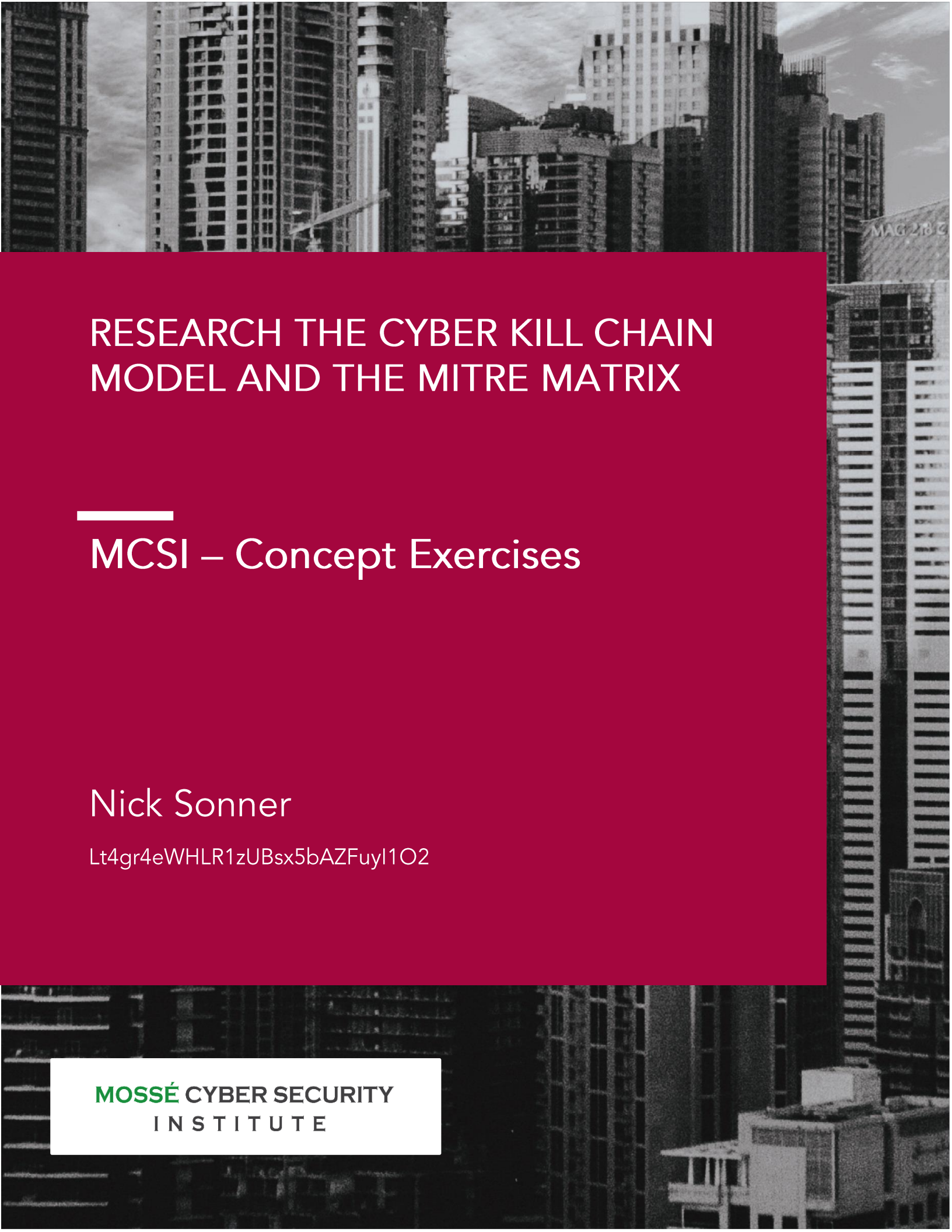




RESEARCH THE CYBER KILL CHAIN MODEL AND THE MITRE MATRIX

MCSI – Concept Exercises

Nick Sonner

Lt4gr4eWHLR1zUBsx5bAZFuyI1O2

MOSSÉ CYBER SECURITY
INSTITUTE

The Kill Chain and the MITRE Matrix

Executive Summary

Cyber Kill Chain

The Cyber Kill Chain is a framework, developed by Lockheed Martin, that tracks the various stages of a cyberattack that adversaries will typically need to complete in order for them to achieve mission success. This includes all requisite steps from the initial access to the exfiltration of sensitive data.

MITRE Matrix

The MITRE ATT&CK is a comprehensive matrix that describes the adversarial behaviour, tactics and techniques based on observations from real-world cyberattacks. The matrix is categorised by the Cyber Kill Chain and can assist in the classification, identification and mitigation of potential attacks on an organisation's network.

INITIAL ACCESS

Initial Access stage is whereby an adversary utilises various entry vectors to gain a foothold in a target network. E.g phishing and/or exploiting vulnerable public facing assets.

EXECUTION

The Execution stage can be defined as the stage in which techniques are employed to execute malicious, adversary-controlled code on a local or remote system.

PERSISTENCE

After an adversary has gained a foothold within a network or system, they will employ various techniques to retain access across restarts, credential resets and other unforeseen changes that may terminate their access.

PRIVILEGE ESCALATION

Privilege Escalation is the process where an adversary gains a higher level of permissions on a network or system. Various kill chain stages and techniques are contingent on an adversary having Administrator, SYSTEM or root level access.

DEFENSE EVASION

Defence Evasion is comprised of techniques used by adversaries to avoid detection during an operation. This can include uninstalling and/or disabling security software such as Anti-Virus software, abusing trusted processes and obfuscation/encryption techniques.

CREDENTIAL ACCESS

Credential Access describes techniques adversaries use to steal account credentials such as keylogging and credential dumping.

DISCOVERY

During the Discovery stage, an adversary will use various tools and techniques to obtain valuable knowledge about the system and network. This can provide an adversary with a wealth of usable information that can be subsequently used to inform them on further activities, targets and obstacles.

LATERAL MOVEMENT

Lateral Movement involves the activities where an adversary gains access and moves throughout a network. In order to achieve mission success, adversaries will often require them to pivot through multiple systems and environments.

COLLECTION

The Collection stage is where adversaries gather targeted information, data or IP relevant to their objectives. This can come in the form of files, document, emails, audio, video and user activity (keyboard input, microphone audio, web cam footage/screenshots).

EXFILTRATION

Exfiltration is where an adversary will extract stolen data from a compromised network, typically following the collection stage. This is commonly achieved by retrieving data through the adversaries Command and Control (C2) channel or by alternate methods (cloud storage services such as google drive or GitHub are two common methods).

COMMAND AND CONTROL

Command and Control (commonly abbreviated to C2) is the techniques used by adversaries to communicate and issue instructions to compromised machines within a target network.