4

المركـز الوطنـي للأمـن السيبرانــي
National Cyber Security Center

Critical Infrastructure Cyber Security Controls

CICSC THREAT ANNEX

December 2024

CICSC & THREAT MITIGATION

Informed by The Mitre Corporation’s analysis of the tactics, technique and procedures (TTPs) typically involved in cyber attacks, this annex is designed to highlight the practical benefits of applying the Critical Infrastructure Cyber Security Controls (CICSC). This is not a prescriptive guide to control implementation, but is intended to show how the combined application of CICSC controls can help to reduce the risk posed by TTPs involved in a range of common threats: defacement, denial of service, ransomware, espionage, and destructive attacks.

The TTPs used by threat actors change over time, however, and so the controls included here should be seen as illustrative, not exhaustive.

1.1 Threat Actors

The controls within CICSC aim to counter cyber threats, minimise disruption, and enhance resilience against three categories of threat actors:

Activists
Serving the cause

Driven by political causes or other ideological agendas, activists (also referred to as hacktivists) often make exaggerated claims alongside relatively low-level Distributed Denial of Service or defacement activity. State-sponsored groups are also known to leverage false hacktivist personas to conduct disruptive or destructive activity.

Criminals
Serving themselves

Financially motivated criminals encompass a broad range of cyber threats. Ransomware and extortion groups pose a serious threat to organisations across all sectors and geographies. Operators consistently explore new infection methods and use 'affiliate' structures. Some criminal groups, especially those with significant resources, have been observed leveraging capabilities such as zero-day vulnerabilities, however, TTPs such as the use of macros, known exploits, phishing, and compromised infrastructure remain most common.

State Actors
Serving the nation

At a nation-state level, geopolitically, security and economically motivated threat groups maintain a focus on conducting espionage and disruptive operations. Representing the most sophisticated threat actors, these groups will use a combination of simple tools for deniability as well as custom tooling.

While their capabilities of these threat actors range from basic to advanced, the tools available to them will vary and there are some overlaps. For example, some techniques used by hacktivists require more than the implementation of Level 1 controls to help manage the risk effectively.

1.2 Common Mitre ATT@CK Techniques

The MITRE ATT&CK framework describes the TTPs employed by cyber threat actors when conducting offensive cyber operations. Mitre's framework recognises that adversaries must operate within the constraints imposed by the target technology, usually employing a small number of known techniques rather than expending resources to develop novel ones.

Analysis of TTP data from its research since 2022 shows that the tactics most routinely observed in use by threat actors in the Middle East are:

- Resource Development
- Defence Evasion
- Command and Control
- Execution tactics

These trends, as illustrated in attack tactics shown in the graph below, relate primarily to state-sponsored threat actors and high-end criminal actors.

