Haydn Bowers

NIST CSF

Building a Security Operations Centre

Contents

01

Frameworks

How to choose a framework?

National Institute of Standard & Technology

Frameworks

NIST CSF

SP 800-12

SP 800-30

MITRE ATT&CK Matrix

Australian ISM

ASD Essential 8

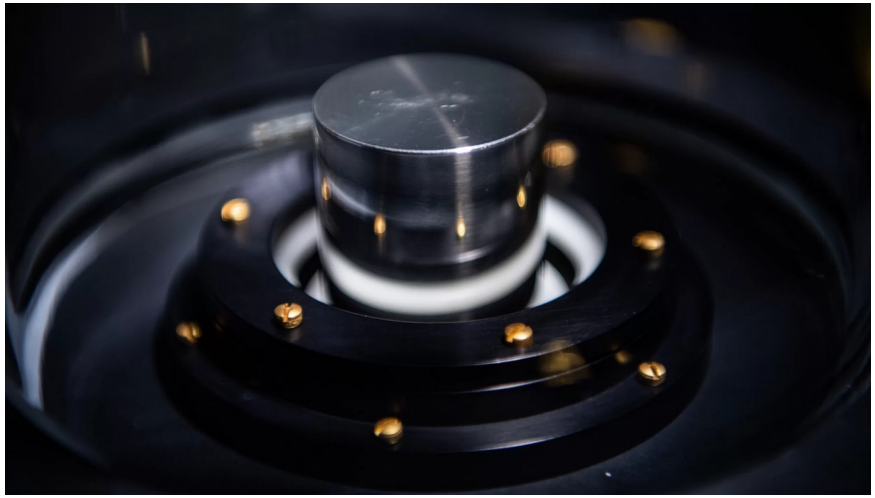
ASD 37 Security Controls

ISO 27001/27002

SABSA

PCI DSS

NIST: National Institute of Standards and Technology



In the news:

- Developing a Privacy framework
- Developing a new Atomic Clock

THIS WEEK:

- Re-defined the Kilogram
  - Mass is now just an abstract concept

NIST: Special Publications 800 series
Computer Security

accelerate your ambition

- **SP 800-12: Intro to Security**
- SP 800-22: Random Number Generation
- SP 800-37: Risk Management Framework
- SP 800-38: Block Cipher Modes
- SP 800-41: Firewall Policies
- SP 800-114: BYOD Security
- SP 800-124: Mobile Device Management
- SP 800-144: Public Cloud Computing
- SP 800-145: Definition of Cloud Computing
- SP 800-177: Trustworthy Email
- SP 800-179: Securing Apply macOS
- SP 800-187: LTE Security
- SP 800-204: Microservice Security

https://csrc.nist.gov/publications
https://www.nist.gov/itl/nist-special-publication-800-series-general-information

SP 800-12 Rev.1

accelerate your ambition

- Security Mission
- Role & Responsibilities
- Threat & Vulnerabilities
- Policy Objectives
- Risk Management
- Assurance & Audits
- Cryptography
- Controls

Defined Controls

- Access Control
- Audit & Accountability
- Configuration Management
- Incident Response
- Privacy
- Personnel Security
- Risk Assessment

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

NIST: Special Publications 1800 series
Cybersecurity Practice Guides

accelerate your ambition

- SP 1800-1: e-Health Records
- SP 1800-3: Attribute Access Control
- SP 1800-4: Mobile Device Security
- SP 1800-6: DNS Email Security
- SP 1800-7: Situational Awareness
- SP 1800-15: Small Business & Home
- SP 1800-16: TLS Certificate Management
- SP 1800-17: Privilege Management for Financial Services
- SP 1800-19: Trusted Cloud

https://www.nist.gov/itl/nist-special-publication-1800-series-general-information

02

Security Operations Centre

NIST - Cyber Security Framework

- Identify
- Protect
- Detect
- Respond
- Recover

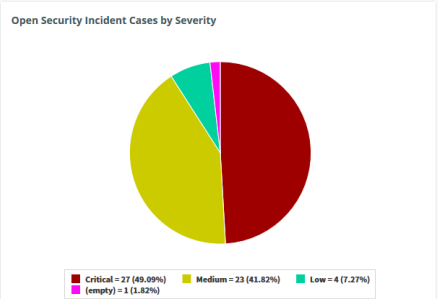
Objectives of a Security Operations Centre

Operate – Execute operational processes

Manage – Prevent, predict, detect, and respond

Optimize – Continually improve security processes, platform, and controls.

