TECH3

www.tech3.my

SURVIVING RANSOMWARE ATTACK

Taking You On The Narrative Journey Of The Attack And The Steps Taken In Response To The Incident.

Case Study

PROLOGUE

The Client recently overhauled its Backup and Disaster Recovery infrastructure with TECH3 Solutions. On top of refreshing the infrastructure, a thorough backup and recovery strategy were also put in place to ensure the Client is better prepared to mitigate any eventuality. The group had also signed up with our managed service, TECH3Care, to further monitor the backup validation and mitigate any issues.

Unfortunately, The Client recently fell victim to an opportunistic ransomware attack that had encrypted their master server and all virtual farms for 2 of their campuses. As a result, work was unable to continue, bringing operations to a standstill.

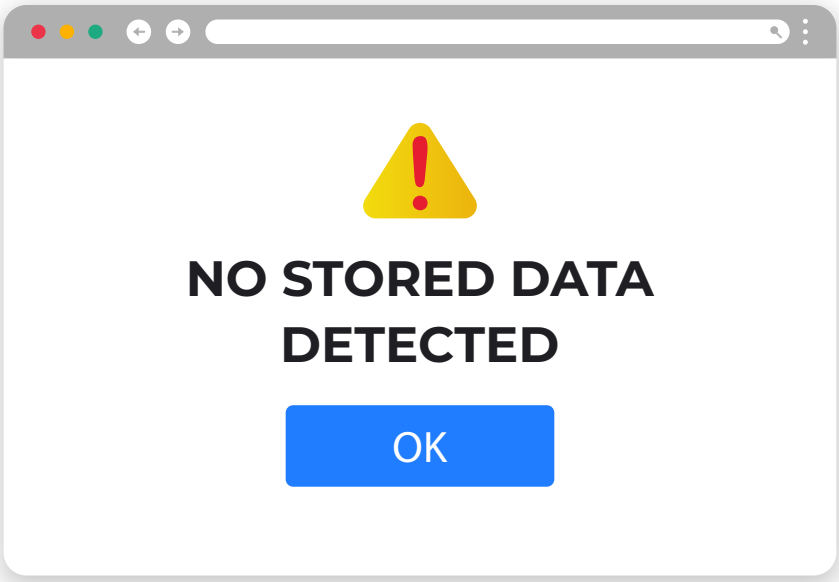
Remarks: The company requested this case study on their ransomware recovery project be posted anonymously.

PHASE 1

Identifying The Problem

Day 1 - Prepared For The Challenges

0530 HRS - It was a quiet morning when our team checked in to The Client's Data Center to monitor and validate the group's Backup from the day before. **Today, Something Was Amiss.**



The backups data was nowhere to be found, **"No Stored Data Detected"** was logged, and our engineers had a hunch that what they feared most, might have just come true.

“No Stored Data Detected”

