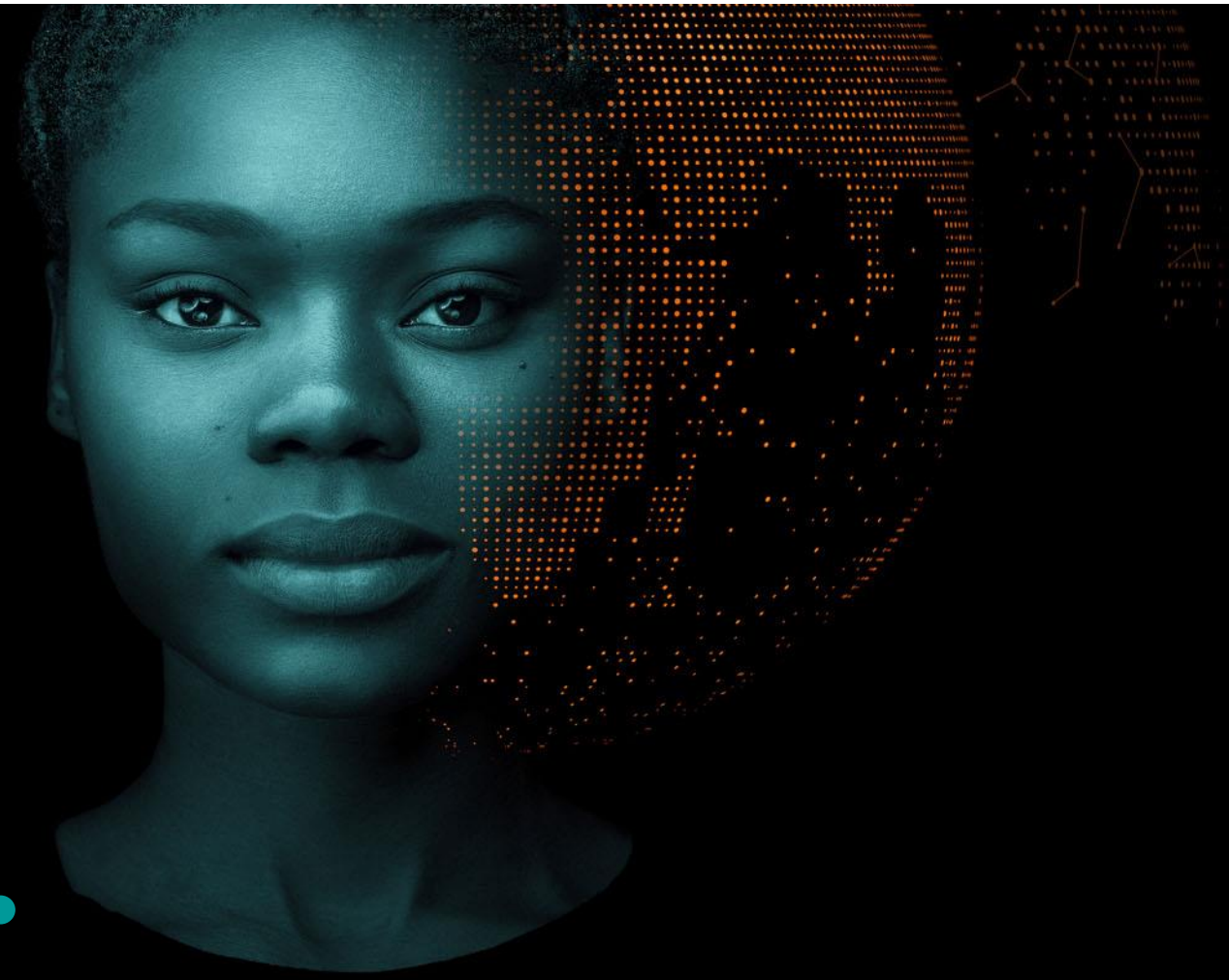
SIEMENS Healthineers

Structuring (cyber) incident root-cause investigations

A practical walk-through

João Collier de Mendonça
Munich, November 2025



This session covers

Background
Healthcare threat landscape, incident response and a team journey

Approach
Understand environment constraints and stakeholders' needs

Structuring the investigation
Using DFIQ to structure an investigation

Takeaways
Learnings for similar journeys

SIEMENS Healthineers

Understand the healthcare setting

Background

Threat landscape
Healthcare as a profitable target, real risk for patients

RANSOMWARE

Company Paid Record-Breaking $75 Million to Ransomware Group: Report

Zscaler is aware of a company that paid a record-breaking $75 million ransom to the Dark Angels ransomware group.

Cyber attacks are one of the biggest threats facing healthcare systems

The vast amount of information held by health services makes them a prime target for cyber criminals

npr

Ransomware attacks against hospitals put patients' lives at risk, researchers say

NEPRASH: The good news here is that dying in a hospital is still a really unlikely event. The bad news is it's more likely to happen if you have the bad luck to be admitted to a hospital during a ransomware attack.

ANDY GREENBERG SECURITY JUN 12, 2024 6:30 AM

Medical-Targeted Ransomware Is Breaking Records After Change Healthcare's $22M Payout

Cybersecurity firm Recorded Future counted 44 health-care-related incidents in the month after Change Healthcare's payment came to light—the most it's ever seen in a single month.

Company Paid Record-Breaking $75 Million to Ransomware Group: Report | Securityweek
Cyber attacks are one of the biggest threats facing healthcare systems | FT
Ransomware attacks against hospitals put patients' lives at risk, researchers say | NPR
Medical-Targeted Ransomware Is Breaking Records After Change Healthcare's $22M Payout | Wired

Why do threat actors target Healthcare?

Healthcare sector is an easy target
- Large and interconnected attack surface
- Poor cybersecurity practices
- Understaffed teams and severe pressure

Healthcare is intrinsically complex
- Legacy systems, security as an add-on
- Unpatched medical devices
- Digitalization push to increase process efficiency

Criminals make money from healthcare data
- Direct financial gains from ransomware
- Selling patient data on criminal markets
- Exploiting patient data in fraud schemes

