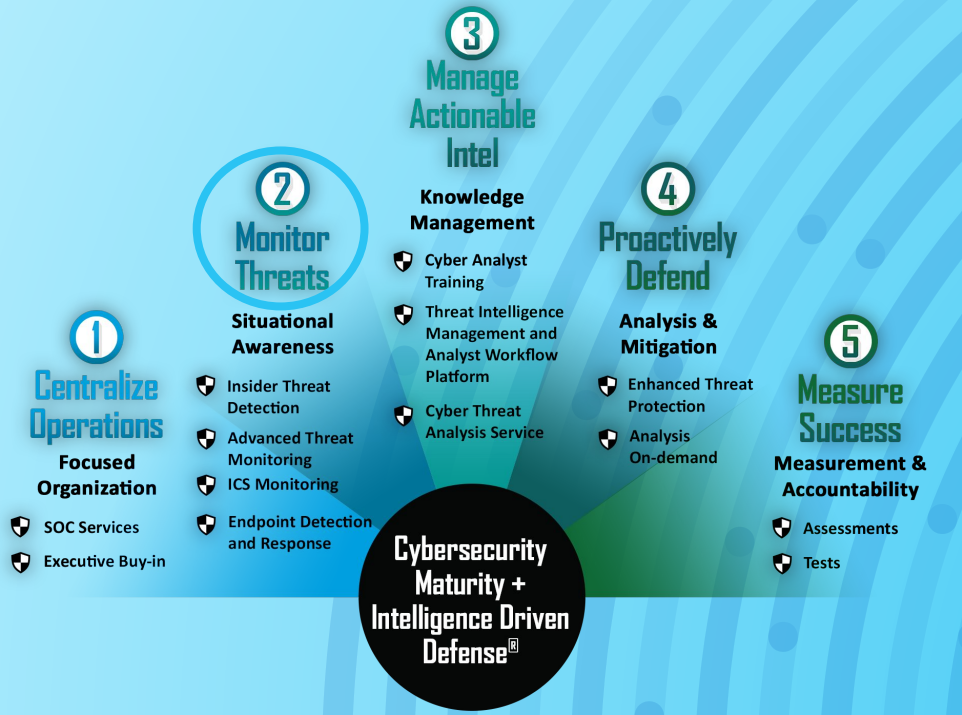
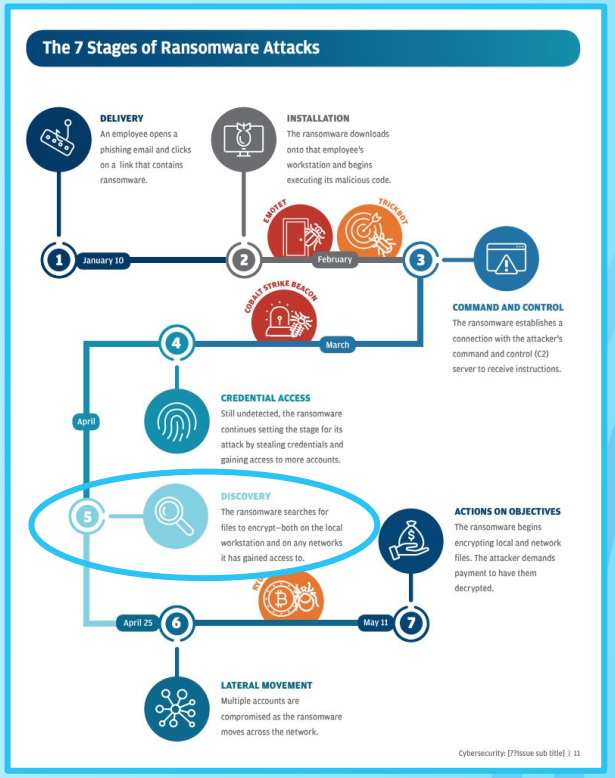
Where Does nanoIDS Fit In?