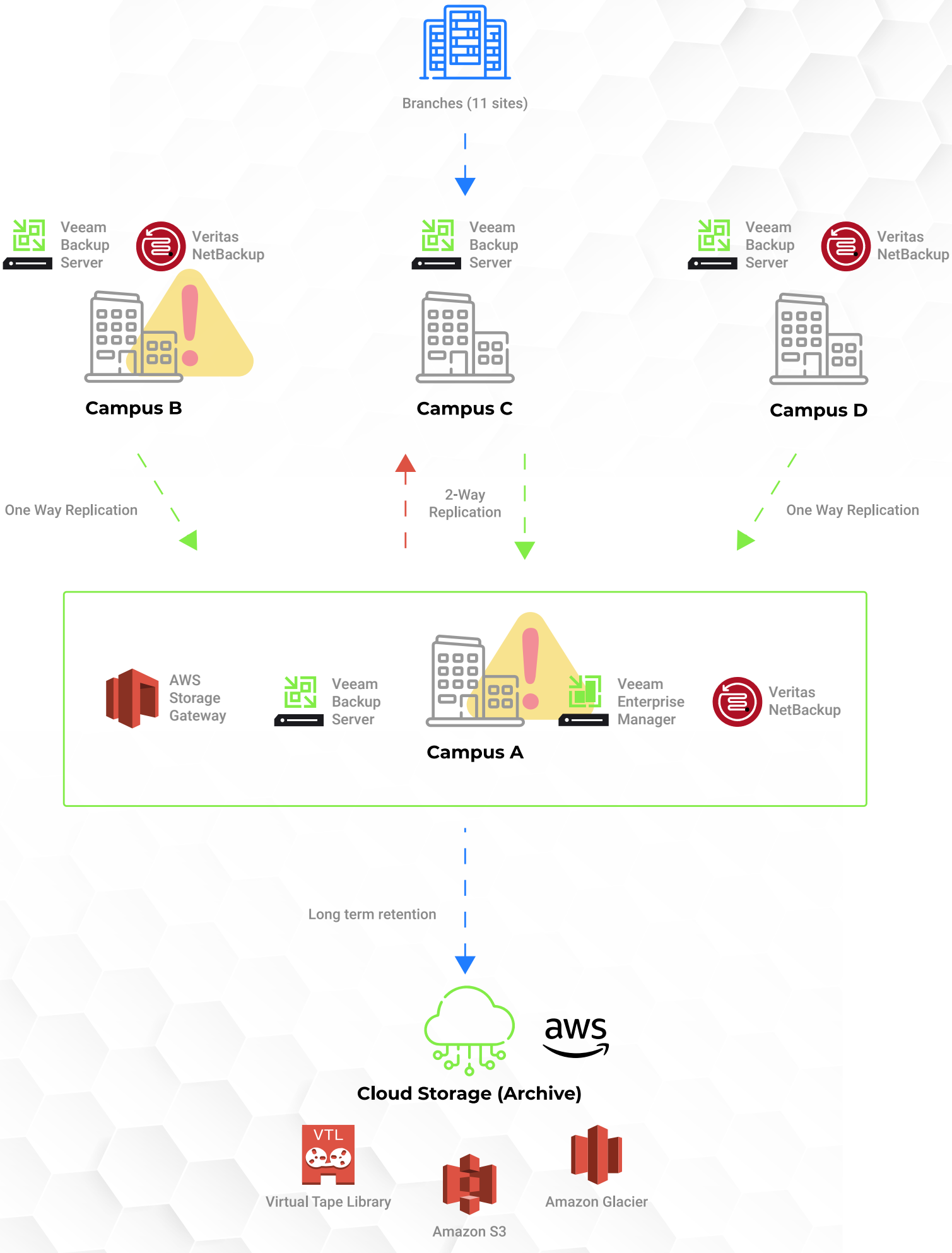
“No Stored Data Detected” could mean a few things at this point. Our engineers quickly ran through a series of checks and kickstarted the structured procedures, which were in place to address and mitigate such situations. With TECH3Care’s area of responsibility covering only the backup infrastructure, we have no access to the computing system to assess the attack further.

The customer’s Network Team was informed, and both teams raced to validate and cross-check all campuses to assess the extent of the damage.

Acting Fast

0630 HRS - Both teams were cut off from accessing the data center. The VPN connections were severed by the attackers to slow down any rescue effort.

Every new symptom allowed our engineers to assess the situation or incident better, which aligns with all the earlier checks and points toward one direction. The engineers made an educated decision:


Branches (11 sites)
Veeam Backup Server
Veritas NetBackup
Campus B
Veeam Backup Server
Campus C
Veeam Backup Server
Veritas NetBackup
Campus D
One Way Replication
2-Way Replication
One Way Replication
AWS Storage Gateway
Veeam Backup Server
Veeam Enterprise Manager
Veritas NetBackup
Campus A
Long term retention
aws
Cloud Storage (Archive)
VTL
Virtual Tape Library
Amazon S3
Amazon Glacier

0830 HRS - It was also concluded that the master server running NetBackup was no longer accessible as the data were wiped out altogether. Both teams regrouped, and by 0830 hrs, the client's Management team was notified of all the initial collected information and assessment reports.

The recovery process was initiated and the TECH3's engineers were ready to get on-site to get to the core of the problems.