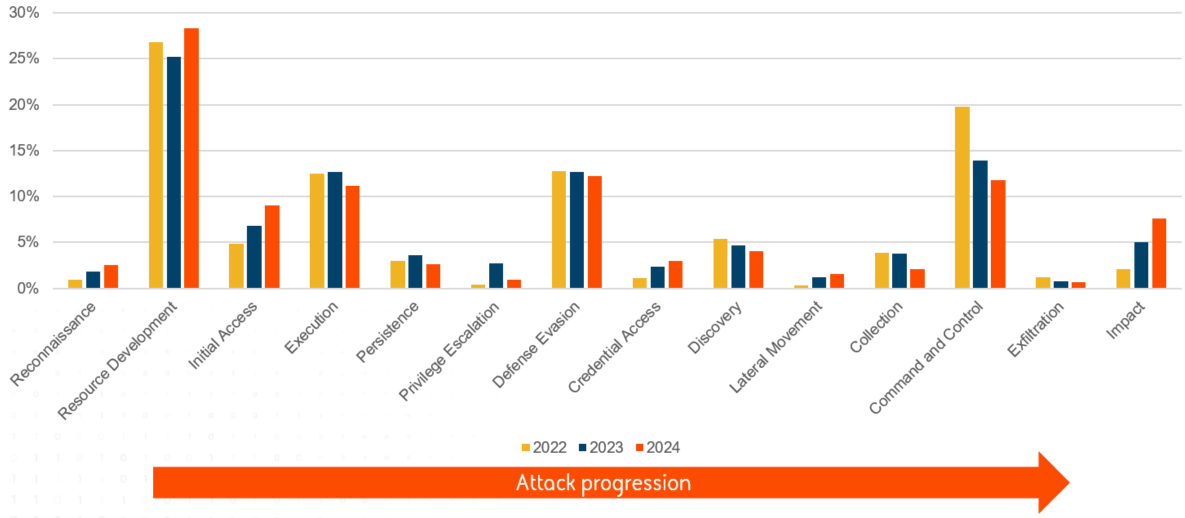

Figure 1: Distribution of tactics observed, 2022-2024
(Source: BAE Systems Digital Intelligence)

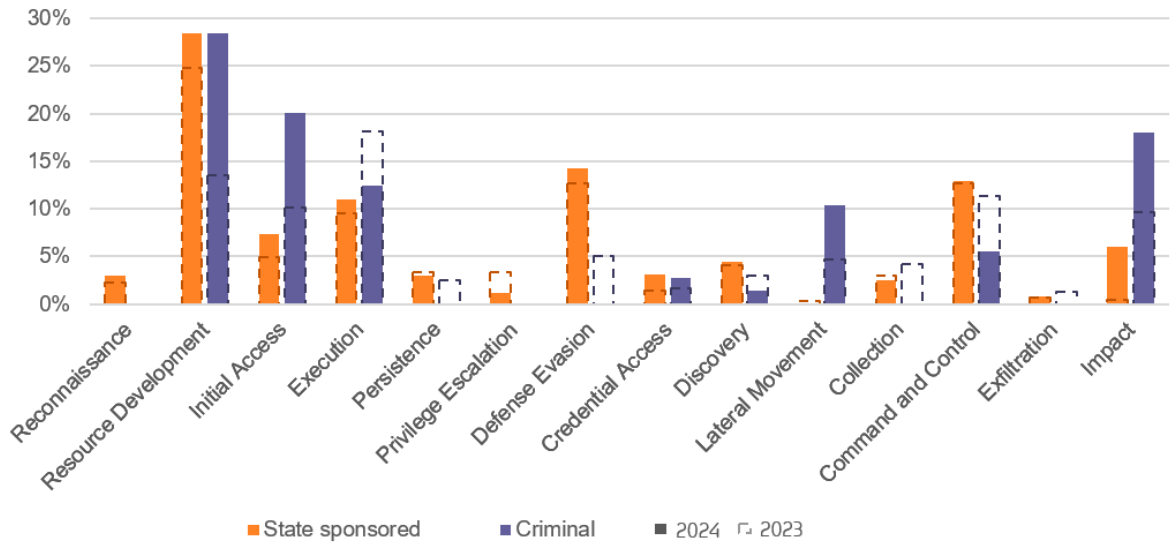

Figure 2: Distribution of tactics between state sponsored and criminal actors 2023-2024
(Source: BAE Systems Digital Intelligence)

Throughout 2024, an increase in ransomware and data extortion campaigns by criminal groups continued despite multiple high-profile international indictments and arrests of affiliated individuals in 2023, as well as disruption some of the major ransomware groups.[1]

1.3 Control Value

Section 1.1 introduced three types of threat actor, whose capabilities the controls within CICSC help to mitigate. The next section demonstrates the range of controls required to help counter attacks commonly associated with each of these threat actors.

This is not an exhaustive list of high-value or priority controls, but serves to show how - when combined - the controls within CICSC can help to protect Jordan's critical assets from a range of damaging attack techniques.

1.3.1 Activist Threats – Defacement & Denial of Service Attacks

The table below displays common TTPs exhibited by prominent ideologically and financially motivated hacktivist groups. These groups have been observed targeting entities in the Middle East in relation to ongoing conflicts and targeting a wide range of sectors, among dozens of other groups operating in a similar capacity.