- 24/7 log collection and active monitoring
- Security event escalation and context-aware alerting
- Customizable advanced analytics
- Analysis and validation by certified security experts

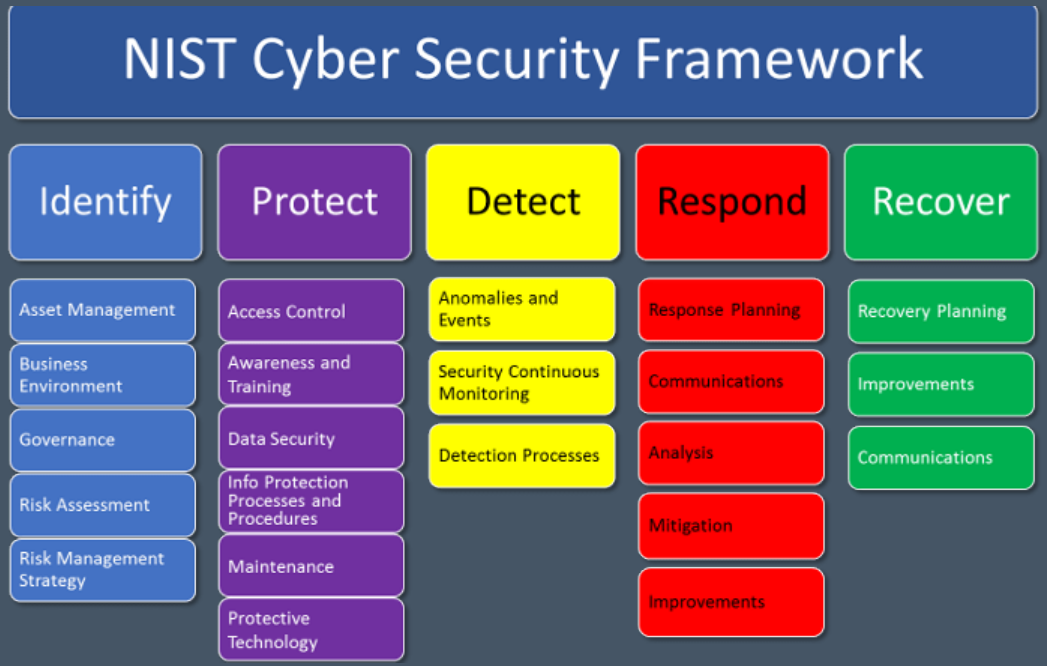


NIST: Cyber Security Framework

- Developed in 2014
- Use Business Drivers to guide Cyber Activities
- Cyber Activities & Outcomes
- Structure for Cyber Security practices

SOC & CSF

- Give structure to your security operations
- Multiple responsible teams
- Not a cycle; all functions in constant operation
- Guidelines for organisation maturity



Challenges

What metrics should we use?

How do we report?

Do we need more people?

When will we know we've been breached?

Do we need more technology?

What are our processes?

