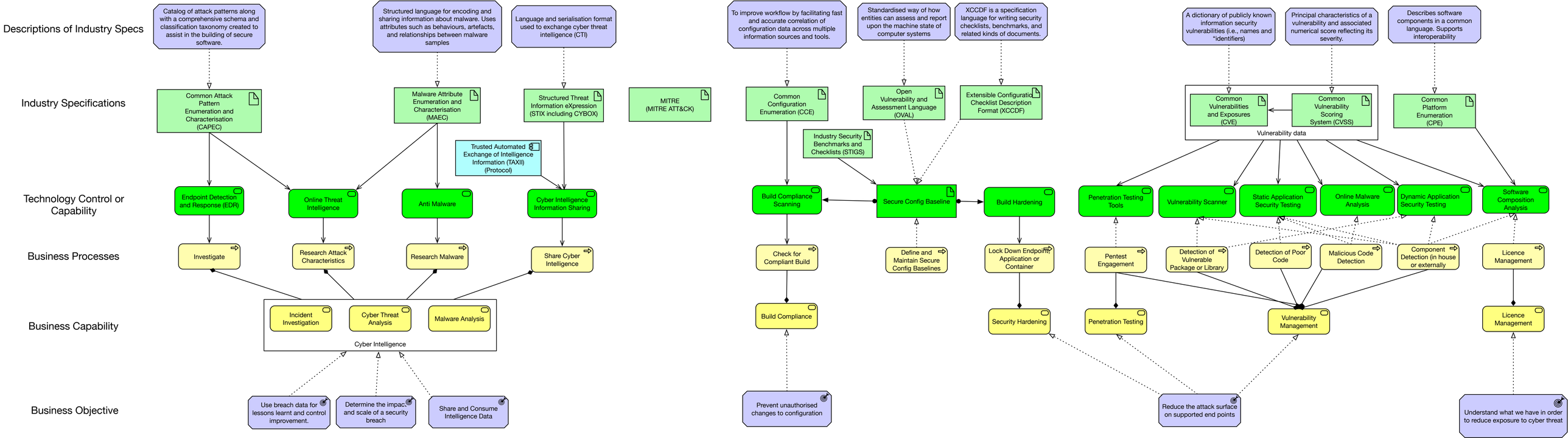
Descriptions of Industry Specs
Industry Specifications
Technology Control or Capability
Business Processes
Business Capability
Business Objective
Catalog of attack patterns along with a comprehensive schema and classification taxonomy created to assist in the building of secure software.
Structured language for encoding and sharing information about malware. Uses attributes such as behaviours, artefacts, and relationships between malware samples
Language and serialisation format used to exchange cyber threat intelligence (CTI)
To improve workflow by facilitating fast and accurate correlation of configuration data across multiple information sources and tools.
Standardised way of how entities can assess and report upon the machine state of computer systems
XCCDF is a specification language for writing security checklists, benchmarks, and related kinds of documents.
A dictionary of publicly known information security vulnerabilities (i.e., names and "identifiers)
Principal characteristics of a vulnerability and associated numerical score reflecting its severity.
Describes software components in a common language. Supports interoperability
Common Attack Pattern Enumeration and Characterisation (CAPEC)
Malware Attribute Enumeration and Characterisation (MAEC)
Structured Threat Information eXpression (STIX including CYBOX)
MITRE (MITRE ATT&CK)
Trusted Automated Exchange of Intelligence Information (TAXII) (Protocol)
Common Configuration Enumeration (CCE)
Open Vulnerability and Assessment Language (OVAL)
Extensible Configuratio Checklist Description Format (XCCDF)
Industry Security Benchmarks and Checklists (STIGS)
Common Vulnerabilities and Exposures (CVE)
Common Vulnerability Scoring System (CVSS)
Vulnerability data
Common Platform Enumeration (CPE)
Endpoint Detection and Response (EDR)
Online Threat Intelligence
Anti Malware
Cyber Intelligence Information Sharing
Build Compliance Scanning
Secure Config Baseline
Build Hardening
Penetration Testing Tools
Vulnerability Scanner
Static Application Security Testing
Online Malware Analysis
Dynamic Application Security Testing
Software Composition Analysis
Investigate
Research Attack Characteristics
Research Malware
Share Cyber Intelligence
Check for Compliant Build
Define and Maintain Secure Config Baselines
Lock Down Endpoint Application or Container
Pentest Engagement
Detection of Vulnerable Package or Library
Detection of Poor Code
Malicious Code Detection
Component Detection (in house or externally
Licence Management
Incident Investigation
Cyber Threat Analysis
Malware Analysis
Cyber Intelligence
Build Compliance
Security Hardening
Penetration Testing
Vulnerability Management
Licence Management
Use breach data for lessons learnt and control improvement.
Determine the impact and scale of a security breach
Share and Consume Intelligence Data
Prevent unauthorised changes to configuration
Reduce the attack surface on supported end points
Understand what we have in order to reduce exposure to cyber threat