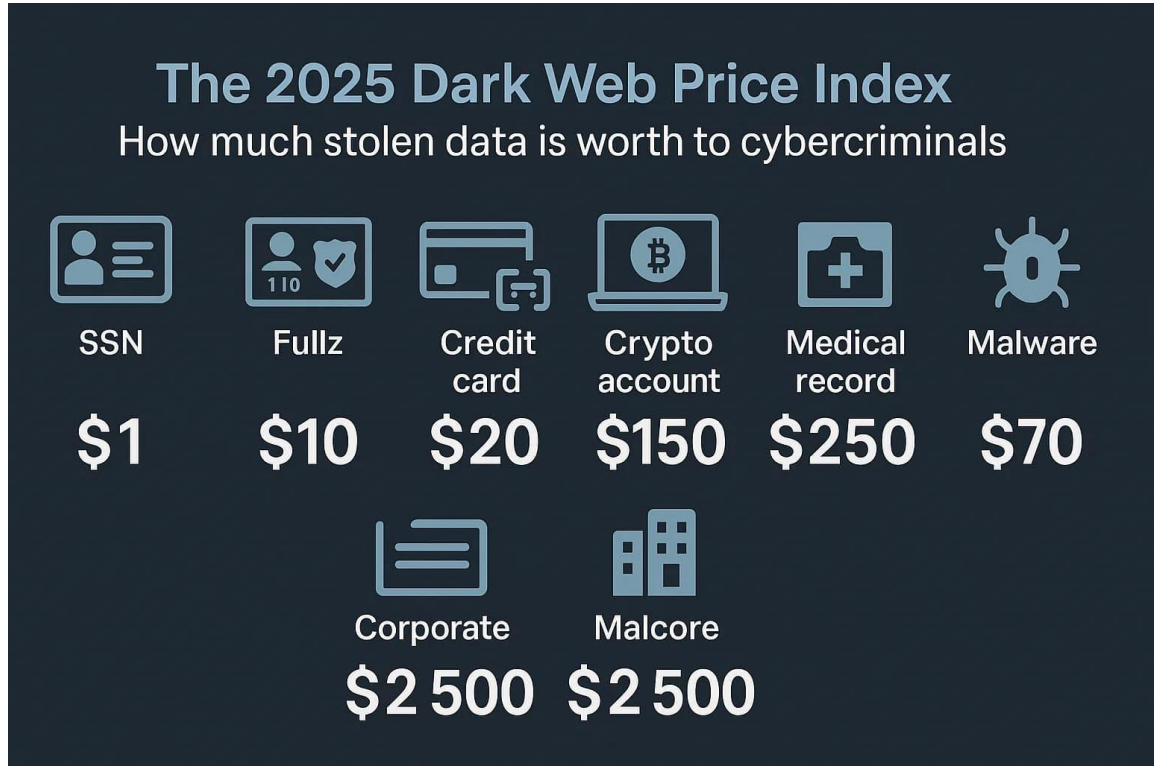


Image source: deepstrike.io/blog/dark-web-data-pricing-2025

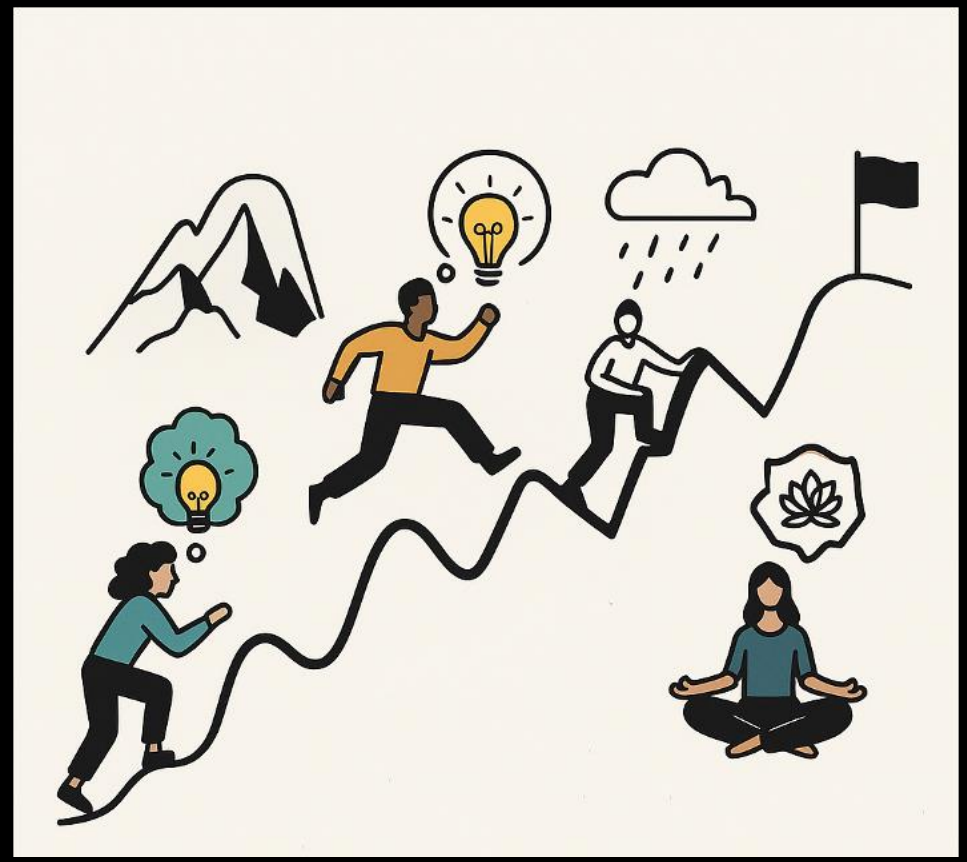
PSIRT and forensics

SIEMENS Healthineers

Siemens Healthineers PSIRT
- Incident response for **products and solutions**
- Assets owned and operated by customers
- Root-cause determination

