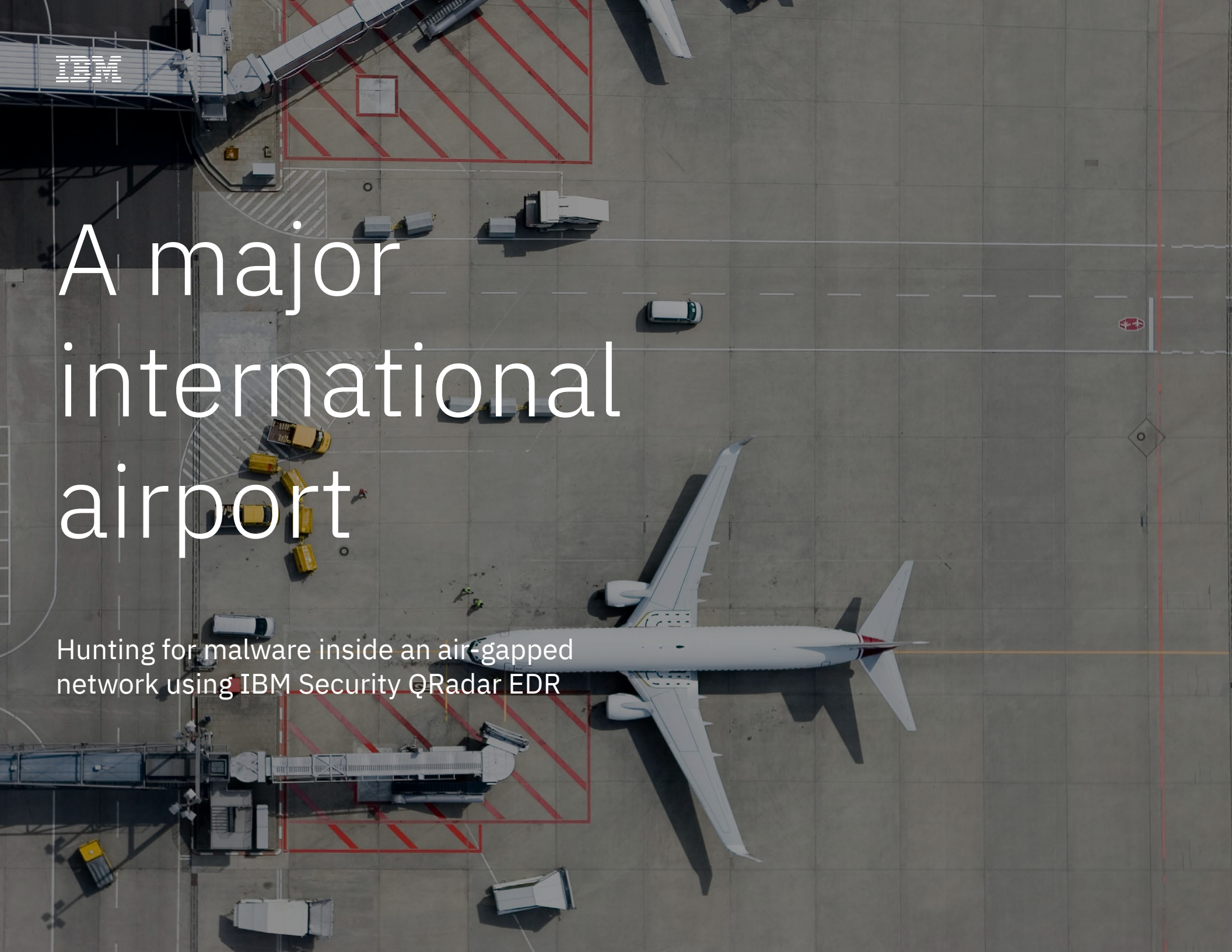
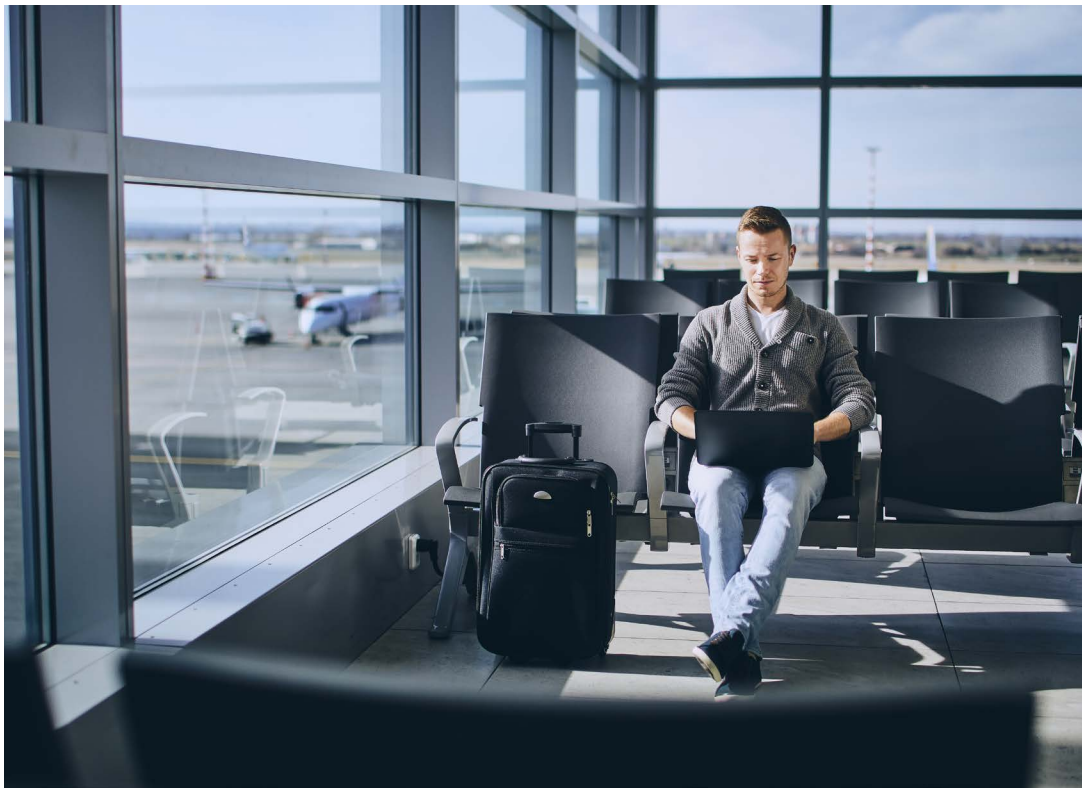