03

Discussion

Identify

Asset Management

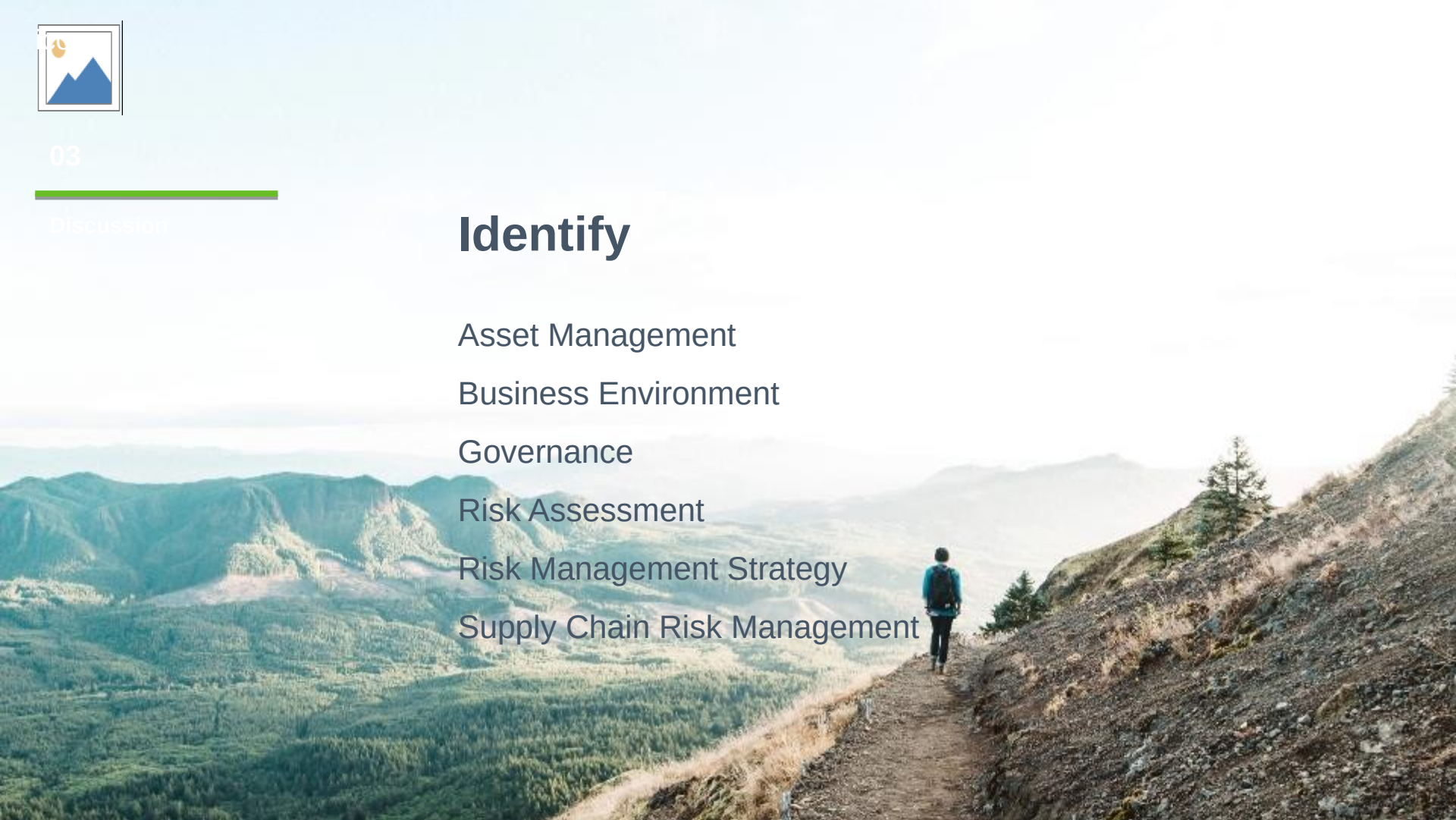
Business Environment

Governance

Risk Assessment

Risk Management Strategy

Supply Chain Risk Management



Asset Management

Physical Inventory

Software Inventory

Data Flows

Prioritisation

External Systems

Roles & Responsibilities

Business Environment

Industry Criticality

Supply Chain

Organisational Objectives & Mission

Resilience Requirements

Dependencies & Critical Functions

Governance

Policy

Legal & Regulation

Governance & Risk Management

Role & Responsibilities

Risk Assessment

Vulnerabilities

Threat Intelligence

Threats

Business Impacts

Risk Response

Risk Likelihood

Risk Management

Business Environment
Tolerance

Processes

Risk Tolerance

Supply Chain

Identify Supply

Response & Recovery Planning

Review Contracts

Prioritise Chain

Routinely Assess

04

Discussion

Protect

Identity & Access Control

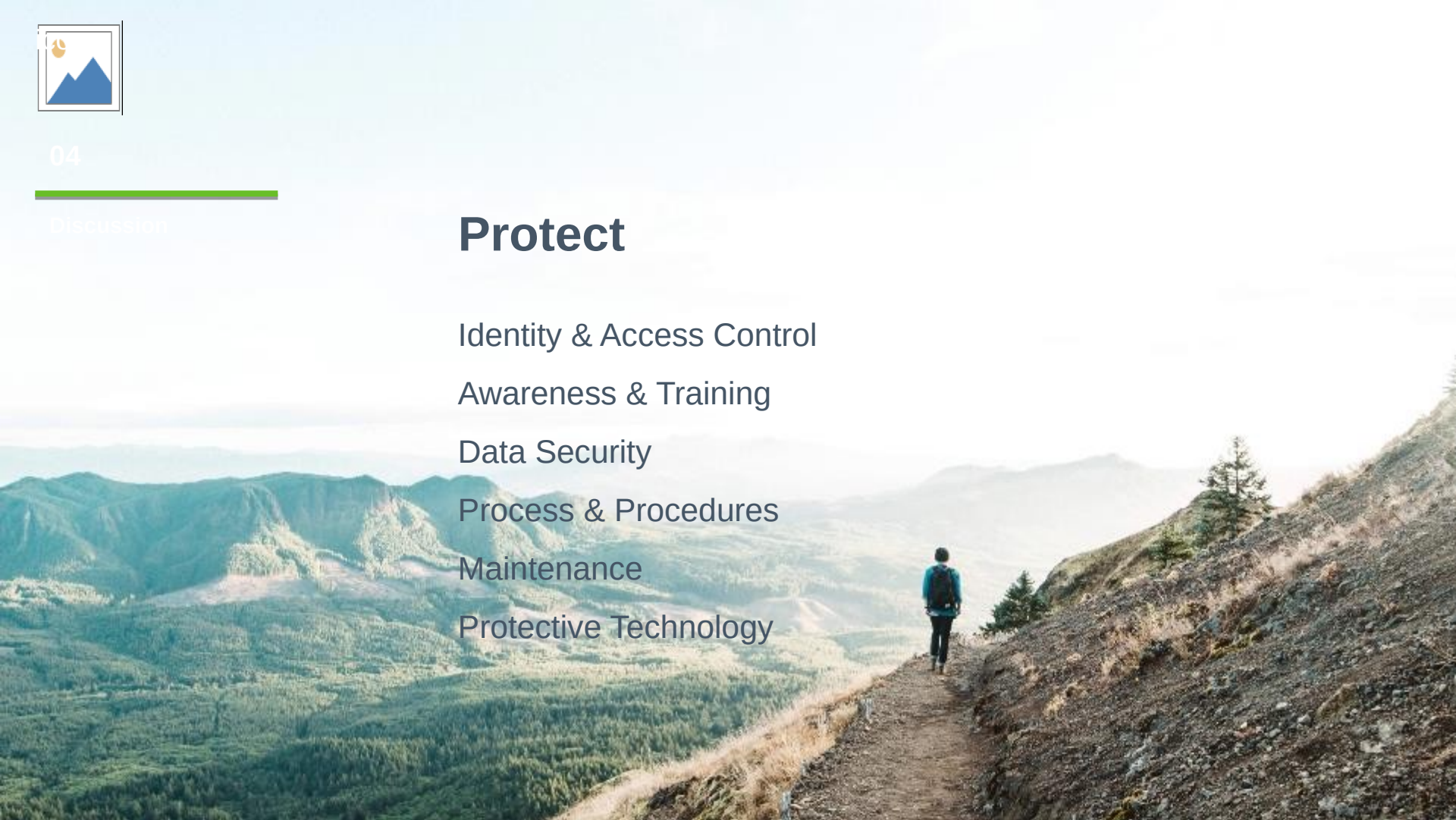
Awareness & Training

Data Security

Process & Procedures

Maintenance

Protective Technology



Access Controls

Identity Mapping

Physical Access

Credential Management

Remote Access

Network Segmentation

Least Privilege Management

Awareness & Training

User Training

Privilege Users

Roles & Responsibilities

Third-Parties

Senior Executives

Data Security

Segregated Development Environment

Capacity Management

Asset Management

Encryption at Rest

Encryption in transit

Data Loss Prevention

Processes & Procedures

- Development Life Cycle
- Change Control Processes
- Regular Backups
- Physical Operating Environment
- Data Destruction
- Shared Technology Responsibility
- Response & Recovery Plan Testing
- HR Integration
- **Vulnerability Management Plan**

Maintenance

- **Maintain assets**
- Remote Maintenance auditing

Protective Technology

- Audit Logging
- **Removable Media**
- Principle of Least Functionality
- Resilience Mechanisms