Why do we investigate root-cause?
- Enable sustainable recovery
- Fulfill regulatory needs (safety and quality)
- Enable continuous improvement

Next version of the service: fantastic opportunity to review
- Process
- Tooling
- Investigation technical aspects



AI-generated image (created with OpenAI GPT-5 / DALL·E)

Start and adjust along the way

Approach

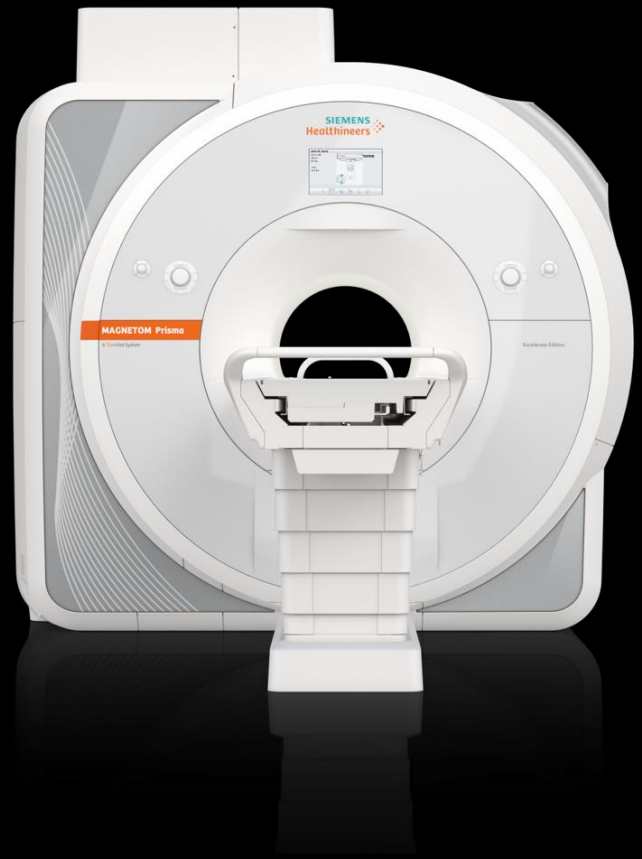
Key elements to define process, tools and investigation

Environment
- Fundamental constraints to be observed

Stakeholders
- Specific needs to be met

Specialist knowledge (threat intelligence)
- Identify risks and mitigate them
- Ensure the approach is complete

From those elements, derive:
- Requirements (process, tools and investigation)
- Adequate documentation
- New investigation process



Take one

Understand your environment

Healthcare specific challenges for forensics

SIEMENS Healthineers

 Priority is on restoring operations	**Do not get on the way of restoring operations!**
 Long lifecycles (legacy components)	**Know your installed base & ensure compatibility**
 You only have one shot!	**Take as much as data you need but as little as possible**

Determining and **addressing root-cause of incidents**
is essential to **avoid reoccurrence** and unnecessary downtime.

...

IT and healthcare incident response
Fundamental differences

IT security: telemetry and automation are commonplace
- Security operation centers, detection and monitoring
- EDR agents, orchestration, automation
- **Abundance of tools for detection and containment**

Healthcare cybersecurity: commonplace medical devices
- Often no integration into cybersecurity operations
- Priorities clinical features vs. cybersecurity features
- **Scarcity of tools for detection and containment**

Size matters
- For small medical devices: turn-off and replace device
- For larger medical devices
  - Recovery performed on-site
  - Forensics data acquired on-site
  - A 13-ton device cannot be easily shipped

Lack of telemetry and automation

Logistics and on-site support needed

Sources
https://www.siemens-healthineers.com/magnetic-resonance-imaging/3t-mri-scanner/magnetom-prisma