PHASE 2

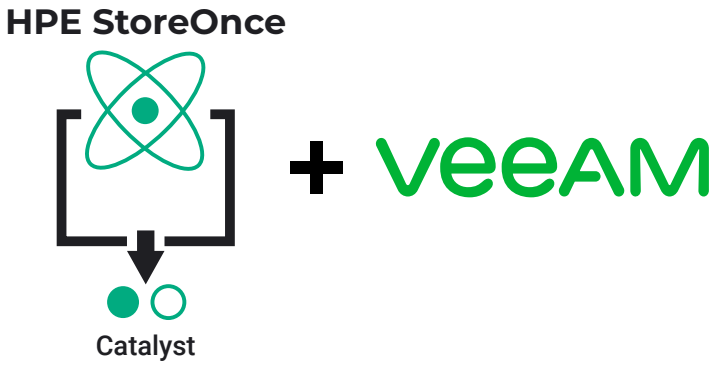
Tackling The Problem

Day 1 - Isolated Recovery Response

1100 HRS - Our engineers reached the Data center and performed further checks, and confirmed that the client was hit by ransomware. The extent of damage was also assessed further, and validation on local backup data was made.

Almost all backup data was wiped clean except for the copy stored in HPE's StoreOnce Catalyst.

StoreOnce Catalyst protect the mission-critical data stored from being either targeted or affected. Ransomware cannot encrypt what it cannot see, and because the Catalyst store does not use standard operating system command instructions for its operations, malware cannot become active while inside.



2300 HRS - TECH3's team completed the loan server setup to perform isolated recovery to verify the integrity of the data stored in HPE's StoreOnce Catalyst. Veeam's data recovery process commenced on the loan server once the setup was ready.

Our TECH3 Personnel also moved towards the 2nd affected campus to commence the recovery process for the remote site.

Day 2 - Data Integrity

0400 HRS - The Loan Server running Veeam recovery completed its first restoration after 7 hours, and a validation and check were run to ensure the restored data on both servers are safe and clean from any virus/code from the attack.

Unfortunately, both restorations from the data backup on the day before still contained traces of the malicious code. A few other cycles of restoration were made to ensure a clean copy of data was tracked down. It was fortunate that the team didn't have to look too far and only into three days ago.

1900 HRS - 37 hours into the incident, the team successfully located the clean data, reformatted the storage device to ensure that they were clear from any virus/malicious codes and performed a full backup restore into the loan unit.

A meeting was called between the client and TECH3 to both agree to the restoration version and proceed further to restore to the production server.

