Zero Day
Security

Business Continuity Plan

Zero Day Security Ltd.

Colin Cooper
R00240295

Security Contingency Planning
(COMP 9081) 2022/23 - Assignment 2

Table of Contents

1) Introduction

1.1. Background

Zero Day Security ("0-DS") is a Managed Detection and Response (MDR) provider specialising in outsourced cybersecurity monitoring, threat detection and remediation services to its customers. 0-DS's typical customers are small enterprises with between 50 and 250 employees for whom a dedicated in-house Security Operations Centre (SOC) would not be financially feasible. Through a shared service model, 0-DS is able to dilute SOC operational costs - such as the physical secure SOC environments, hardware, networking, threat analyst staff costs, and threat detection and forensics software licensing costs - among its customer base to offer a service that scales to the needs and budgets of small organisations.

To perform threat detection, 0-DS's customers install a client application on managed endpoint devices to capture events that are then sent to a cloud-hosted application called TITAN. TITAN stores all events for up to 30 days in a data storage service where the events are analysed against several threat intelligence feeds and known patterns of threat activity. If a suspicious event pattern is matched, an incident investigation ticket is created in TITAN and queued for manual inspection by a threat analyst in the detection team. If the analyst determines that the investigation ticket requires escalation for further analysis or reaction by the customer, TITAN assigns a responder from the Customer Incident Response team and the affected customer is informed.

0-DS had gross revenues of €15.2m in 2021 from 350 customers mainly based in the UK, Ireland, and Sweden from which it made an operating profit of €3.6m in the same period. The company has three centres of operation: in Cork (Ireland), Reading (UK) and Stockholm (Sweden). All three sites are fully operational Security Operations Centres and share visibility of data stored in TITAN.

0-DS also has its own internal operational functions and systems including HR, payroll, finance, sales, marketing, and procurement departments. Each department uses a variety of applications to perform its day-to-day functions, some of which are cloud-based, and others hosted in a small on-premises data centre that is physically located in Cork.

1.2. Scope

This Business Continuity Plan has been developed for the customer Threat Detection and Response system which includes the TITAN suite of data and services and the sites that operate the TITAN application to serve customers' security needs. This system is classified as a high-impact system [1]. Procedures in this Continuity Plan are designed to recover Threat Detection and Response services within 4 hours (Maximum Tolerable Downtime).

1.3. Assumptions

The following assumptions were used when developing this Continuity Plan:

- TITAN has been established as a high-impact system [1].
- TITAN is a set of data storage and processing services hosted by a Cloud Service Provider, Amazon Web Services.
- Internal TITAN users are mainly threat analysts located in three site facilities. Each of the sites acts as a potential redundant backup for the others. Each site also has physical seating and facilities capacity to cope with a temporary 50% increase in employee numbers due to relocation from another site
- One of the three site facilities is unavailable due to flooding and is unable to host employees or allow access to TITAN.
- Due to security concerns and to minimise the threat surface of TITAN, access to TITAN through VPN is not permissible and not considered while at least two of the three regional sites are operational.
- Current backups of the TITAN backend databases are intact and available on secure AWS S3 storage services.
- Key TITAN personnel have been identified and trained in their emergency response and recovery roles and are available to activate this Continuity Plan.