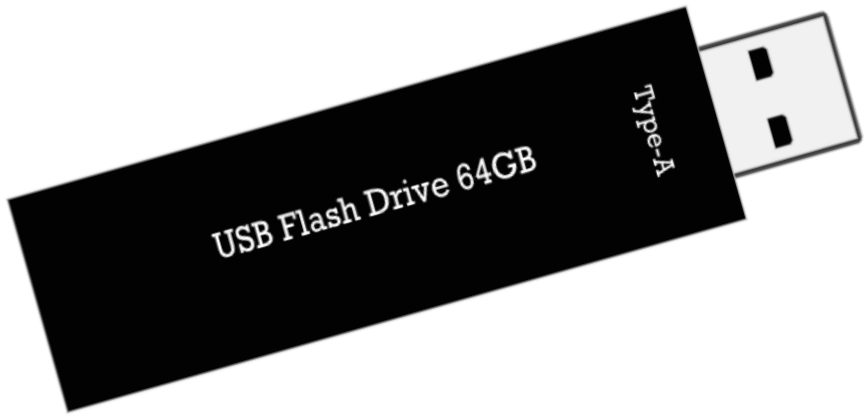
Translating your environment's constraints into requirements

SIEMENS Healthineers

Focus on restoring operations	Long lifecycles	Only one shot
Patient first: field technicians' job is to **get system back up and running**	Siemens Healthineers is largely a "Windows shop"	Systems will be **swiftly reimaged** and reconfigured to restore operations
Customers want fastest possible recovery, minimize patient waiting	Installed base has from Windows 7 to latest Windows versions	**No chance to recollect artifacts** after the initial triage
Forensic acquisition tools must be safe, intuitive, and accessible	Ensure **compatibility** of tools and have alternatives (scripts)	**Short acquisition times,** prioritize artifacts (adaptive collection FTW!)
Documentation must be usable and adequate to field work needs	Enable teams to collect **full disk images** if necessary	Offer **different acquisition profiles**, some cases allow broader collection
Focus of field teams is recovery and not forensics acquisition	**Offer alternative acquisition tools (tools might fail on older systems)**	**Take as much as you reasonably need but as little as possible**

…

Data acquisition for incident response



Collector (forensics acquisition tool)

- Opensource collectors (Velociraptor, Fox-IT acquire/dissect framework)
- In-house developed scripts
- Commercial tools

