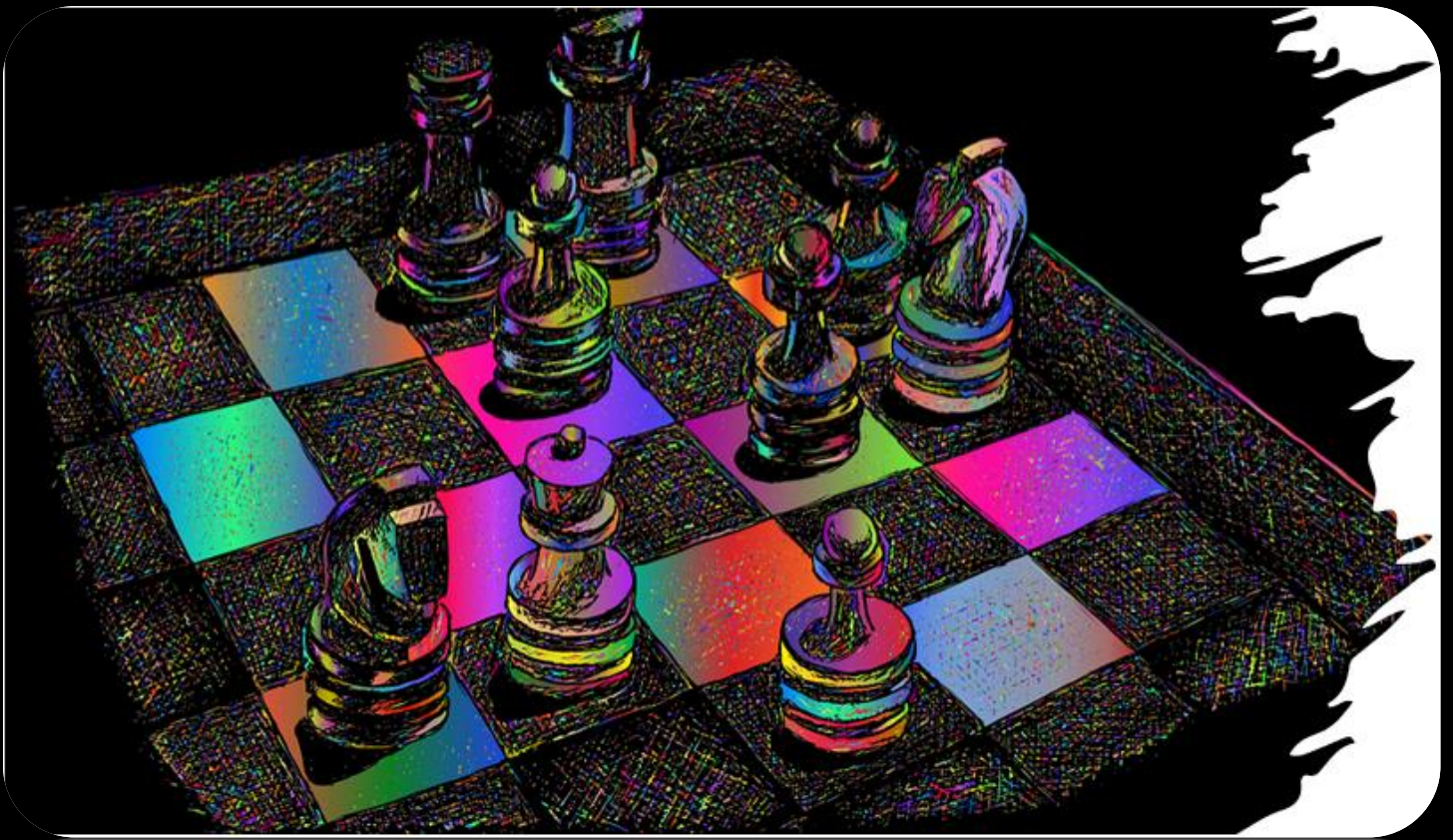


The **Accidental CISO**



Survival Kit

Version 1 – March 2022

The fruit of passion to my calling, I lovingly dedicate this masterpiece to my family; Chef Jennie Budomo Rebultan, Ashera Jear, and Akhira Andrei.

To God be the glory!