Day 3 - Restoration Completed

0400 HRS - Master VM Restore on NetBackup Server **COMMENCED.**

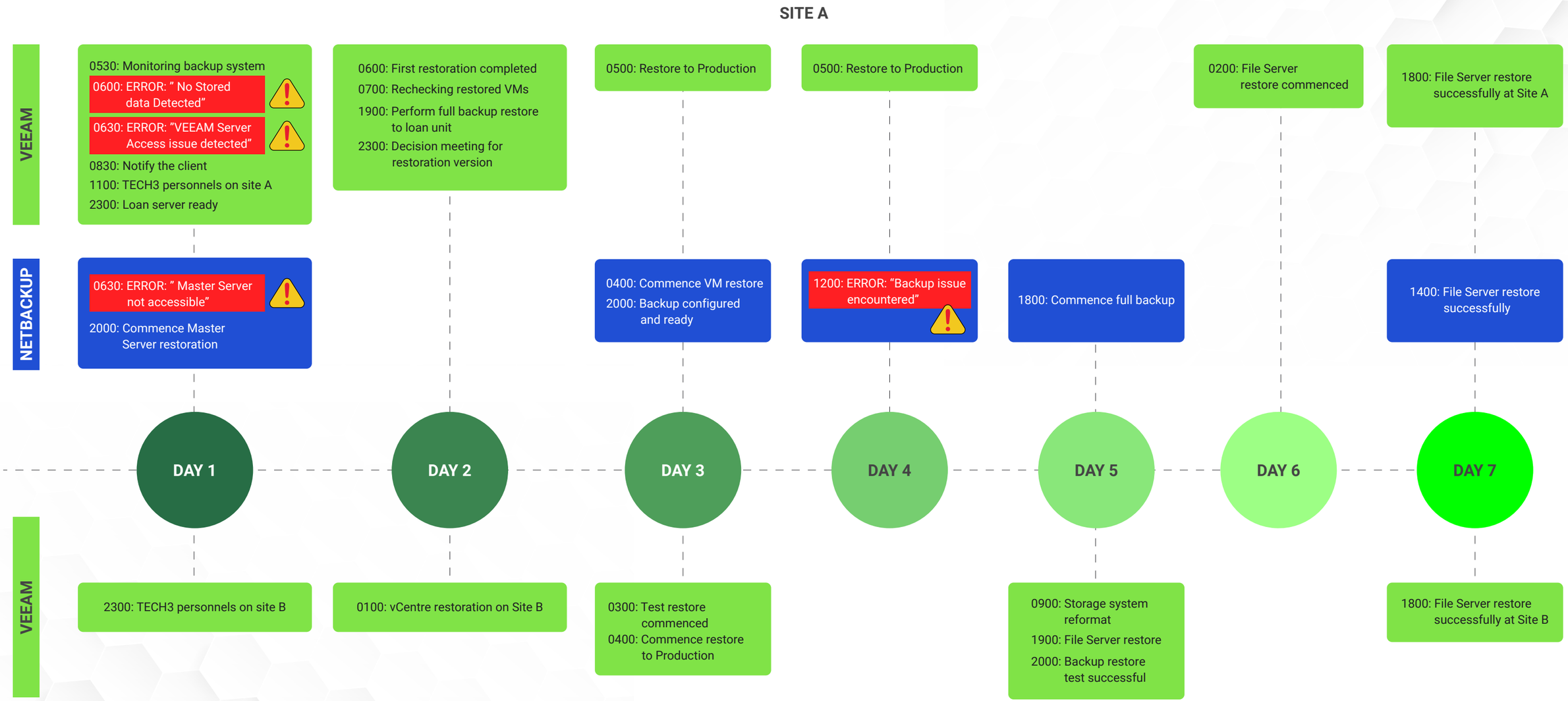
2000 HRS - Master VM Restore on NetBackup Server **COMPLETED.**

Day 4 - Restoration Completed & Resetting Backup

1200 HRS - Production Server restoration in both sites **COMPLETED.**

1330 HRS - The production server runs smoothly, and the backup repository was successfully reconfigured. This brought us closer to completing the restoration process, and a backup test was rerun 5 hours later, after working hours, to ensure everything was done right.

1930 HRS - Backup scheduling was set and running smoothly on the Production Server of the main campus.


SITE A
VEEAM
0530: Monitoring backup system
0600: ERROR: " No Stored data Detected"
0630: ERROR: "VEEAM Server Access issue detected"
0830: Notify the client
1100: TECH3 personnels on site A
2300: Loan server ready
0600: First restoration completed
0700: Rechecking restored VMs
1900: Perform full backup restore to loan unit
2300: Decision meeting for restoration version
0500: Restore to Production
0500: Restore to Production
0200: File Server restore commenced
1800: File Server restore successfully at Site A
NETBACKUP
0630: ERROR: " Master Server not accessible"
2000: Commence Master Server restoration
0400: Commence VM restore
2000: Backup configured and ready
1200: ERROR: "Backup issue encountered"
1800: Commence full backup
1400: File Server restore successfully
DAY 1
DAY 2
DAY 3
DAY 4
DAY 5
DAY 6
DAY 7
VEEAM
2300: TECH3 personnels on site B
0100: vCentre restoration on Site B
0300: Test restore commenced
0400: Commence restore to Production
0900: Storage system reformat
1900: File Server restore
2000: Backup restore test successful
1800: File Server restore successfully at Site B
SITE B