The hacktivist threat landscape is often blurry given the broad range of issues which these types of groups respond to, as well as each group's individual level of capability or credibility. Further

[1] For example, the international action to disrupt the Lockbit ransomware operation.

complicating matters, it is common for hacktivist actors to claim responsibility for successful attacks or intrusions which they have not done, or were not successful in doing. Additionally, state-sponsored groups have also been observed operating under false hacktivist personas to conduct disruptive or destructive activity in order to avoid repercussions and maintain anonymity.

Since 2020, various hacktivist groups targeting critical infrastructure across Middle Eastern countries have been observed. This activity mostly comprised of website defacement, data leaks and Distributed Denial of Service (DDoS) attacks to varying degrees of success. Representative of relatively low-level threat actor capability, the controls in the table below provide appropriate mitigation to help protect against techniques commonly used to conduct defacement and denial of service attacks.

Impact T1498 Denial Of Service			
CICSC Control Identifier	CICSC Control Name	MITRE Framework Technique	MITRE Attack Framework Title
AC-3	Access Enforcement	T1498	Endpoint/Network Denial of Service
AC-4	Information Flow Enforcement	T1498	Endpoint/Network Denial of Service
CA-7	Continuous Monitoring	T1498	Endpoint/Network Denial of Service
CM-6	Configuration Settings	T1498	Endpoint/Network Denial of Service
CM-7	Least Functionality	T1498	Endpoint/Network Denial of Service
SC-7	Boundary Protection	T1498	Endpoint/Network Denial of Service
SI-10	Information Input Validation	T1498	Endpoint/Network Denial of Service
SI-15	Information Output Filtering	T1498	Endpoint/Network Denial of Service
SI-4	System Monitoring	T1498	Endpoint Denial of Service
SI-15	Information Output Filtering	T1498	Endpoint/Network Denial of Service
SI-4	System Monitoring	T1498	Endpoint Denial of Service

Impact T1491 Defacement			
CICSC Control Identifier	CICSC Control Name	MITRE Framework Technique	MITRE Attack Framework Title
AC-6	Least Privilege	T1491	Defacement
CM-2	Baseline Configuration	T1491	Defacement
CP-10	System Recovery and Reconstitution	T1491	Defacement
CP-2	Contingency Plan	T1491	Defacement
CP-7	Alternate Processing Site	T1491	Defacement
CP-9	System Backup	T1491	Defacement
SI-3	Malicious Code Protection	T1491	Defacement
SI-4	System Monitoring	T1491	Defacement
SI-7	Software, Firmware, and Information Integrity	T1491	Defacement

Execution T1059 & T1203			
CICSC Control Identifier	CICSC Control Name	MITRE Framework Technique	MITRE Attack Framework Title
AC-17	Remote Access	T1059	Command and Scripting Interpreter
AC-2	Account Management	T1059	Command and Scripting Interpreter
AC-3	Access Enforcement	T1059	Command and Scripting Interpreter
AC-4	Information Flow Enforcement	T1203	Exploitation for Client Execution
AC-5	Separation of Duties	T1059	Command and Scripting Interpreter
AC-6	Least Privilege	T1059 T1203	Command and Scripting Interpreter, Exploitation for Client Execution