Michael Artemio Go Rebultan
Author, March 2022



TABLE OF CONTENTS

INTRODUCTION	3
CHAPTER 1: BUILDING CYOPS PROGRAM WITH MITRE FRAMEWORK	4
CHAPTER 2: SWOT ANALYSIS ON PEOPLE, PROCESS, AND TOOLS	25
CHAPTER 3: CYOPS MATURITY ASSESSMENT	27
CHAPTER 4: OPERATIONALIZING DFIR PROGRAM IN IT AND ICS/OT	28
CHAPTER 5: OPERATIONALIZING NEXGEN-SOC	33
CHAPTER 6: XDR BUSINESS CASES.....	35
CHAPTER 7: DIGITAL FORENSICS TOOL BUSINESS CASES	38
CHAPTER 8: OPERATIONALIZING CTI PROGRAM.....	39
CHAPTER 9: CTI PLATFORM BUSINESS CASES.....	42
CHAPTER 10: OPERATIONALIZING TVM PROGRAM	44
CHAPTER 11: OPERATIONALIZING INTERNAL BUG BOUNTY HUNTING PROGRAM	46
CHAPTER 12: ANNEX.....	49
▪ Network Detection and Response Business Cases	49
▪ Attack Surface Management Business Cases	50
▪ Security Risk Scorecard Business Cases	51
▪ IoT Asset and Inventory Intelligence Business Case	54
ACKNOWLEDGEMENT	56
ABOUT THE AUTHOR	57

INTRODUCTION

The chief information security officers (CISO) including the leaders, directors, and managers in most cases intend to duplicate their methodologies from their previous or past companies to their next journey with blindly understanding the business environment and cases with the current set-up of the security postures of both the information technology (IT) and the operational technology (OT) environments of the organization they just newly joined.

They seem to be drowned in their past recognitions and public fame that they have forgotten the fundamentals of “knowing yourself” first through SWOT (strength, weakness, opportunity, and strength) analysis of the people, process, and technology of the company and the cybersecurity critical mission and vision of the program.

Whilst tools for protecting and securing the organization’s digital fortress are equally important, leaders tend to overlook the significance of the people and process’ capabilities which most of the cases, the budget are not wisely spent and worse is, tools are overlapping because they just want to bring the security solutions from their past lives.

This e-book is solely intended to share the author’s experience on building various cybersecurity programs in operations – security operation center (SOC), digital forensics and incident response (DFIR), threat and vulnerability management (TVM), internal bug bounty hunting, and cyber threat intelligence (CTI) that incorporates with the purple teaming, red teaming, security awareness, and operational threat modeling with vendor neutrality for guidance in covering all the cybersecurity operations (CyOps) programs in a holistic manner – technical, business, and strategic.



CHAPTER 1

BUILDING CYOPS PROGRAM WITH MITRE FRAMEWORK

With the collaboration of thousands of cyber defenders and researchers from both the IT and OT networks, the MITRE ATT&CK framework is a great tool for reference that even a seasoned or first-time CISO could apply in building or revamping the cybersecurity program for technical, business, and strategical aspects. This will eliminate the overlapping of tools and clearly identify the program's gap in the people, processes, and policies. Hence, not only the defense-in-depth will be addressed but most importantly the cyber resilience and right budgeting.

In most of the instances that are evidently seen in many practices and conferences, the framework is being used for the reactive approach. Even many CTI providers and analysts were trying to track the adversaries' tactics, techniques, and procedures (TTPs); advanced persistent threats are constantly changing their attack vectors because they know that their signatures are already known to all security solutions.

Whilst artificial intelligence (AI) and machine learning (ML) have been adopted in cybersecurity detection and prevention systems, APTs use the same method and even more cleverly bypassed those defenses. Hence, many organizations are still being breached and compromised.

The table below is meant to assess the true current state of the security program on people, processes, and tools. This is even more effective if there are no existing tools and other members of the team yet and only the CISO is the first to be on-boarded so even the hiring criteria would be more people and process experience-centric with positive mindsets rather than the degree and certifications-oriented which are theoretical in nature. At the end of the day, it is how the CISO would want to achieve to make the CyOps operational within 3 to 6 months' time rather.

How to use this table?

The SECURITY PROGRAM column answers on what the MITIGATION is supposed to be under (i.e.: grc, dfir, tvrm, cti, etc.) and the DETECTION is a combination of the analysts, engineers, or operational processes (i.e.: audit control, threat hunting, vapt, etc.) in the absence or with the help of security tech-stacks. The PREVENTION is the actual tools or tech-stacks that can help the security program or detection to proactively defend the digital fortress of the organization, for both IT and OT networks.