A major international airport

Hunting for malware inside an air-gapped network using IBM Security QRadar EDR

One of the world's largest airports runs an air-gapped network to manage internal operations ranging from security to logistics. Despite the airport's isolated nature, several devices are found to be infected with malware capable of capturing and storing information locally.



Security challenges:

- Critical infrastructure with no tolerance for downtime
- Lack of security measures within the network
- Air-gapped network connecting low-security and high-security devices together
- No visibility into any device within the air gap

This major international airport, one of the world's largest transportation hubs, connects 70 million passengers each year with more than 1,000 flights per day. The airport followed very good security protocols overall. It adopted a completely isolated network to operate

several essential services and prevent infections from the internet. However, the air-gapped network created a false sense of security. Although all devices within the air gap had no access to the internet, every network segment within was connected to each other with no traffic control.

Furthermore, the air-gapped network included devices that were physically accessible by the public, such as information kiosks, leaving essential services exposed to a potential attack. On top of that, the only means to bring information from the outside to the inside was by using USB drives, leaving the endpoints vulnerable to potential malware brought in, unwittingly, by airport employees.

Detection & remediation, without disruption

Solution overview:

- The airport implemented IBM® Security QRadar EDR software, which uses NanoOS technology for exceptional visibility across endpoints and infrastructure.
- QRadar EDR's behavioral engines perform with no degradation on isolated networks.
- Using powerful threat hunting capabilities, the airport can reconstruct and analyze incidents.