Lockheed Martin Intelligence Driven Defense® Model



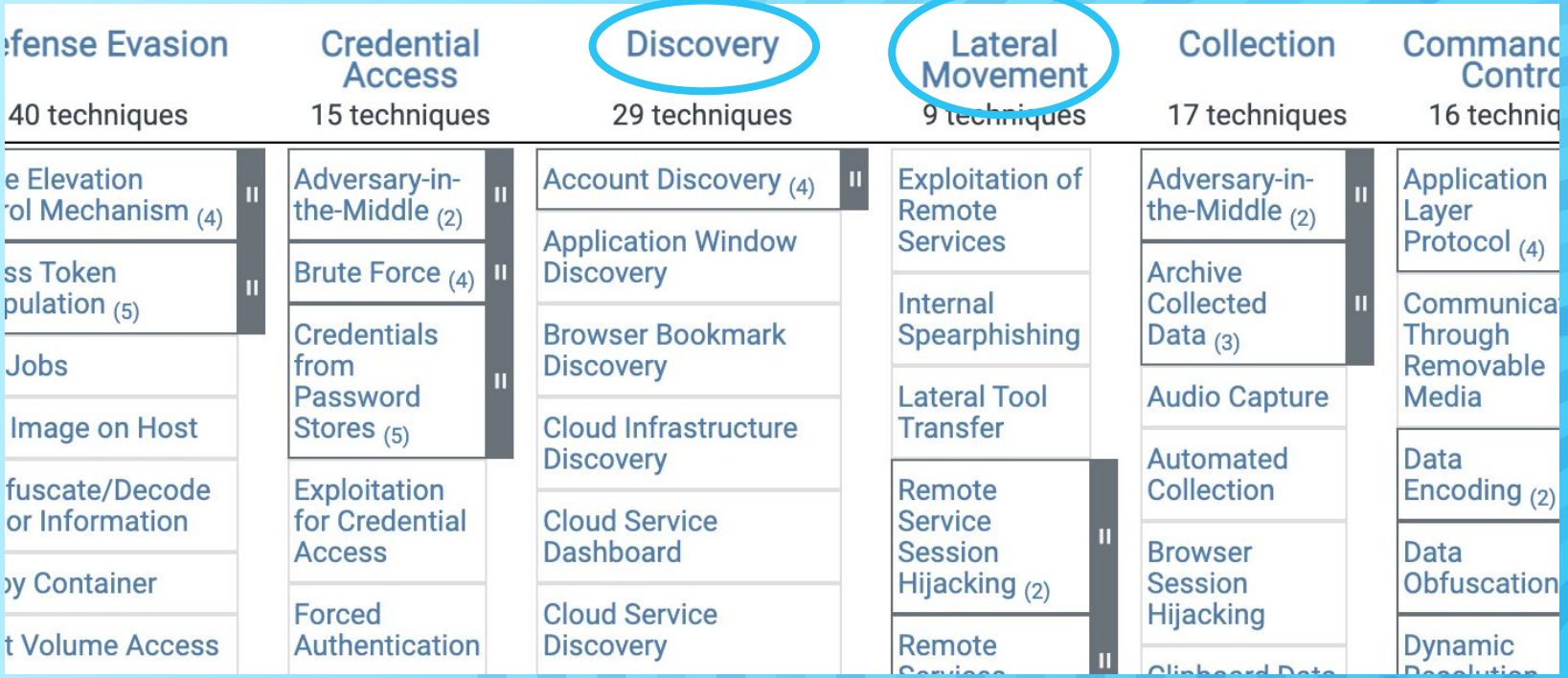
Where Does nanoIDS Fit In?

JP Morgan: The Anatomy of a Ransomware Attack



Where Does nanoIDS Fit In?

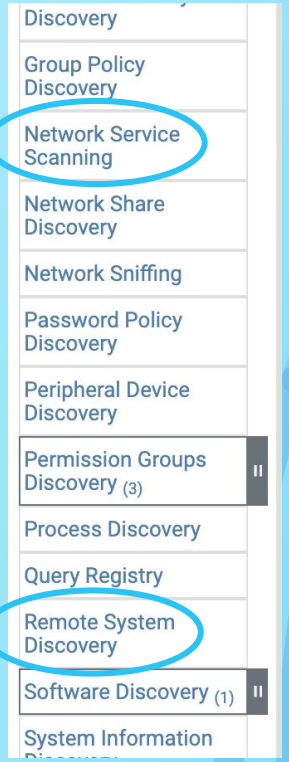
MITRE ATT&CK® Techniques



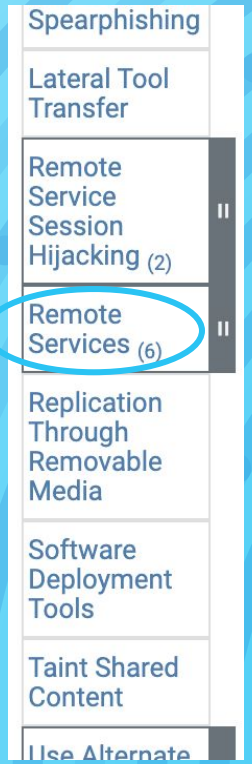
Where Does nanoIDS Fit In?

MITRE ATT&CK® Techniques

DISCOVERY



LATERAL MOVEMENT



Where Does nanoIDS Fit In?

MITRE ATT&CK® Data Sources

DS0004	Malware Repository	Information obtained (via shared or submitted samples) regarding malicious software (droppers, backdoors, etc.) used by adversaries
DS0011	Module	Executable files consisting of one or more shared classes and interfaces, such as portable executable (PE) format binaries/dynamic link libraries (DLL), executable and linkable format (ELF) binaries/shared libraries, and Mach-O format binaries/shared libraries
DS0023	Named Pipe	Mechanisms that allow inter-process communication locally or over the network. A named pipe is usually found as a file and processes attach to it
DS0033	Network Share	A storage resource (typically a folder or drive) made available from one host to others using network protocols, such as Server Message Block (SMB) or Network File System (NFS)
DS0029	Network Traffic	Data transmitted across a network (ex: Web, DNS, Mail, File, etc.), that is either summarized (ex: Netflow) and/or captured as raw data in an analyzable format (ex: PCAP)
DS0021	Persona	A malicious online profile representing a user commonly used by adversaries to social engineer or otherwise target victims
DS0014	Pod	A single unit of shared resources within a cluster, comprised of one or more containers