Execution T1059 & T1203			
CICSC Control Identifier	CICSC Control Name	MITRE Framework Technique	MITRE Attack Framework Title
CA-7	Continues Monitoring	T1059 T1203	Command and Scripting Interpreter, Exploitation for Client Execution
CA-8	Penetration Testing	T1059	Command and Scripting Interpreter
CM-11	User-installed Software	T1059	Endpoint Denial of Service
CM-11	User-installed Software	T1059	Command and Scripting Interpreter
CM-2	Baseline Configuration	T1059	Command and Scripting Interpreter
CM-5	Access Restrictions for Change	T1059	Command and Scripting Interpreter
CM-6	Configuration Settings	T1059	Command and Scripting Interpreter
CM-7	Least Functionality	T1059	Command and Scripting Interpreter
CM-8	System Component Inventory	T1059 T1203	Command and Scripting Interpreter, Exploitation for Client Execution
IA-2	Identification and Authentication (organizational Users)	T1059	Command and Scripting Interpreter
IA-8	Identification and Authentication (non-organizational Users)	T1059	Command and Scripting Interpreter
IA-9	Service Identification and Authentication	T1059	Command and Scripting Interpreter
RA-5	Vulnerability Monitoring and Scanning	T1059	Command and Scripting Interpreter
SC-18	Mobile Code	T1059	Command and Scripting Interpreter
SC-18	Mobile Code	T1203	Exploitation for Client Execution
SC-2	Separation of System and User Functionality	T1203	Exploitation for Client Execution
SC-29	Heterogeneity	T1203	Exploitation for Client Execution
SC-3	Security Function Isolation	T1203	Exploitation for Client Execution

Execution T1059 & T1203			
CICSC Control Identifier	CICSC Control Name	MITRE Framework Technique	MITRE Attack Framework Title
SC-30	Concealment and Misdirection	T1203	Exploitation for Client Execution
SC-39	Process Isolation	T1203	Exploitation for Client Execution
SC-44	Detonation Chambers	T1203	Exploitation for Client Execution
SC-7	Boundary Protection	T1203	Exploitation for Client Execution
SI-10	Information Input Validation	T1059	Command and Scripting Interpreter
SI-16	Memory Protection	T1059	Command and Scripting Interpreter
SI-2	Flaw Remediation	T1059	Command and Scripting Interpreter
SI-3	Malicious Code Protection	T1059 T1203	Command and Scripting Interpreter, Exploitation for Client Execution
SI-4	System Monitoring	T1059 T1203	Command and Scripting Interpreter, Exploitation for Client Execution
SI-7	Software, Firmware, and Information Integrity	T1059 T1203	Command and Scripting Interpreter, Exploitation for Client Execution

1.3.2 Criminal Threats – Ransomware Attacks

While the cyber threats posed by criminals vary, the table below displays common TTPs exhibited by one of the most prolific and disruptive techniques employed by financially motivated threat actors: ransomware. This threat has grown significantly in recent years and has been used against numerous critical infrastructure organisations in the Middle East and around the world that depend on industrial control systems and operational technology.

Despite its success, with the appropriate controls in place the threats posed by ransomware can be mitigated. Representative of mid-level threat actor capability, the controls in the table below provide appropriate mitigation against techniques commonly used to enable ransomware attacks.

Defence Evasion T1027			
CICSC Control Identifier	CICSC Control Name	MITRE Framework Technique	MITRE Attack Framework Title
CM-2	Baseline Configuration	T1027	Obfuscated Files or Information
CM-6	Configuration Settings	T1027	Obfuscated Files or Information
SI-2	Flaw Remediation	T1027	Obfuscated Files or Information
SI-3	Malicious Code Protection	T1027	Obfuscated Files or Information
SI-4	System Monitoring	T1027	Obfuscated Files or Information
SI-7	Software, Firmware, and Information Integrity	T1027	Obfuscated Files or Information

Execution T1203			
CICSC Control Identifier	CICSC Control Name	MITRE Framework Technique	MITRE Attack Framework Title
AC-4	Information Flow Enforcement	T1203	Exploitation for Client Execution
AC-6	Least Privilege	T1203	Exploitation for Client Execution
CA-7	Continuous Monitoring	T1203	Exploitation for Client Execution
CM-8	System Component Inventory	T1203	Exploitation for Client Execution
SC-18	Mobile Code	T1203	Exploitation for Client Execution
SC-2	Separation of System and User Functionality	T1203	Exploitation for Client Execution
SC-29	Heterogeneity	T1203	Exploitation for Client Execution
SC-3	Security Function Isolation	T1203	Exploitation for Client Execution
SC-30	Concealment and Misdirection	T1203	Exploitation for Client Execution
SC-39	Process Isolation	T1203	Exploitation for Client Execution
SC-44	Detonation Chambers	T1203	Exploitation for Client Execution
SC-7	Boundary Protection	T1203	Exploitation for Client Execution