2) Concept of Operations

2.1. System Description

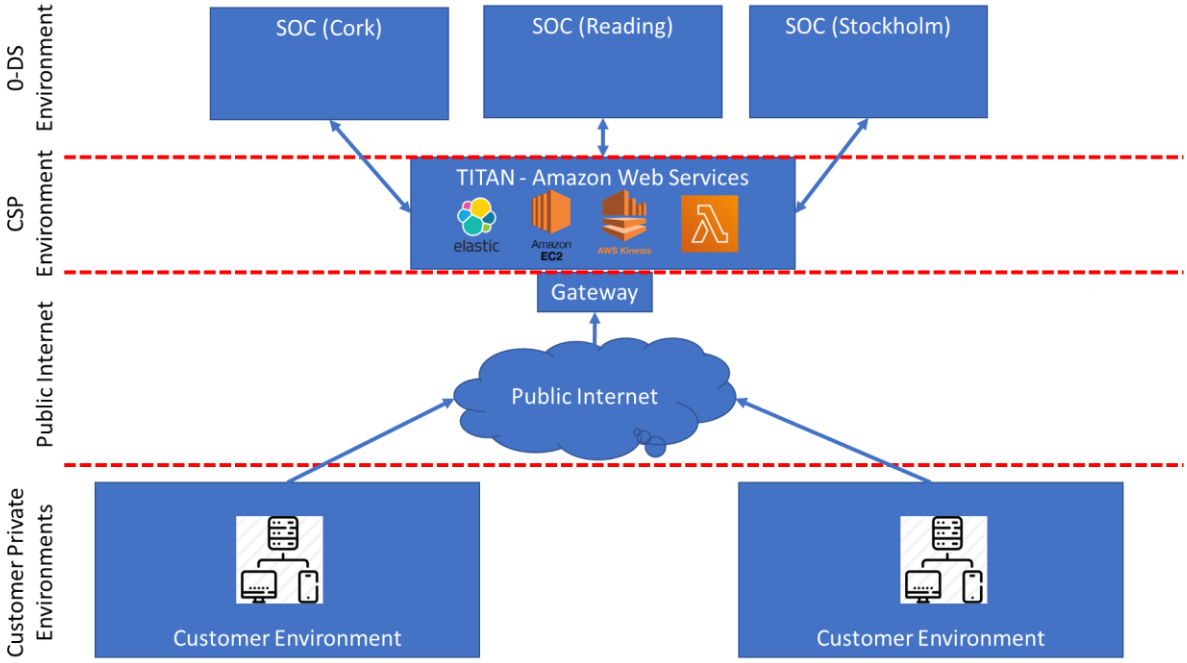

Figure 1: TITAN High Level Architecture

Figure 1 shows a high-level conceptual overview of the TITAN architecture. Event collection agents are deployed by the customer in their own environments, where they are queued for sending to a public-facing gateway. The on-device queuing mechanism allows for events to be buffered on each individual endpoint if the gateway is unreachable for any reason such as an endpoint being offline for a period, or the gateway itself experiencing a service outage or degradation. The buffer size is configurable by each customer, but as a rule of thumb an average endpoint buffer can store up to 5 days of event data before old events are flushed to make way for newer ones.

Communication between customer environments and the public-facing gateway is over the public internet. This communication is sent over HTTPS using TLS 1.2 to ensure the privacy and integrity of the data-in-transit. The gateway uses metadata (effectively API keys linked to the customer ID) sent in the communication to validate that the data being received is from a legitimate customer endpoint.

Once validated by the gateway, the data enters the main processing and data storage functions within private Virtual Private Clouds (VPCs). These VPCs link the storage and processing services running in the AWS environment and are not publicly accessible except through the gateway or from AWS users and roles that have been given appropriate access rights.

As a cybersecurity services vendor, 0-DS is its own customer for threat detection and response services. The company deploys its endpoint agents on its own internal infrastructure and sends endpoint events to the same TITAN system for analysis that is used by its customers.

Finally, the three regional sites utilise AWS Direct Connect to establish a dedicated connection from each office to the TITAN VPCs. This allows threat analysts working in each site to access the TITAN application interface to perform their work. However, it also means that the TITAN application is not available from outside the physical SOC sites. Employees can only access basic email services, payroll, and HR systems from their homes through VPN.

2.2. Business Continuity Phases

The BCP has been developed to recover the Threat Detection and Response system (including TITAN) using a three-phased approach:

- **Activation and Notification Phase** that involves activation of this plan where a disruption or outage has been identified that may exceed the MTD. System owners and stakeholder will be notified, and an assessment of the outage executed that will determine the recovery process specific to the cause of the outage.
- **Recovery Phase** that involves using established documented procedures to recover the system while ensuring key stakeholders receive appropriate and timely communications.
- **Reconstitution Phase** that involves testing and confirming the restored system capability and deactivating the continuity plan.