+ Hardware specs

Take two

Understand your stakeholders' needs

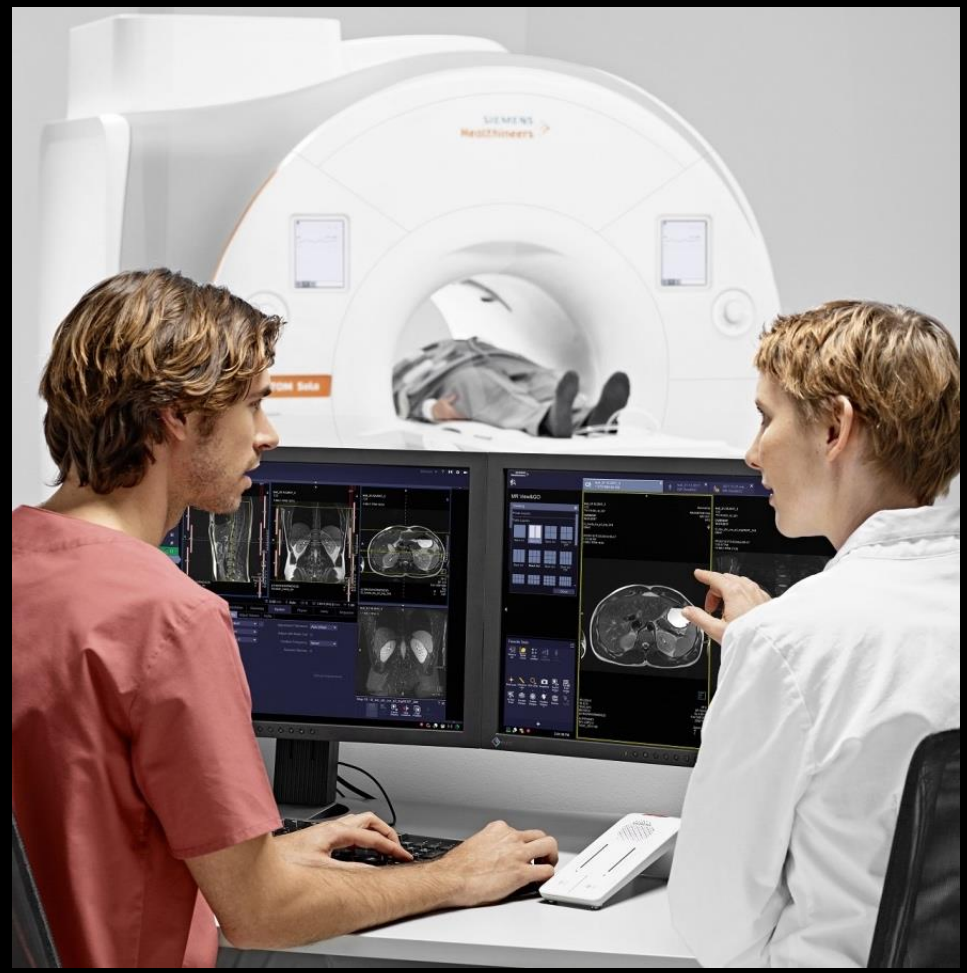
Stakeholders around cyber incidents on medical devices

SIEMENS Healthineers

Customers
- Healthcare delivery organizations (hospitals)
- Business continuity and patient care
- **Must install** upgrades to address security flaws

Regulators
- Define conditions for market access of medical devices
- Focused on patient safety and clinical aspects

Manufacturer's R&D
- Security architecture of medical devices
- Device safety and quality
- **Must deliver** upgrades to address security flaws



Disclaimer: content simplified for the sake of explanation.

Example of investigation requirements

Cluster	Questions
Incident scope & identification of affected assets	• Affected device(s), versions, serial numbers and environments • Timelines event detected vs. occurred
Containment & Isolation	• Were immediate containment/mitigation measures performed? • Can the device operate in a standalone mode? (off network) • Were clinical workarounds provided?
Clinical data integrity	• Were clinical images (DICOM images) modified? • Were clinical databases or structured data sets modified?
Patient safety & essential performance	• Impact for clinical functionality or essential performance • Impact for safety, performance, or calibration of the device • Actual or potential patient harm

Different stakeholders will analyze incidents from a different perspective.
Digital forensics is an enabler for all of them.

Disclaimer: the content has been simplified from its original form for the sake of explanation. Focus here is to derive technical investigation questions.

SIEMENS Healthineers

DFIQ enters the room

A way to capture knowledge

DFIQ overview

SIEMENS Healthineers

DFIQ basics

- Framework of **forensic questions and approaches** – think **a catalog** 📘
- Stores information in YAML (text)
- Lives at https://dfiq.org

DFIQ benefits

- Deliberate thinking vs. Intuitive thinking
- Repeatability and explainability
- Quality and depth of investigations

Scenarios	**Starting point** for investigations High level logical grouping
Facets	**Intermediate level** grouping Too broad to answer directly
Questions	**The What** Atomic questions Specific enough to be readily answered
Approaches	**The How** Details on how to answer a question Specific to the question being answered

dfiq

Reference: hack.lu 2024, DFIQ: Codifying Digital Forensic Intelligence, Thomas Chopitea, youtube.com/watch?v=M3kZ7TTxW8Y

DFIQ basics

Fictive scenario: host infected by USB removable media

A host on the field was apparently infected with malware.
An external hard disk was being used to transfer files before the crash happened.
A hospital technician opened a complaint after the host crashed and got corrupted.