PHASE 3

Ensuring Minimal Impact

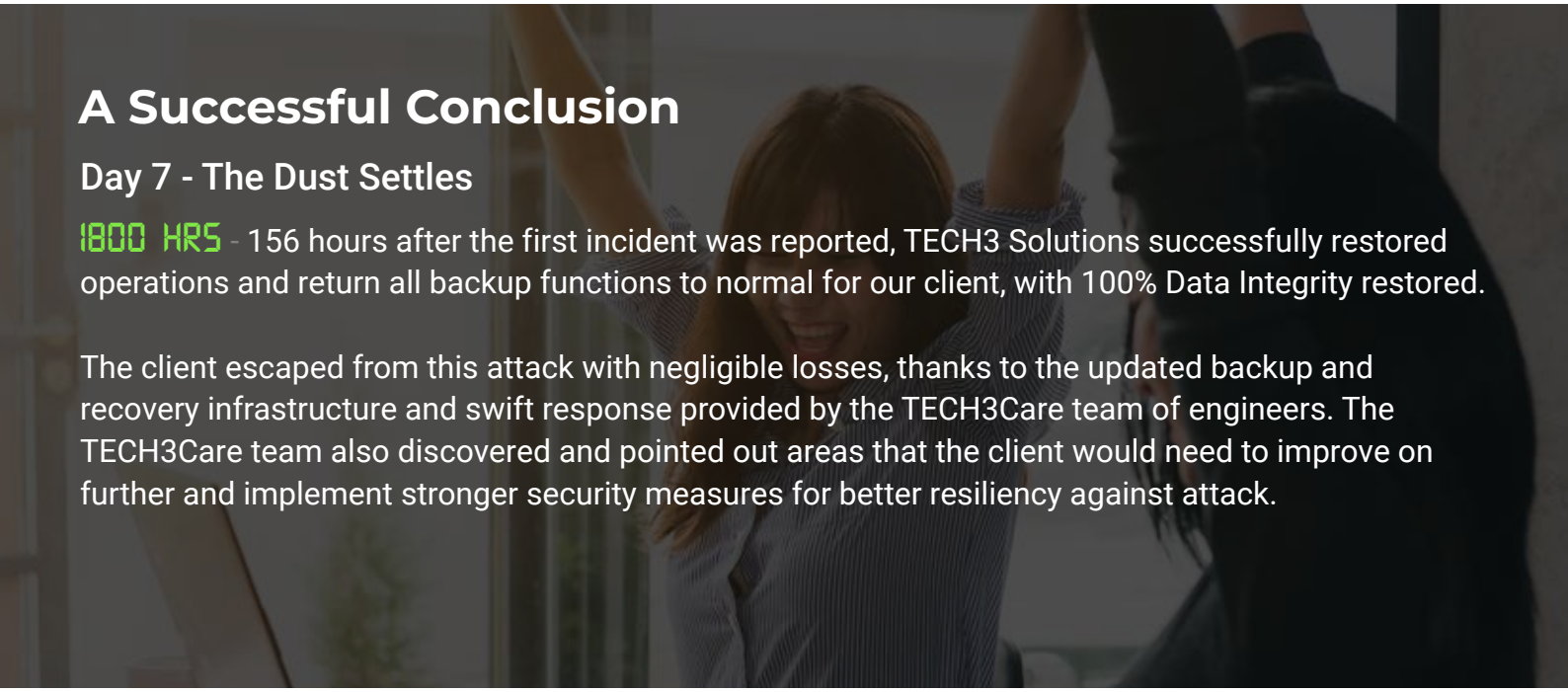
Day 5

1900 HRS - File Server restore for both affected campuses **COMMENCED.**

Day 6

1800 HRS - File Server restore for both affected campuses **COMPLETED.**

Things were not as smooth on the master server-side, as the backup was configured on 2000 hrs on Day 3, and a Data mismatch amongst the backup data on 1200 hrs, Day 4. This was due to the fact that the system did not find the incremental data between Restore Data Version and Data on Day 3 as the client restored the earlier data, skipping two days in between due to infected backup copies. This, however, is not a critical problem, but it took the next 60 hours to complete a full backup of the master server over the weekend on Day 6 & 7.