05

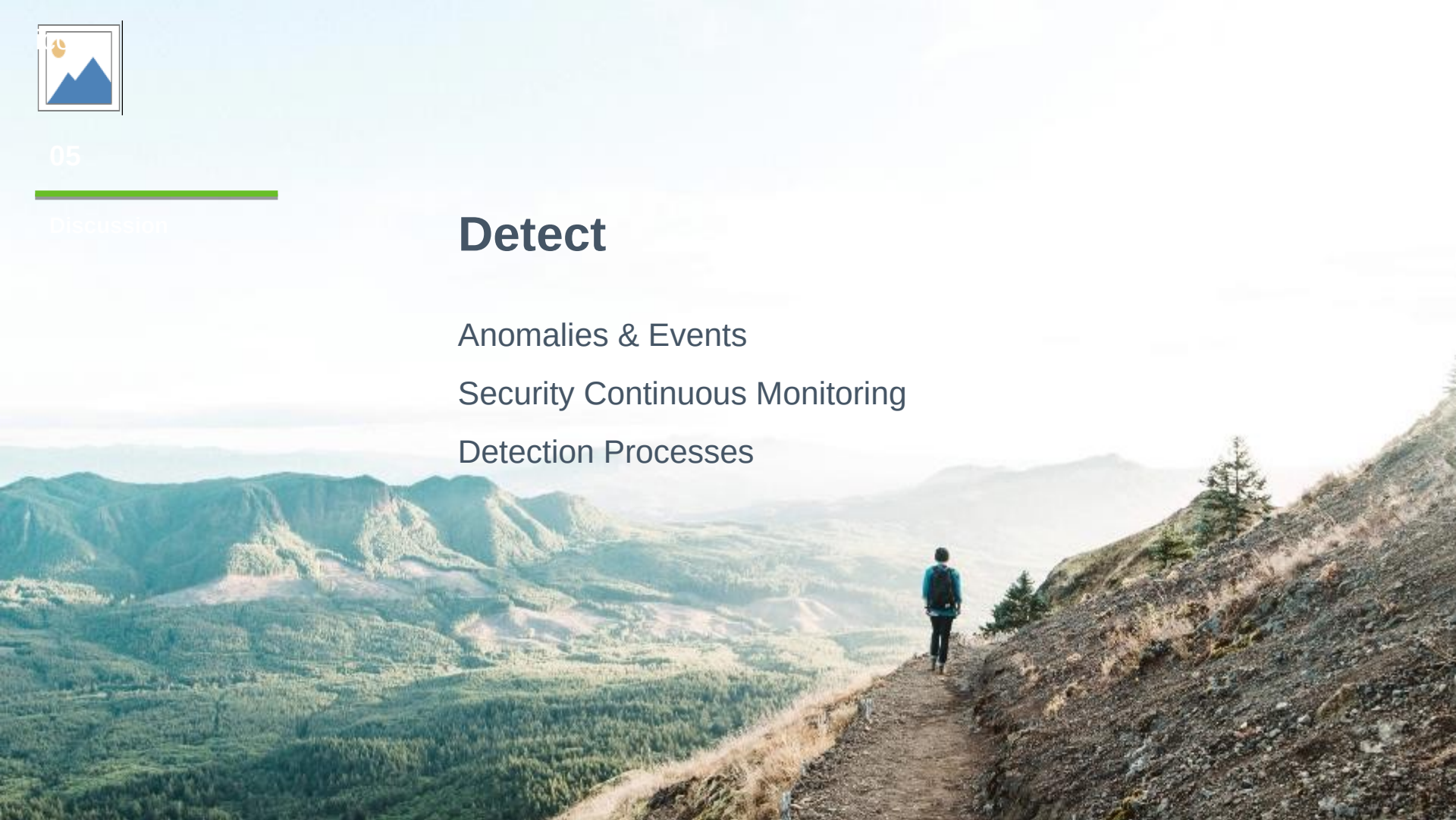
Discussion

Detect

Anomalies & Events

Security Continuous Monitoring

Detection Processes



Anomalies & Events

Baseline Network Operations

Collection of Event Data

Incident Thresholds

Analyse Events

Determination of Impact

Continuous Monitoring

Network & Physical

Personnel Activity

Code: Malicious & Unauthorised

Service Providers

Vulnerability Scanning

Unauthorised Identities

Process & Procedures

Roles & Responsibilities