Execution T1203			
CICSC Control Identifier	CICSC Control Name	MITRE Framework Technique	MITRE Attack Framework Title
SI-3	Malicious Code Protection	T1203	Exploitation for Client Execution
SI-4	System Monitoring	T1203	Exploitation for Client Execution
SI-7	Software, Firmware, and Information Integrity	T1203	Exploitation for Client Execution

1.3.3 State Threats – Espionage & Destructive Attacks

State-sponsored threat actors have been routinely observed targeting critical infrastructure and government entities across the Middle East. Representative of high-level threat actor capability, the controls in the table below provide appropriate mitigation against common TTPs exhibited by state-sponsored threat actors active in the Middle East - and elsewhere - to conduct espionage and destructive attacks.

Initial Access T1566 & T1598 Spearphishing			
CICSC Control Identifier	CICSC Control Name	MITRE Framework Technique	MITRE Attack Framework Title
AC-4	Information Flow Enforcement	T1566.001	Spearphishing Attachment
AC-4	Information Flow Enforcement	T1598.002	Spearphishing Attachment
AC-4	Information Flow Enforcement	T1566.002	Spearphishing Link
AC-4	Information Flow Enforcement	T1598.003	Spearphishing Link
CA-7	Continuous Monitoring	T1566.001	Spearphishing Attachment
CA-7	Continuous Monitoring	T1598.002	Spearphishing Attachment
CA-7	Continuous Monitoring	T1566.002	Spearphishing Link
CA-7	Continuous Monitoring	T1598.003	Spearphishing Link
CM-2	Baseline Configuration	T1566.001	Spearphishing Attachment

Initial Access T1566 & T1598 Spearphishing			
CICSC Control Identifier	CICSC Control Name	MITRE Framework Technique	MITRE Attack Framework Title
CM-2	Baseline Configuration	T1598.002	Spearphishing Attachment
CM-2	Baseline Configuration	T1566.002	Spearphishing Link
CM-2	Baseline Configuration	T1598.003	Spearphishing Link
CM-6	Configuration Settings	T1566.001	Spearphishing Attachment
CM-6	Configuration Settings	T1598.002	Spearphishing Attachment
CM-6	Configuration Settings	T1566.002	Spearphishing Link
CM-6	Configuration Settings	T1598.003	Spearphishing Link
IA-9	Service Identification and Authentication	T1566.001	Spearphishing Attachment
IA-9	Service Identification and Authentication	T1598.002	Spearphishing Attachment
IA-9	Service Identification and Authentication	T1566.002	Spearphishing Link
IA-9	Service Identification and Authentication	T1598.003	Spearphishing Link
SC-20	Secure Name/address Resolution Service (authoritative Source)	T1566.001	Spearphishing Attachment
SC-20	Secure Name/address Resolution Service (authoritative Source)	T1598.002	Spearphishing Attachment
SC-20	Secure Name/address Resolution Service (authoritative Source)	T1566.002	Spearphishing Link
SC-20	Secure Name/address Resolution Service (authoritative Source)	T1598.003	Spearphishing Link
SC-44	Detonation Chambers	T1566.001	Spearphishing Attachment
SC-44	Detonation Chambers	T1598.002	Spearphishing Attachment
SC-44	Detonation Chambers	T1566.002	Spearphishing Link