2.3. Roles and Responsibilities

This BCP establishes several roles for the phases outlined in Section 2.2. The people in these roles have been trained to respond to an incident that affects the Threat Detection and Response system.

Role	Phase	Responsibilities

Threat Analyst	Activation & Notification	• Notify immediate line management if any service disruption is noticed in TITAN.
Customer Support Analyst	Activation & Notification	• Notify immediate line management if any service disruption is noticed in TITAN.
Customer Support Director	Activation & Notification	• Create customer KB articles to direct customers to the latest service availability information • Send notification to affected customers with links to KB. • Inform all customer support agents about the incident and the KB so they can quickly answer customer escalations and direct customers to the right information.
Security Operations Director	Activation & Notification	• Review TITAN outage escalations, and if MTD is likely to, or has exceeded 4 hours, notify CISO
CISO	Activation & Notification	• Declare and communicate an Incident and initiate the Business Continuity Plan • Constitute the Business Continuity Team, including the BC Project Manager to send the initiation communications
Business Continuity Project Manager	Activation & Notification	• Set up incident war room (Zoom online meeting) and a portal to show latest incident status, action plans and owners
IT Director	Activation & Notification	• Perform initial outage assessment
Security Operations Director	Recovery	• Provide ongoing feedback to the Business Continuity Team on system status
IT Director	Recovery	• Provide ongoing information around root cause investigation of the incident • Open Severity 1 ticket with Amazon Web Services and act as an interface between the AWS customer service agent and the Business Continuity Team • Act as liaison point between the organisation and network services /

		electricity / utility providers to the site where appropriate • Order or source replacement hardware
Business Continuity Project Manager	Recovery	• Provide co-ordination services to the Business Continuity Team to ensure actions are clear, assigned, and have definite timeline expectations.
Facilities Director	Recovery	• Provide ongoing information around site availability issue investigation • Act as liaison point between local services such as emergency services where appropriate
Security Operations Director	Reconstitution	• Confirm restoration of network, electric services to site
IT Director	Reconstitution	• Confirm restoration of network, electric services to site
Security Operations Director	Reconstitution	• Confirm restoration of Threat Detection and Response services
Customer Support Director	Reconstitution	• Send notification to customers about service restoration
CISO	Reconstitution	• Deactivate the Business Continuity Plan

2.4. Business Continuity Planning Background

In recognition of the fact that the company depends on several key activities and services to operate, senior management at 0-DS initiated a Business Continuity Planning exercise. A BCP team was established consisting of knowledgeable team members from Operations, IT, Sales, Marketing (including Public Relations), Facilities, HR, and Finance & Accounting departments. A BCP project manager had also been hired to oversee the development of the BCP and Disaster Recovery planning, design, implementation, and maintenance of these plans.

The scope of the Business Continuity Planning was defined and signed off by senior management with agreement that the scope of the exercise should focus on:

- Site loss due to events such as natural disaster that would make a site inoperable for an extended period.
- Loss of critical cloud-based services related to the TITAN system

The development of this plan was guided by the NIST SP 800-34 Standard [2].

3) Plan Activation Procedures

3.1. Activation Criteria and Procedure

The Threat Detection and Response System BCP may be activated when any of the following criteria are met:

- The nature of the outage suggests that the system will be out of services for more than 4 hours.
- A site that is involved in Threat Detection and Response services is damaged and may not be available for more than 1 week.

3.2. Notification

On activation of this BCP, notification will be sent immediately to appropriate business and IT staff. Contact information for each point of contact is included in the Appendix C: Contact List section. To ensure that key contacts do not miss the notification, both text and email notifications should be sent.

Communication Initiator: Business Continuity Project Manager

Communication Method: Email and Text Message to the contacts in Appendix C. Recipients are required to respond to at least one of the communication methods to confirm they have received the notification.