Information Communication

Verify Detection Mechanisms

Legal Requirements

Continuous Improvement

06

Discussion

Respond

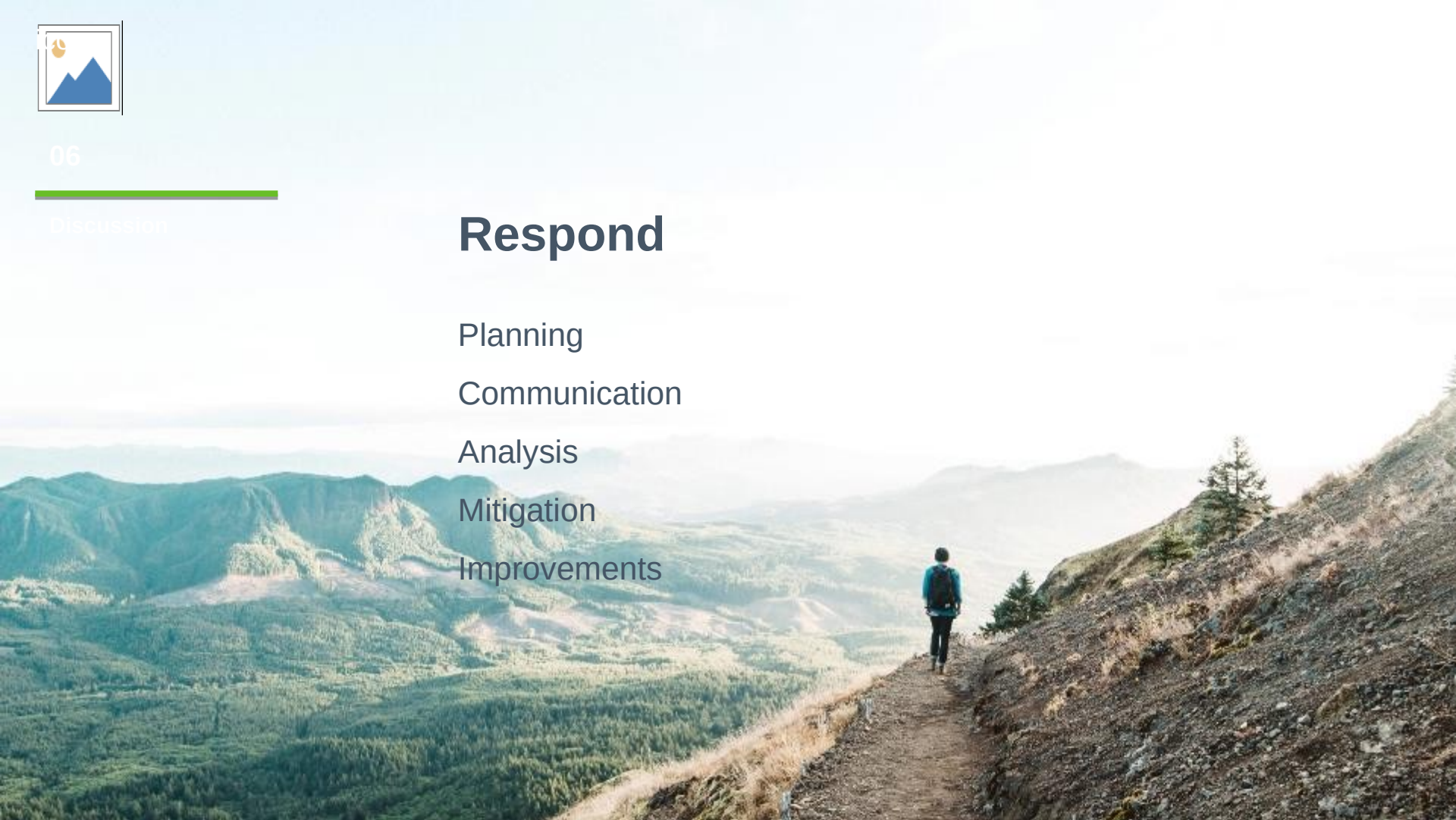
Planning

Communication

Analysis

Mitigation

Improvements



Planning

- **Execution of Response Planning**

Communication

Order of Operations

Stakeholder Coordination

Information Sharing

Reporting Criteria

Analysis

Forensics

Notification
Investigation

Incident Impact

Incident Categorisation