Structuring the investigation

SIEMENS Healthineers

Investigation progress

Initial facets and questions

Usage of USB devices on system

- Removable storage devices used on host?

Files transferred from USB device

- Files copied from USB media to host?

Malware present on USB device

- Autorun files present on storage device?
- Hidden folders present storage device?

Files executed from USB device?

- Autorun configuration on host?
- User executed file on USB device?

Deepening the investigation

Recent changes on the affected system

- Created or modified files?
- Created or modified user accounts?

Suspicious files running at system boot?

- Files in Registry "Run" keys?
- Items are in startup folders?

Staging data for future exfiltration

- Any files collected into a container?
- Access to sensitive files?
- Screenshots taken on the host?

Joao Collier de Mendonca | Cybersecurity

DFIQ example

SIEMENS Healthineers

Data Exfiltration

UUID: aba6b02b-2ee7-49ab-9cbe-20b7259d4661 **ID**: S1001

Description: An employee is suspected of unauthorized copying of sensitive data (code, trade secrets, etc) from internal systems to those outside of the company's control.

Are there signs of staging data for future exfiltration? F1008

"Staging" refers to the collection of data of interest onto a local system, as a precursor step for future exfiltration of that data. When reviewing data from Questions in this Facet, look for unusual volumes of results (number or size of files downloaded or sent, for example).

- Q1001 What files were downloaded using a web browser?
- Q1004 What screenshots were taken on a computer?
- Q1005 What files have ever been on a computer?
- Q1006 What files are present on a computer?
- Q1017 Were any files collected into a container?

https://dfiq.org/scenarios/S1001/

DFIQ example

SIEMENS Healthineers

What files were downloaded using a web browser?

UUID: 8620a183-d67f-481e-a63c-d8b8dfa5e968 **ID**: Q1001

Approaches to Answer

- Collect download records from local browser artifacts [Q1001.10]
  - Parse download records from web browsers' own databases.
  - Tags: Web Browser SQLite Chrome Safari Edge
- Detect browser downloads via file system event logs [Q1001.11]
  - File downloads by some web browsers create a specific pattern of events on the file system. We can use this to see browser downloads using file system logs (like Santa).
  - Tags: Web Browser macOS
- Detect browser downloads via change journal records [Q1001.12]
  - File downloads by some web browsers create a specific pattern of events on the file system. We can use this to see browser downloads using NTFS change journal (USN journal) records.
  - Tags: Web Browser Windows USN Journal NTFS

https://dfiq.org/questions/Q1001/

SIEMENS Healthineers

For your own journey

Takeaways

Takeaways

Know your environment

Where is your digital forensics process inserted?

How do you acquire data?

Telemetry and remote access available? (deployment of deeper analysis tools)

Target systems: age and resource state?

For the people working on your behalf
- are your process and tools usable for them?
- what priorities and resources do they have to perform collection on your behalf?

Know your stakeholders' needs

Who are your stakeholders?

What are their objectives in the investigation?

What key questions must be answered?

From those key questions:

- which ones must be **answered urgently**? (scoping and containment!)
- which ones can be answered **after containment and recovery**? (downstream products)

Integrate specialist know-how

Threat landscape: provide requirements for collection and analysis

What attack techniques are relevant for you?

What artifacts cannot be missed?

What anti-forensics techniques should be considered in your hypothesis?

› Use those three areas as **source of requirements** to define the optimal incident investigation process. **Review** them with **your stakeholders regularly**.

#thinkbeforeuclick

Thank you for your time!

Siemens Healthineers AG
João Collier de Mendonça

joao.collierdemendonca@
siemens-healthineers.com

linkedin.com/in/joaocmendonca

LinkedIn
Joao C.

Understanding how **threats materialize** and **acting on insights** is essential for **strengthening cyber resilience**.

Do the right thing. Together.