprise version with advanced features and **24/7 support**.

	Free and open - Basic [1,2]	Platinum	Enterprise
ELASTIC SECURITY			
Ransomware prevention	—	✓	✓
Malicious behavior protection	—	✓	✓
Memory threat protection	—	✓	✓
Self healing	—	✓	✓
Host Isolation	—	✓	✓
Interactive response console	—	—	✓
Tamper protection	—	✓	✓
Elastic AI Assistant	—	—	✓
Threat intelligence management	—	—	✓
Customizable on-endpoint protection notifications	—	✓	✓
Cloud and Kubernetes Security Posture Management (K/CSPM)	—	—	✓
Workload session auditing	—	—	✓
Device Control	—	—	✓

Reference:
https://www.elastic.co/subscriptions

HKIIT 課程 : SkillsUP在職培訓服務

- HKIIT提供各種實戰技術與專業認証在職培訓課程、並歡迎企業客戶根據需要自訂課程。

獲授權開辦註冊信息安全專業人員（CISP）課程

- ❑ 培訓機構及考試中心
- ❑ 已完成17班，完成課程人數累計超過400人。

HKiiT

其他網絡安全在職培訓課程

- 資訊安全專業證書課程
  - 註冊信息系統審計師（CISA）考試預備單元
  - 註冊信息安全經理（CISM）考試預備單元
  - 註冊信息系統安全師（CISSP）考試預備單元

- 網頁程式滲透測試證書
  - 滲透測試基礎
  - Web應用程序滲透測試

師資 - 證書

- ISC^2 (CISSP , CCSP)
- ISACA (CISM, CISA)
- OffSec (OSCE3, OSEP, OSWE, OSED, OSCP)
- IAPP (FIP, CIPP/E, CIPP/A, CIPT)
- 中國信息安全測評中心(CISI , CISP)
- EC Council (CEH)
- CREST (CRT / CPSA)
- 華為, 阿里雲, CISCO , AWS, CheckPoint, Palo Alto 授權培訓師

我們的企業客戶

政府部門

- 數字政策辦公室（香港特別行政區政府）
- 香港警務處（香港特別行政區政府）
- 民政事務總署（香港特別行政區政府）
- 地政總署（香港特別行政區政府）

重要基建及公用服務

- 香港機場管理局
- 香港金融管理局
- 醫院管理局
- 香港房屋協會
- 港鐵（MTR）
- 港燈（HK Electric）
- 中華電力（CLP 中電）
- 香港中華煤氣（Towngas）

服務提供者

- 愛浦京軟件（香港）有限公司（APJ）
- 自動系統（香港）有限公司 (ASL)
- Check Point 軟體技術有限公司
- 富士膠片商業創新香港（FUJIFILM）
- Global Technology Integrator (GTI)
- Hewlett Packard Enterprise (HPE)
- 香港電訊（HKT)
- 倢冠控股有限公司（Kinetix）
- 聯想電訊盈科企業方案（LPS）
- 理光（RICOH）

商業機構及商會

- 中國工商銀行（亞洲）
- 帝盛酒店集團
- 領展
- 香港總商會（HKGCC）

*排名不分先後

HKiiT

- More :
- https://hkiit.edu.hk/skills-up