The airport used IBM Security QRadar EDR software to run a hygiene check in the air-gapped network because some endpoints appeared to have slowed down. Once QRadar EDR was deployed on an initial segment, the engines picked up potentially malicious activities coming from a small number of devices. The initial analysis pointed to a publicly accessible kiosk as the initial entry point, but a later analysis brought to light a second entry point, this time from a device in the check-in area. These two malicious vectors managed to spread to a limited number of devices touching different network segments.

The visibility provided by the QRadar EDR platform allowed the reconstruction of the incident from the beginning and the safe remediation of the infection, without interrupting the airport's business continuity.

Root cause analysis

The initial deployment flagged several behavioral anomalies. An application installed an in-memory keylogger by injecting it into a hidden instance of the default browser. After that, another thread managed to scrub the disk looking for Microsoft Word files, PDF files, cookies and browser databases. This information was

collected inside a hidden folder, and an attempt to send it to a command and control (C2) server was made at regular intervals, though it was unsuccessful due to the network being completely isolated from the world.

A more in-depth look at the infection vector brought back interesting results: the vector was unusually large and contained a series of mechanisms aimed at bypassing not just a local antivirus but also a sandbox analysis. The large size was most likely part of an attempt at evading an antivirus emulation engine, since such systems usually emulate a small chunk of the entire binary.

In the end, two different vectors were identified, one installed at a public kiosk and a second installed on a device that was part of the check-in management network sensor. Though the two vectors looked different—mainly because of the copious amounts

The airport used the remediation module in QRadar EDR to clean up the infected devices and avoid data leakage. The solution's threat hunting interface helped confirm the absence of the vector from the entire infrastructure.

of junk instructions used to avoid detection—the malware appeared to be the same. In both cases, it was attempting to contact the same C2 server and behaving in the same way.

Attack reconstruction

When QRadar EDR is only deployed post-breach, not all information is available, and the native infrastructure uses only minimal operating system–level logging. Despite the minimal amount of information, a follow-up analysis showed that the infection happened five months earlier and that the two endpoints were infected a few days apart from two different USB drives. Other endpoints were infected by one of these vectors, mainly due to weak passwords that the malware tried matching at random intervals on every device it could connect to. The malware managed to collect information constantly and didn't appear to adopt any retention control or to apply limits to its own storage. A connection to the C2 was attempted every eight hours, but it was never successful due to the air gap.

The final analysis showed that, although the malware had self-replication capabilities and could automatically copy its storage to an external USB drive, this functionality was not enabled. Presumably, the exfiltration was supposed to be initiated manually.

Response and remediation

The airport used the remediation module in QRadar EDR to clean up the infected devices and clear the storage folders identified to avoid any data leakage. The solution's threat hunting interface proved essential for confirming the absence of the same vector from the entire infrastructure, except from the infected devices already identified. The airport also conducted a behavioral search to ensure that no instances of the malware were running undetected on other devices. It hunted for all identified behaviors, persistent threats and data collection methods until it could confirm the absence of that vector and its variants from the infrastructure.

Finally, the local security team established a more rigid set of rules for internal traffic control. The public part of the network was isolated from the operations, and the local security team started to run continuous endpoint monitoring and regular threat hunting campaigns.

Conclusions: eliminating major risks to airport service

An air gap can provide a strong level of security, but if not implemented in a strict way, it can create a false sense of security. Although the attack motivations remain unclear, because data was collected but never exfiltrated, we can confidently assume that the attackers had an open door into the infrastructure not just to exfiltrate information but also to actively damage the airport's operations. A simple ransomware launched against the check-in area would have created inevitable delays; the same attack launched against the security area would have outright managed to block flights and create severe repercussions.

The visibility provided by QRadar EDR allowed the reconstruction of the incident from the beginning and the safe remediation of the infection, without interrupting the airport's business continuity.

About the major international airport

This major international airport is one of the world's largest transportation hubs. Connecting 70 million passengers each year with more than 1,000 flights per day, the facility is classified as critical infrastructure.

Solution component

- IBM Security® QRadar® EDR

To learn more, contact your IBM Business Partner:

AI SecureNet LLC
208-407-2265 | team@aiSecureNet.com
www.aiSecureNet.com