Vulnerability Assessment

Improvements

- Lessons Learnt Analysis

- **Updated Response Strategies**

07

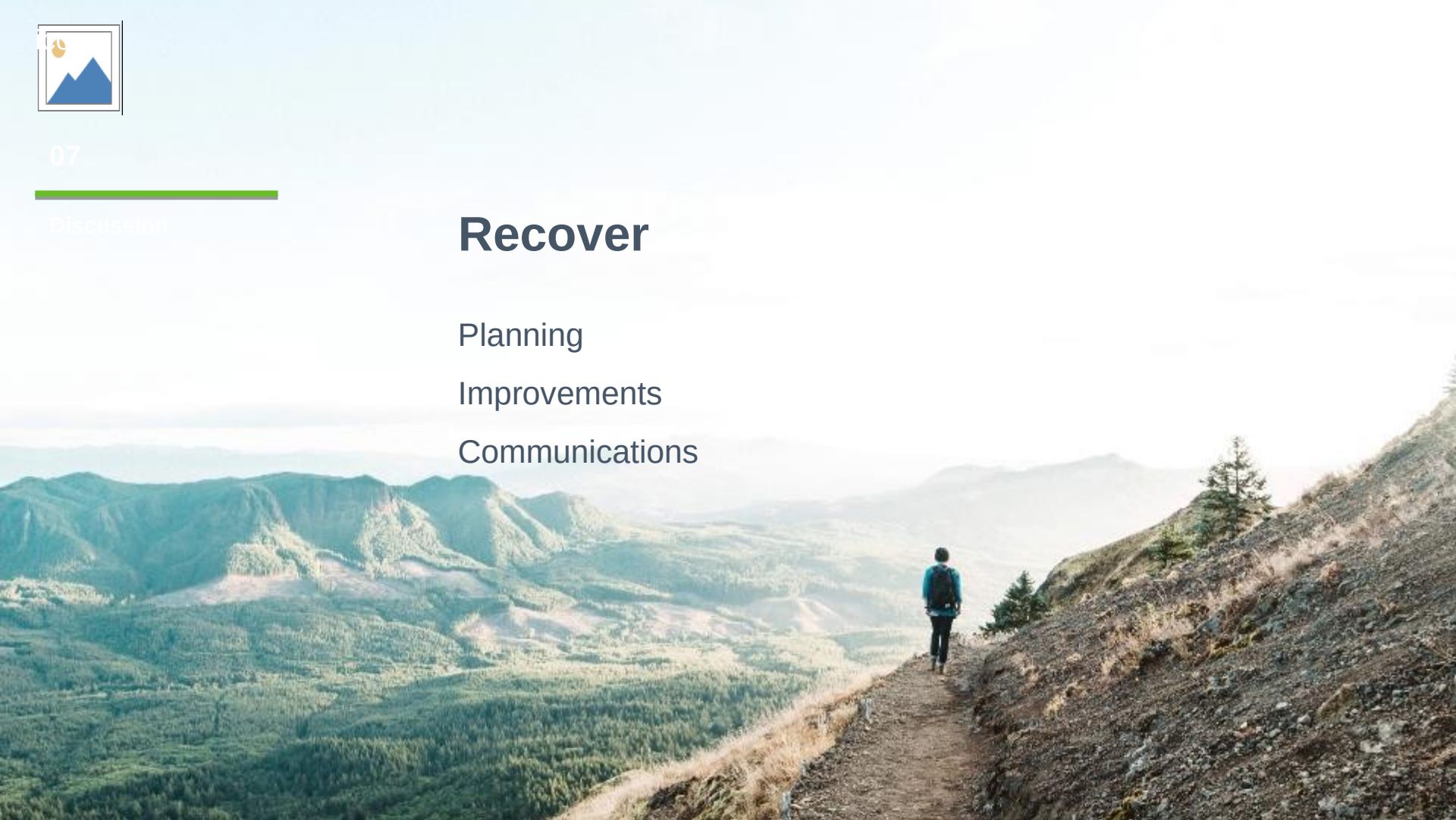
Discussion

Recover

Planning

Improvements

Communications



Planning

- Recovery Plan Execution
  - **Mean-Time-to-Repair**

Improvements

accelerate your ambition

- Lessons Learnt Analysis
- **Update Strategies**

Communications

accelerate your ambition

- Public Relations
- Reputation Reparation
- **Internal & External Stakeholders**