ID	MITIGATION	DESCRIPTION	SECURITY PROGRAM	DETECTION (People/Process)	PREVENTION (Tools)
1	Account Use Policies	Configure features related to account use like login attempt lockouts, specific login times, etc.			
2	Active Directory Configuration	Configure Active Directory to prevent use of certain adversarial techniques; use SID Filtering, etc.			
3	Antivirus / Antimalware	Use signatures or heuristics to detect malicious software.			
4	Application Developer Guidance	Guidance or training given to developers of applications to avoid introducing security weaknesses that an adversary may be able to take advantage of.			
5	Application Isolation and Sandboxing	Restrict execution of code to a virtual environment on or in transit to an endpoint system.			
6	Audit	Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.			
7	Behaviour Prevention on Endpoint	Use capabilities to prevent suspicious behaviour patterns from occurring on endpoint systems.			
8	Boot Integrity	Use secure methods to boot a system and verify the integrity of the operating system and loading mechanisms.			
9	Code Signing	Enforce binary and application integrity with digital signature verification to prevent untrusted code from executing.			
10	Credential Access Protection	Use capabilities to prevent successful credential access by adversaries; including blocking forms of credential dumping.			
11	Data Backup	Ensure backup and storage systems are hardened and kept separate from the corporate network to prevent compromise.			
12	Data Loss Prevention	Use a data loss prevention (DLP) strategy to categorize sensitive data, identify data formats indicative of personal identifiable information (PII), and restrict exfiltration of sensitive data.			
13	Disable or Remove	Remove or deny access to unnecessary and potentially			

	Feature or Program	vulnerable software to prevent abuse by adversaries.			
14	Encrypt Sensitive Information	Protect sensitive information with strong encryption.			
15	Environment Variable Permissions	Prevent modification of environment variables by unauthorized users and groups.			
16	Execution Prevention	Block execution of code on a system through application control, and / or script blocking.			
17	Exploit Protection	Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring.			
18	Filter Network Traffic	Use network appliances to filter ingress or egress traffic and perform protocol-based filtering.			
19	Limit Access to Resource Over Network	Prevent access to file shares, remote access to systems, unnecessary services.			
20	Limit Hardware Installation	Block users or groups from installing or using unapproved hardware on systems, including USB devices.			
21	Limit Software Installation	Block users or groups from installing unapproved software.			
22	Multi-Factor Authentication	Use two or more pieces of evidence to authenticate to a system.			
23	Network Intrusion Prevention	Use intrusion detection signatures to block traffic at network boundaries.			
24	Network Segmentation	Architect sections of the network to isolate critical systems, functions, or resources.			
25	Operating System Configuration	System hardening			
26	Password Policies	Set and enforce secure password policies for accounts.			
27	Pre-compromise	This category is used for any applicable mitigation activities that apply to techniques occurring before an adversary gains Initial Access, such as Reconnaissance and Resource Development techniques.			
28	Privileged Account Management	Manage the creation, modification, use, and permissions associated to			

		privileged accounts, including SYSTEM and root.			
29	Privileged Process Integrity	Protect processes with high privileges that can be used to interact with critical system components; i.e. Process Injection			
30	Remote Data Storage	Use remote security log and sensitive file storage where access can be controlled better to prevent exposure of intrusion detection log data or sensitive information.			
31	Restrict File and Directory Permissions	Restrict access by setting directory and file permissions that are not specific to users or privileged accounts.			
32	Restrict Library Loading	Prevent abuse of library loading mechanisms in the operating system and software to load untrusted code.			
33	Restrict Registry Permissions	Restrict the ability to modify certain hives or keys in the Windows Registry.			
34	Restrict Web-Based Content	Restrict use of certain websites, block downloads / attachments, block JavaScript, restrict browser extensions, etc.			
35	Software Configuration	Implement configuration changes to software (other than the operating system) to mitigate security risks associated to how the software operates.			
36	SSL / TLS Inspection	Break and inspect SSL / TLS sessions to look at encrypted web traffic for adversary activity.			
37	Threat Intelligence Program	A threat intelligence program helps an organization generate their own threat intelligence information and track trends to inform defensive priorities to mitigate risk.			
38	Update Software	Perform regular software updates to mitigate exploitation risk.			
39	User Account Control	Configure Windows User Account Control to mitigate risk of adversaries obtaining elevated process access.			
40	User Account Management	Manage the creation, modification, use, and permissions associated to user accounts.			

41	User Training	To reduce the risk of successful spear-phishing, social engineering, and other adversarial techniques that involve user interaction.			
42	Vulnerability Scanning	Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them.			

The mitigations stated are applicable for both Cloud and OT as the impact is similar to IT even though they have different environments that are being protected; data (CIA – confidentiality, integrity, and availability) vs physical (SRP – safety & availability, reliability, and productivity).