Initial Access T1566 & T1598 Spearphishing			
CICSC Control Identifier	CICSC Control Name	MITRE Framework Technique	MITRE Attack Framework Title
SC-44	Detonation Chambers	T1598.003	Spearphishing Link
SC-7	Boundary Protection	T1566.001	Spearphishing Attachment
SC-7	Boundary Protection	T1598.002	Spearphishing Attachment
SC-7	Boundary Protection	T1566.002	Spearphishing Link
SC-7	Boundary Protection	T1598.003	Spearphishing Link
SI-2	Flaw Remediation	T1566.001	Spearphishing Attachment
SI-3	Malicious Code Protection	T1566.001	Spearphishing Attachment
SI-3	Malicious Code Protection	T1598.002	Spearphishing Attachment
SI-3	Malicious Code Protection	T1566.002	Spearphishing Link
SI-3	Malicious Code Protection	T1598.003	Spearphishing Link
SI-4	System Monitoring	T1566.001	Spearphishing Attachment
SI-4	System Monitoring	T1598.002	Spearphishing Attachment
SI-4	System Monitoring	T1566.002	Spearphishing Link
SI-4	System Monitoring	T1598.003	Spearphishing Link
SI-8	Spam Protection	T1566.001	Spearphishing Attachment
SI-8	Spam Protection	T1598.002	Spearphishing Attachment
SI-8	Spam Protection	T1566.002	Spearphishing Link
SI-8	Spam Protection	T1598.003	Spearphishing Link

Defence Evasion T1562 Impair Defences			
CICSC Control Identifier	CICSC Control Name	MITRE Framework Technique	MITRE Attack Framework Title
AC-2	Account Management	T1562	Impair Defences
AC-3	Access Enforcement	T1562	Impair Defences
AC-5	Separation of Duties	T1562	Impair Defences
AC-6	Least Privilege	T1562	Impair Defences
CA-7	Continuous Monitoring	T1562	Impair Defences
CA-8	Penetration Testing	T1562	Impair Defences
CM-2	Baseline Configuration	T1562	Impair Defences
CM-5	Access Restrictions for Change	T1562	Impair Defences
CM-6	Configuration Settings	T1562	Impair Defences
CM-7	Least Functionality	T1562	Impair Defences
IA-2	Identification and Authentication (organizational Users)	T1562	Impair Defences
IA-4	Identifier Management	T1562	Impair Defences
RA-5	Vulnerability Monitoring and Scanning	T1562	Impair Defences
SI-3	Malicious Code Protection	T1562	Impair Defences
SI-4	System Monitoring	T1562	Impair Defences
SI-7	Software, Firmware, and Information Integrity	T1562	Impair Defences

Credential Access T1056 Capture Input			
CICSC Control Identifier	CICSC Control Name	MITRE Framework Technique	MITRE Attack Framework Title
AC-2	Account Management	T1056.003	Web Portal Capture
AC-3	Access Enforcement	T1056.003	Web Portal Capture
AC-5	Separation of Duties	T1056.003	Web Portal Capture
AC-6	Least Privilege	T1056.003	Web Portal Capture
CA-7	Continuous Monitoring	T1056.002	GUI Input Capture
CM-5	Access Restrictions for Change	T1056.003	Web Portal Capture
CM-6	Configuration Settings	T1056.003	Web Portal Capture
IA-2	Identification and Authentication (organizational Users)	T1056.003	Web Portal Capture
SI-3	Malicious Code Protection	T1056.002	GUI Input Capture
SI-4	System Monitoring	T1056.002	GUI Input Capture
SI-7	Software, Firmware, and Information Integrity	T1056.002	GUI Input Capture

Credential Access T1110 Password Spraying			
CICSC Control Identifier	CICSC Control Name	MITRE Framework Technique	MITRE Attack Framework Title
AC-2	Account Management	T1110.003	Password Spraying
AC-20	Use of External Systems	T1110.003	Password Spraying
AC-3	Access Enforcement	T1110.003	Password Spraying
AC-5	Separation of Duties	T1110.003	Password Spraying
AC-6	Least Privilege	T1110.003	Password Spraying

Credential Access T1110 Password Spraying			
CICSC Control Identifier	CICSC Control Name	MITRE Framework Technique	MITRE Attack Framework Title
AC-7	Unsuccessful Logon Attempts	T1110.003	Password Spraying
CA-7	Continuous Monitoring	T1110.003	Password Spraying
CM-2	Baseline Configuration	T1110.003	Password Spraying
CM-6	Configuration Settings	T1110.003	Password Spraying
IA-11	Re-authentication	T1110.003	Password Spraying
IA-2	Identification and Authentication (organizational Users)	T1110.003	Password Spraying
IA-4	Identifier Management	T1110.003	Password Spraying
IA-5	Authenticator Management	T1110.003	Password Spraying
SI-4	System Monitoring	T1110.003	Password Spraying

