satisnet
streamlining security management

satisnet
CSIV service

# Continuous Security Investment Validation (CSIV) Service

Satisnet provide an advanced CSIV Service which unlocks insights into your cyber security spending against security frameworks such as NIST and the Cyber Defense Matrix.

The CSIV Service enables you to identify any areas of underinvestment and overlap in your security tooling, and gives the organisation a strategic, ongoing roadmap. Your security tooling will be predominantly based on the Microsoft Security stack, so this roadmap will keep pace with Microsoft product developments and new platforms, as well as other security tooling being utilised, e.g. firewalls, ransomware protection, etc.

## Microsoft Defender

Defender for Endpoint
Defender for Office 365
Defender for Identity
Defender for Cloud Apps
Defender Vulnerability Management
Azure Active Directory Identity Protection
Data Loss Prevention
App Governance
Defender External Attack Surface Management
Defender Threat Intelligence

## Microsoft Defender for Cloud

**Cloud-Native Application Protection Platform (CNAPP)**

Development Security Operations (DevSecOps)
Cloud Security Posture Management (CSPM)
Cloud Workload Protection Platform (CWPP)

## Microsoft Sentinel

Security Information and Event Management (SIEM)
Security Orchestration, Automation and Response (SOAR)

**Other Security Tooling**

The CSIV Service then maps the identified gaps, underinvestment, and overlaps from the above capability against threat actors in your company sector, ensuring your organisation is protected from them.

## Secret Sauce: Capability Description Model

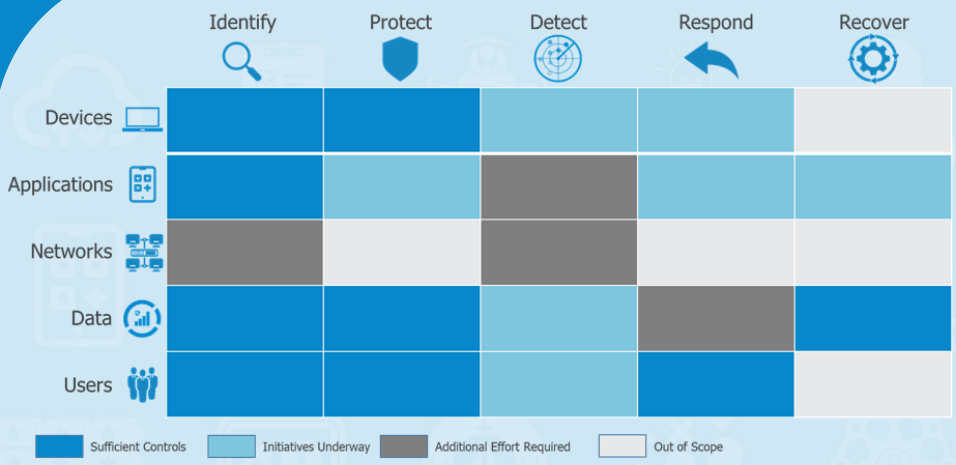
The Capability Description Model explains, at a micro level, what products do against how threat actors operate. Essentially, it is a living catalogue of security products and the threats they address, referred to as the Capability Exchange – kept up to date as Microsoft and other cyber security tools advance and add new features.

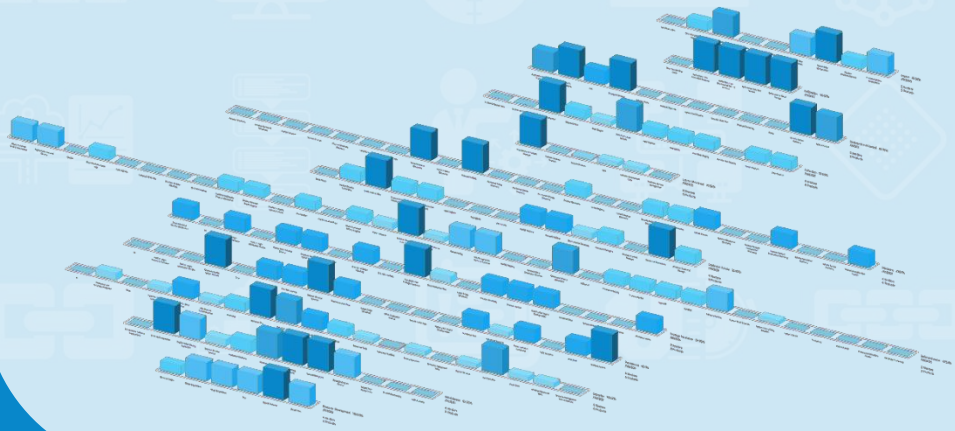
**www.satisnet.co.uk**
**+44 (0) 1582 369330**

satisnet
streamlining security management

In summary, using MITRE ATT&CK as an example framework, you will know how well you are covered for the below, and how well your stack performs against specific threat actors.

- **Reconnaissance** (42 techniques)
- **Resource Development** (38 techniques)
- **Initial Access** (19 techniques)
- **Execution** (33 techniques)
- **Persistence** (108 techniques)
- **Privilege Escalation** (95 techniques)
- **Defense Evasion** (170 techniques)
- **Credential Access** (58 techniques)
- **Discovery** (43 techniques)
- **Lateral Movement** (21 techniques)
- **Collection** (37 techniques)
- **Command and Control** (38 techniques)
- **Exfiltration** (17 techniques)
- **Impact** (26 techniques)



### Incident Integration and Reporting

The CSIV Service provides the insight to understand how your security investment is performing against past incidents and simulated engagements for control and strategy validation.

### C-Level Reporting

The CSIV Service fuses high-fidelity information across multiple domains, including contractual, financial, and security efficacy, to highlight key areas to address for management.

### Scalable and Advanced Coverage

Visualise your protection coverage aligned to MITRE Enterprise ATT&CK techniques utilised by threat groups attributed to your organisational sector.

## Key Questions The CSIV Service Answers

- Which products are overlapping in terms of the security capabilities (split by domain)?
- Which areas of MITRE do we completely lack product coverage in, in terms of being able to block tactics, techniques, and procedures (TTPs)?
  - Count of TTPs we have either detection or protection against
  - Count of TTPs we don't have any detection or protection against
- Which products are due to expire in the next twelve months, and if we choose not to renew, which existing capabilities or products can cover the potential TTP gaps that arise?

**www.satisnet.co.uk**
**+44 (0) 1582 369330**

satisnet
streamlining security management