3.3. Outage Assessment

Following notification, the IT Director is responsible for leading the initial outage assessment to determine the best estimated scope of the outage (including affected systems and component subsystems), likely causes, expected recovery time, and next remediation steps. The IT Director can call in support as needed from specialised teams such as Database Administrators, Network Engineers, Application Architects, and 3rd Party provider customer support contacts.

4) Recovery

Once the initial Activation and Notification phase has completed, the team moves into a Recovery phase to recover control over any compromised systems, restore data from backups, or return non-functioning components to a functioning state.

4.1. Recovery Procedures

- Site Outage
  - If the outage is related to long-lasting damage to a single site that means that recovery will take more than 2 days, but less than 1 week, the Security Operations Director will work with HR and staff to institute an emergency rota in the remaining sites to increase the threat analyst capacity of those teams on a temporary basis.
  - If the recovery of the site is likely to take more than 1 week, then additionally the company will plan to transport and accommodate threat analysts from the affected site to one or both remaining sites. While this would involve significant short-term additional operating costs for the company, it is critical for the company to maintain its SLAs.
- If the TITAN system itself is affected, the company will initiate the following:
  - Take the API Gateway offline if it available to prevent new events from coming into the TITAN system while it is being restored. Events will queue on the individual endpoints while the system is offline.

  - Retrieve full, incremental, and differential backups as appropriate from the write-once / no delete S3 backup.
  - Restore any corrupted or destroyed databases from the backups.
  - Tear down any compromised virtual machines and restore from an approved image.
  - Review the restored system against a CloudFormation template to identify any anomalies in the configuration (such as unapproved users or roles being in existence) and remove them.
  - Put the API Gateway back online.

4.2. Recovery Escalation Notices / Awareness

During the period of recovery, the Business Continuity Project Manager will maintain a portal containing the latest status of the incidents including metrics, actions and owners, next steps and timelines, and key contact information. The status of the incident will be communicated to company senior leadership not less than once every 12 hours or as necessary.

A link to the status portal will be included with all email status updates to ensure that everyone is working off the latest information and plans and to ensure there is always one "source-of-truth" about the incident.

5) Reconstitution

Reconstitution and BCP deactivation occur when recovery activities have been completed and regular operations can resume.

If a site is complete unrecoverable (for example due to a devastating fire or natural disaster), preparation for a long-term replacement site will commence in this phase.

During this phase, the successful reconstitution of the system will be verified, and this plan will be formally deactivated.

5.1. Concurrent Processing

0-DS's cloud architecture is multi-regional, and load-balanced. Redundant data storage for databases and redundant virtual machines for threat detection processing occurs in multiple regions and is load balanced. If one of TITAN's regions had suffered a major outage, the other regions would scale up their resource allocations to compensate. For this reason, there is no concept of a temporary operational environment during the incident, so there is no need for a temporary concurrent processing phase. One the affected region has been restored, it will be made active again for handling incoming event loads, and the temporary resources in the other regions scaled back down to normal levels.

5.2. Validation Data Testing

If a primary node for a relational database had been corrupted, the system would automatically fail over to a secondary replica which would then become the primary node until the original primary node had been restored. To ensure that the failover has happened seamlessly, the Database Administrators will run a series of tests to validate that there are no time gaps in the event data that has been stored.

If both the primary and secondary database had become corrupted or destroyed, it would be necessary to restore the databases from S3 backups. Due to the 1-hour incremental backup schedule, it's possible that up to 1 hour of event data could be missing. Database Administrators will again run a series of tests on the data to ensure that no more than 1 hours' worth of data has been lost.

5.3. Validation Functionality Testing

To confirm that the Threat Analysers running in EC2 and AWS Lambda are again fully operational, several validations will be carried out:

- Threat Analysts will review the incoming investigation queues and confirm that investigation cases are being created at a normal rate.
- System telemetry will be reviewed to ensure that events are being ingested to the system through the gateway at a normal rate. A slightly higher than normal rate should be expected if the gateway has been offline for some time. This is expected as the customer queues will have built up during the period of downtime.
- Internal and AWS cloud logs will also be reviewed to ensure that no unexpected errors are being logged.