Exfiltration T1041 Data Exfiltration Over C2 Channel			
CICSC Control Identifier	CICSC Control Name	MITRE Framework Technique	MITRE Attack Framework Title
AC-16	Security and Privacy Attributes	T1041	Exfiltration Over C2 Channel
AC-2	Account Management	T1041	Exfiltration Over C2 Channel
AC-20	Use of External Systems	T1041	Exfiltration Over C2 Channel
AC-23	Data Mining Protection	T1041	Exfiltration Over C2 Channel
AC-3	Access Enforcement	T1041	Exfiltration Over C2 Channel
AC-4	Information Flow Enforcement	T1041	Exfiltration Over C2 Channel
AC-6	Least Privilege	T1041	Exfiltration Over C2 Channel

Exfiltration T1041 Data Exfiltration Over C2 Channel			
CICSC Control Identifier	CICSC Control Name	MITRE Framework Technique	MITRE Attack Framework Title
CA-3	Information Exchange	T1041	Exfiltration Over C2 Channel
CA-7	Continuous Monitoring	T1041	Exfiltration Over C2 Channel
SA-8	Security and Privacy Engineering Principles	T1041	Exfiltration Over C2 Channel
SA-9	External System Services	T1041	Exfiltration Over C2 Channel
SC-13	Cryptographic Protection	T1041	Exfiltration Over C2 Channel
SC-28	Protection of Information at Rest	T1041	Exfiltration Over C2 Channel
SC-31	Covert Channel Analysis	T1041	Exfiltration Over C2 Channel
SC-7	Boundary Protection	T1041	Exfiltration Over C2 Channel
SI-3	Malicious Code Protection	T1041	Exfiltration Over C2 Channel
SI-4	System Monitoring	T1041	Exfiltration Over C2 Channel
SR-4	Provenance	T1041	Exfiltration Over C2 Channel

Impact T1485 Data Destruction			
CICSC Control Identifier	CICSC Control Name	MITRE Framework Technique	MITRE Attack Framework Title
AC-16	Security and Privacy Attributes	T1041	Exfiltration Over C2 Channel
AC-6	Least Privilege	T1485	Data Destruction
CM-2	Baseline Configuration	T1485	Data Destruction
CP-10	System Recovery and Reconstitution	T1485	Data Destruction
CP-2	Contingency Plan	T1485	Data Destruction
CP-7	Alternate Processing Site	T1485	Data Destruction

Impact T1485 Data Destruction			
CICSC Control Identifier	CICSC Control Name	MITRE Framework Technique	MITRE Attack Framework Title
CP-9	System Backup	T1485	Data Destruction
SI-3	Malicious Code Protection	T1485	Data Destruction
SI-4	System Monitoring	T1485	Data Destruction
SI-7	Software, Firmware, and Information Integrity	T1485	Data Destruction

Impact T1561 Disk Wipe			
CICSC Control Identifier	CICSC Control Name	MITRE Framework Technique	MITRE Attack Framework Title
AC-3	Access Enforcement	T1561	Disk Wipe
AC-6	Least Privilege	T1561	Disk Wipe
CM-2	Baseline Configuration	T1561	Disk Wipe
CP-10	System Recovery and Reconstitution	T1561	Disk Wipe
CP-2	Contingency Plan	T1561	Disk Wipe
CP-7	Alternate Processing Site	T1561	Disk Wipe
CP-9	System Backup	T1561	Disk Wipe
SI-3	Malicious Code Protection	T1561	Disk Wipe
SI-4	System Monitoring	T1561	Disk Wipe
SI-7	Software, Firmware, and Information Integrity	T1561	Disk Wipe

المركـز الوطني للأمـن السيبرانـي
National Cyber Security Center