A Successful Conclusion

Day 7 - The Dust Settles

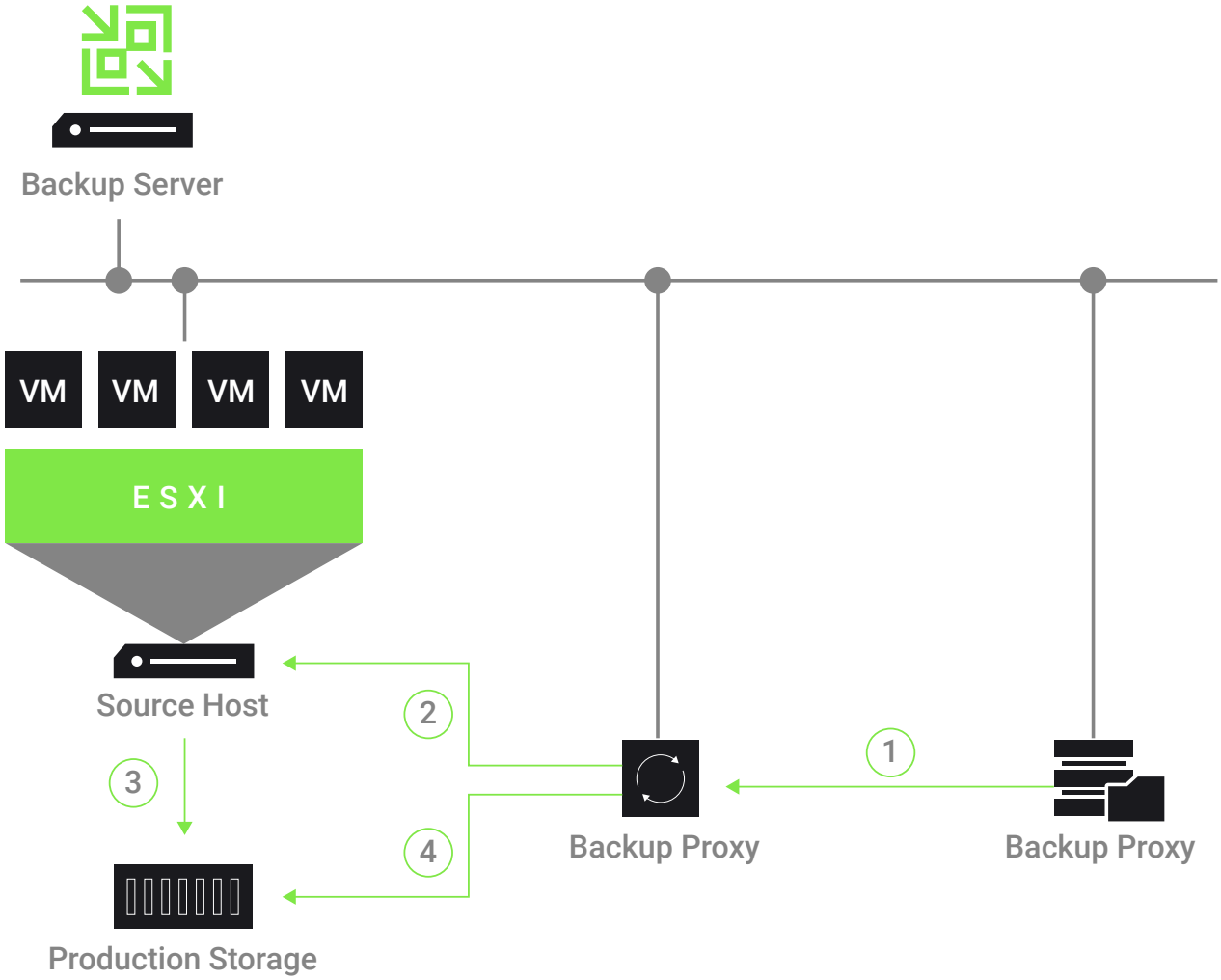
1800 HRS - 156 hours after the first incident was reported, TECH3 Solutions successfully restored operations and return all backup functions to normal for our client, with 100% Data Integrity restored.