5.4. Recovery Declaration

Once the data and functionality validation has been completed, the Business Continuity Team will meet to review the results and if they are agreed, they can collectively declare that the recovery efforts are complete, and that the system has returned to normal operation. The incident portal will be updated to reflect this, and the Project Manager will notify the various stakeholders.

5.5. Notifications (users)

Following the recovery declaration, customers will be informed that normal operations have resumed. The same email list and notification template will be used to make this communication.

If any customers have suffered any data loss during the incident, they will be informed of the scale and likely timeline of the data loss so they can take appropriate action in their environments.

5.6. Data Backup

Following recovery, a full backup should be done on all data sources and added to the S3 write-once no-delete storage location. A full backup can be initiated by the IT Director using a predefined script to kick off cloud backup activities.

5.7. Event Documentation

Records such as meeting minutes, tracking documents, and communications between third parties will be consolidated and saved. The team will conduct a full root cause analysis of the incident and put in a remediation plan to ensure that no similar issue is likely to reoccur in the future. Lessons learned (both positive and negative) will be documented and improvements made to the BCP.

5.8. Deactivation

Once all the preceding tasks have been completed, the Business Continuity Project Manager will formally deactivate the BCP recovery and reconstitution efforts and communicate this to the contact list.

Appendix A: BIA Risk Assessment

A Business Impact Analysis (BIA) was conducted that identified the assets that are used to underpin key operational processes. A risk analysis was carried out with key risks identified and an impact assessment for each was captured and documented.

Asset	Risk	Business Impact	Mitigation & Preventive Controls
Physical Site Availability	Site becomes unavailable due to fire, flood, natural disaster, or long-term power loss	The unavailability of any individual site would impact on threat investigations for that region	The workload of each site would seamlessly fall to the other available sites, however in the medium-erm, human capacity to handle the work volume would cause difficulties until the damaged site could be restored.
TITAN Gateway	DDOS Attack	A sustained attempt to overload the TITAN gateway would slow the ingestion of events from genuine customer endpoints.	Customers provide valid public IP addresses and ranges as part of the customer onboarding processes. There IP addresses are added to a firewall policy that limits access to the Gateway service. If excessive malicious connections are coming from a valid customer IP address, the customer will be first contacted to remediate the issue, and in case of significant cross-customer impact, specific IP addresses will be blocked. Use of AWS Cognito to validate and authorise incoming connections using customer API keys and

			discard unauthorised connections.
TITAN Gateway	Gateway Unavailability due to service fault	Gateway unavailability would prevent customer endpoints from uploading events. Such events would be queued on the endpoints for a period until a storage buffer maximum value is hit, but in the meantime, customers would not be able to get threat detections from those events.	The API is deployed in three regions (eu-west-1 (Dublin), eu-west-2 (London), eu-north-1 (Stockholm)) in an active-active configuration, and set up AWS Route 53 to failover to one of the healthy API endpoints if another should fail.
TITAN Storage	Customer data suffers unauthorised access or modification	Unauthorised access to customer endpoint event data would cause concern for customers as events can contain sensitive data such as endpoint names, usernames, and IP addresses. Unauthorised modification of data would risk missing threat detections and undermine 0-DS's ability to provide a verifiable audit trail for an attack on customer endpoints.	Data is encrypted in transit through HTTPS with a minimum TLS version of 1.2. This ensure data cannot be viewed or modified while being transferred to 0-DS's environment. A SHA-256 checksum is included with event data coming from the endpoint to ensure the data is free from deliberate modification or corruption. Data is encrypted at rest in the AWS Relational Database Service through AWS configuration.
TITAN Storage	Data loss due to deliberate or accidental malicious behaviour such as internal employee deletion	TITAN data loss would be catastrophic in terms of reputation and ability to serve the threat detection needs of customers who would lose up to 30 days of event history.	A full replica of the TITAN storage is configured in a separate AWS region with real-time synchronisation of data modification. If the primary data storage were to become corrupted, the replica storage would become the primary while the corrupt instance is being restored.