Lab

Splunk

Splunk Setup

accelerate your ambition

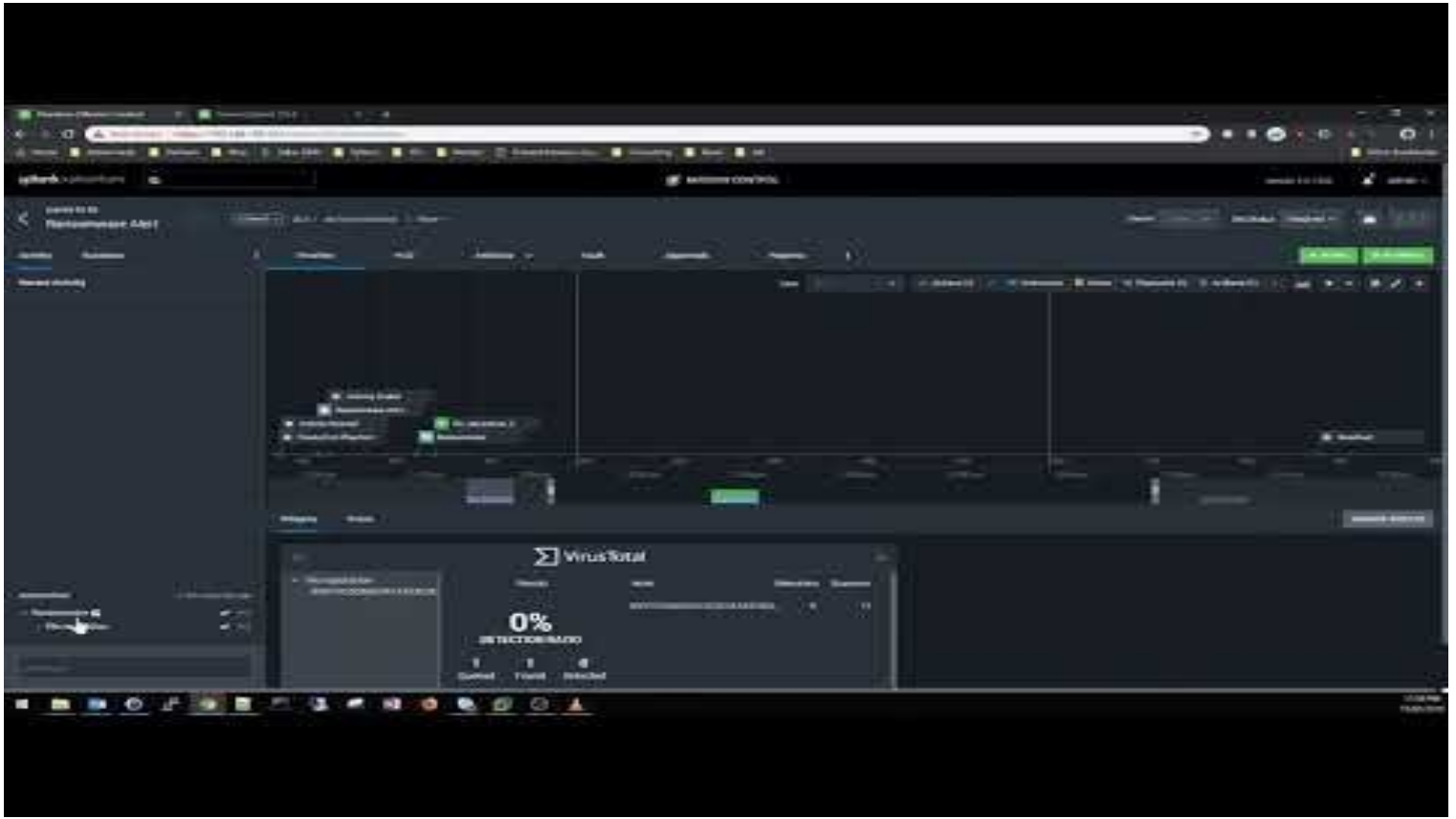
1. Install
2. Ingest data from your local machine
3. See if you can start making some alerts which map to elements of the framework
4. See if you can build a report to help identify and detect more sophisticated attacks

Optional: Phantom

accelerate your ambition

1. Allows automation and orchestration
2. Download and use the free licence
3. See if you can automate some responses to alerts in Splunk.
4. Report on mean-time-to:
    1. Detect
    2. Respond
    3. Remediate
    4. Recover

Splunk & Phantom



Credit: Deven Amode, Dimension Data Security Engineer


Thank you
Questions?