The client escaped from this attack with negligible losses, thanks to the updated backup and recovery infrastructure and swift response provided by the TECH3Care team of engineers. The TECH3Care team also discovered and pointed out areas that the client would need to improve on further and implement stronger security measures for better resiliency against attack.

THE KEY TO SUCCESS

As TECH3 has set up VEEAM Direct SAN (Storage Area Network) access architecture for the backup previously with the client, we can now reap the benefits of VEEAM's Direct SAN Access Mode when running restoration. The Direct SAN access transport method provides the fastest data transfer speed and produces no load on the production network during restoration.

In the Direct SAN access transport mode, Veeam Backup & Replication leverages VMware VADP to transport VM data directly from and to FC, FCoE, and iSCSI storage over the SAN. VM data travels over the SAN, bypassing ESXi hosts and the LAN. The Direct SAN access transport method provides the fastest data transfer speed and produces no load on the production network.



1. The backup proxy retrieves data blocks from the backup repository or a datastore in the target site.
2. The backup proxy sends a request to the ESXi host in the source site to restore data to necessary datastore.
3. The ESXi host in the source site allocates space on the datastore.
4. Data blocks are written to the datastore.

TECH3CARE

The team from TECH3Care plays a vital role throughout the incident as they have proven their added value to the client's business throughout the 156 hours of the restoration process.

Starting from the first phase of the attack, the team of engineers show their commitment to help and work with the client at every step of the DR process and take full accountability for their work, staying overnight and working over multiple sites simultaneously to ensure the downtime is reduced and everything is returned to the norm as soon as possible.

TECH3Care Engineers also assisted the TECH3 Consulting team in assessing and providing clarity and recommendation in areas that would require further improvements during the post-disaster-recovery briefing to the client's top management team so that the client could make a planned decision based on the priority of their future IT spending, ensuring their IT investment are sound and would lead to support their IT environment and help ensure that their systems are safeguarded with improved resiliency against future attack.

TECH3 INCIDENT MANAGEMENT FRAMEWORK

When everything is going well, the framework is like a solid insurance policy that you trigger to ensure that your IT services are restored properly and unlikely to occur again. TECH3 uses a repeatable framework that has been proven and field tested so that our customers can rely on TECH3 to restore the service with confidence.

1. Detection

- Making an initial assessment of the incident
- Categorising software or hardware
- Assess the impact on the client's business

2. Isolation

Ensure that no further spread •
Containment and focus on affected systems •
Getting the right experts to help resolve the issue •

3. Restoration

- Restore service to the original configuration
- Ensure minimal interruption to business
- Restore to the last restoration point

4. Root Cause

Post-restore deep dive into analysing the cause •
Recommendations to prevent future occurrence •
Update knowledge base •
Lesson learned •