			Nightly full backup of TITAN databases to S3 deletion-protected storage, differential backup every 6 hours, and incremental backup every 1 hour. This means the maximum possible data loss is 1 hour.
TITAN Services	Data analysis services fail due to cloud service outage	The failure of data analysis services would prevent threat detection analysis being conducted on the incoming event data. Customers would be delayed in receiving potential threat detection notifications, leading to delayed reaction to cybersecurity attacks.	A copy of the data analysis services that run through a variety of lambda functions and EC2 Linux instances are run in each of the three AWS regions. If one of those regions suffers an outage, the AWS Route 53 DNS service will take that environment offline and distribute the analysis work among the remaining 2 regions until the faulty region has been restored. Auto-scaling of EC2 instances within each region ensures that the additional load can be handled even if 2 of the other 3 regions are offline.
HR & Payroll System	System Unavailability due to service outage or malicious action	The HR and Payroll system is hosted in an on-premises data centre. If this system were to become unavailable, then monthly payroll operations would be impact leading to inability to produce employee payslips or process tax deductions.	The application is self-hosted in the Cork on-site data centre. Full backups are taken monthly on the day after payroll processing has completed. Because employee data such as tax credits and salary change infrequently, differential backups are taken weekly. The system is hosted on a server using RAID-1 storage so that a fault in any individual disk will not cause

			immediate service downtime as data is mirrored across 2 physical disks.

Appendix B: Customer Service Level Agreements

In planning risk mitigation and Business Continuity Planning, the following SLAs were agreed based on contractual customer commitments or internal operational goal setting:

Service	**Minimum Operational Metric**	**BIA Metrics** Maximum Tolerable Downtime (MTD) Recovery Point Objective (RPO) Work Recovery Time (WRT)
TITAN Availability	99.9% Availability (customer contract)	MTD: 4 hours RPO: 1 hour WRT: 3 hours
Threat Detection Lead Time from Event	99% within 1 hour 99.9% within 6 hours (customer contracts)	N/A

Appendix C: Contact List

Threat Detection and Response System Key Personnel		
Key Personnel	**Contact Information**	
CISO	Work	+353 21 4 123456
Rachel Murphy	Home	+353 21 4 877777
76 Roundwood Dr.	Mobile	+353 86 020 0000
Cork	Email	rachel.murphy@0day.ie
IT Director	Work	+46 872 82 89 82
Sven Erikson	Home	+46 872 92 90 26
2 Lothbrook	Mobile	+46 242 87 82 28
Stockholm	Email	sven.erikson@0day.ie
Customer Support Director	Work	+353 21 4 123567
Sasmita Malik	Home	+353 21 4 874018
90 Bellevue Woods	Mobile	+353 86 020 1111
Cork	Email	sasmita.malik@0day.ie
Facilities Director	Work	+44 207 2322 1293
David Greenwood	Home	+44 207 9832 2982
132 Pine View	Mobile	+44 7808 148 2093
Reading	Email	david.greenwood@0day.ie
Business Continuity Project Manager	Work	+353 21 4 123678
Peter O’Neill	Home	+353 21 8637 272

87 Northwood Road	Mobile	+353 86 020 2222
Cork	Email	peter.oneill@0day.ie
Security Operations Director	Work	+353 21 4 123900
Erica Lapuste	Home	+353 23 987 1625
Murragh House, Bandon	Mobile	+353 86 020 3333
Cork	Email	erica.lapuste@0day.ie

Appendix D: References

[1] US Department of Commeric, “Standards for Security Categorization of Federal Information and Information Systems,” February 2004. [Online].

[2] M. Swanson, P. Bowen, A. Wohl Phillips and D. L. D. Gallup, “Contingency Planning Guide for Federal Information Systems,” May 2020. [Online]. [Accessed 02 December 2022].