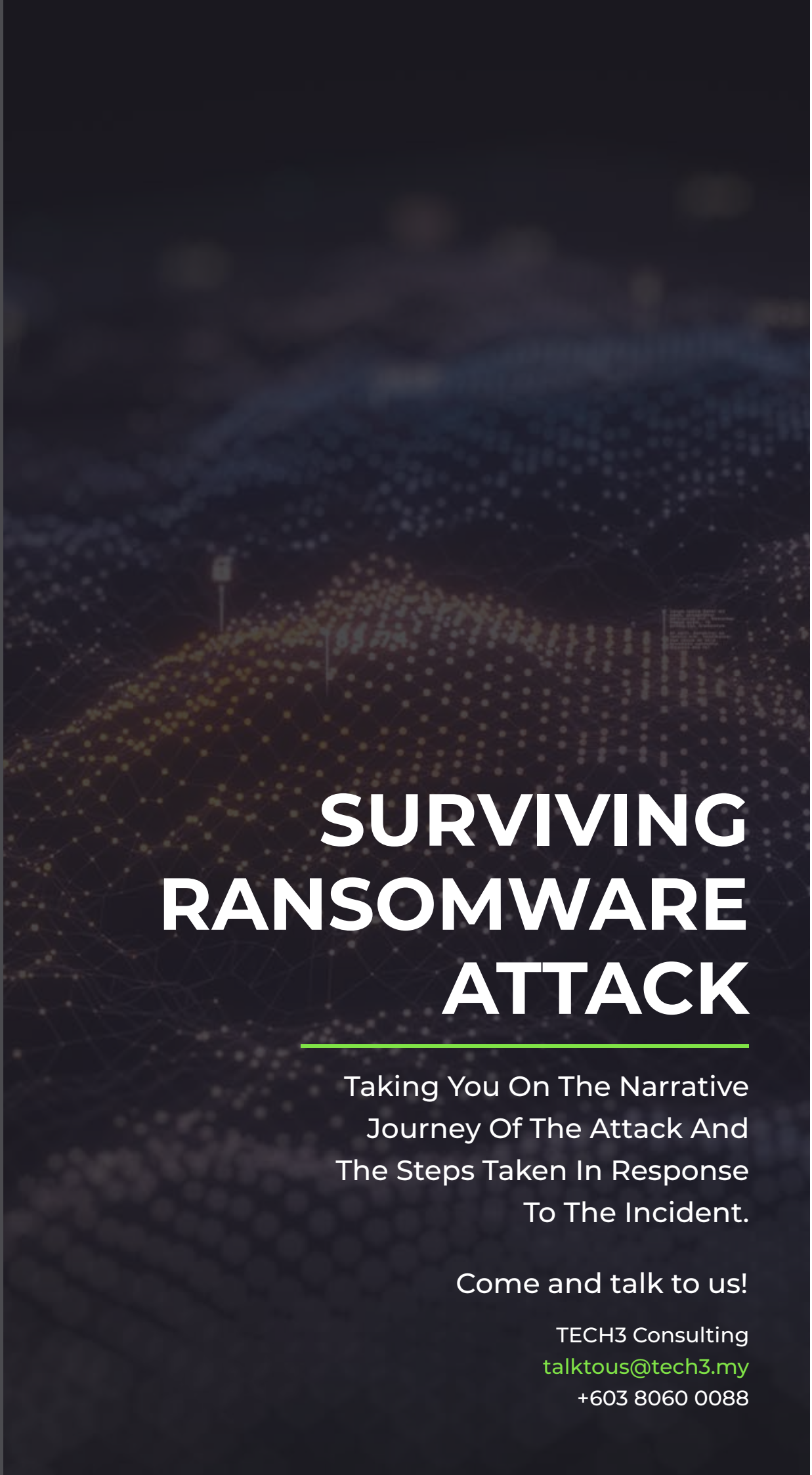
SOLUTION FRAMEWORK FOR FUTURE SAFEGUARDING

TECH3 Consulting approach all client challenges and design solutions based on ITIL's People, Process, and Technology framework. These 3 critical elements form the basis of an organisational management and transformation strategy, providing guidance to organisations in decision making by prioritising certain factors, namely, People first, Process second, and Technology third, especially when designing a new service or making changes to an existing one.

With the attack exposing weak points in system login credentials, an attack as such will cause operational losses and man-hours to restore all systems. Our solution will have to put the people of The Group at the forefront in every decision we make. The recommended changes allow the group to reduce man and labour by having better security, better backup system and faster recovery. Existing IT specialists could then focus on solving higher value issues during a recovery process, and business operations could return to the norm sooner.

Tech3 discovered various process pain points that could further improve the security and integrity of the data protected. The team revisit the backup and recovery process and found room for improvements. With a clear process and the right technology, future recovery processes could be faster, and data could be better protected.

Technology is the primary delivery route for virtually all value in a modern organisation, as most services are enabled by technology. The right technology could fulfil the People and Process factor above. The attack points out several pitfalls in the compute server and network infrastructure that could protect data better, and speed up the recovery process, minimising the impact of such future events.



TECH3

www.tech3.my

SURVIVING RANSOMWARE ATTACK

Taking You On The Narrative Journey Of The Attack And The Steps Taken In Response To The Incident.

Come and talk to us!

TECH3 Consulting
talktous@tech3.my
+603 8060 0088

Case Study