Now, there might be some challenges on this reference, especially for those who are doing proof of concept (POC) or proof of value (POV) on selecting a security solution. Aside from the TTPs that can be found from the MITRE website itself, the lists have been collated below for testing against the security vendor to avoid being deceived by their marketing sales pitch and fancy presentations.

Note that this is a combination of the MITRE ATT&CK versions 1 and 10 but the TTPs are still relatively relevant.

ID	MITIGATION	DESCRIPTION	MITRE ATT&CK IDs
1	Account Use Policies	Configure features related to account use like login attempt lockouts, specific login times, etc.	Brute Force (T1110) Endpoint Denial of Service (T1499) Network Service Scanning (T1046) Code Signing (T1116) Create Account (T1136) Service Execution (T1035) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032)
2	Active Directory Configuration	Configure Active Directory to prevent use of certain adversarial techniques; use SID Filtering, etc.	Access Token Manipulation (T1134) Command-Line Interface (T1059) Credential Dumping (T1003) Domain Trust Discovery (T1482) Network Service Scanning (T1046) Code Signing (T1116) Create Account (T1136) Modify Existing Service (T1031) Pass the Ticket (T1097) SID-History Injection (T1178) Service Execution (T1035) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) Third-party Software (T1072)
3	Antivirus / Antimalware	Use signatures or heuristics to detect malicious software.	Command-Line Interface (T1059) Obfuscated Files or Information (T1027) Deobfuscated/Decode Files or Information (T1140) Network Service Scanning (T1046) Kernel Modules and Extensions (T1215)

			Code Signing (T1116) Data Obfuscation (T1001) Rootkit (T1014) PowerShell (T1086) Scripting (T1064) Service Execution (T1035) Signed Script Proxy Execution (T1216) Software Packing (T1045) Spearphishing Attachment (T1193) Spearphishing via Service (T1194) Standard Cryptographic Protocol (T1032) Template Injection (T1221) User Execution (T1204)
4	Application Developer Guidance	Guidance or training given to developers of applications to avoid introducing security weaknesses that an adversary may be able to take advantage of.	Credential Dumping (T1003) DLL Side-Loading (T1073) Network Service Scanning (T1046) Code Signing (T1116) Plist Modification (T1150) Screen Capture (T1113) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) Valid Accounts (T1078) Video Capture (T1125)
5	Application Isolation and Sandboxing	Restrict execution of code to a virtual environment on or in transit to an endpoint system.	Dynamic Data Exchange (T1173) Exploit Public-Facing Application (T1190) Exploitation for Credential Access (T1212) Exploitation for Defense Evasion (T1211) Exploitation for Remote Services (T1210) Network Service Scanning (T1046) Code Signing (T1116) Drive-by Compromise (T1189) Exploitation for Client Execution (T1203) Exploitation for Privilege Escalation (T1068) Remote Services (T1021) Service Execution (T1035) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032)
6	Audit	Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.	Account Discovery (T1087) Bypass User Account Control (T1088) Command-Line Interface (T1059) Data from Information Repositories (T1213) Domain Trust Discovery (T1482) Email Collection (T1114) Execution through API (T1106) Execution through Module Load (T1129) Exploitation for Remote Services (T1210) Network Service Scanning (T1046) File Deletion (T1107) Group Policy Modification (T1484) Input Capture (T1056) LC_LOAD_DYLIB Additions (T1161) Launch Daemon (T1160) Browser Extensions (T1176) Code Signing (T1116) Create Account (T1136) Credential in Registry (T1214) File and Directory Discovery (T1083) Remote Desktop Protocol (T1076) Local Job Scheduling (T1168) Masquerading (T1036)

			Modify Existing Service (T1031) Path Interception (T1034) PowerShell (T1086) Remote Access Tools (T1219) Remote Services (T1021) Scheduled Task (T1053) Scripting (T1064) Service Execution (T1035) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) System Owner/User Discovery (T1033) Third-party Software (T1072) Trusted Relationship (T1199) User Execution (T1204)
7	Behaviour Prevention on Endpoint	Use capabilities to prevent suspicious behaviour patterns from occurring on endpoint systems.	Command-Line Interface (T1059) Connection Proxy (T1090) Credential Dumping (T1003) Data Encrypted for Impact (T1486) Obfuscated Files or Information (T1027) Deobfuscated/Decode Files or Information T1140) Dynamic Data Exchange (T1173) Execution through API (T1106) Network Service Scanning (T1046) Code Signing (T1116) Data Obfuscation (T1001) Data from Removable Media (T1025) LSASS Driver (T1177) Modify Existing Service (T1031) Office Application Startup (T1137) Process Doppelganging (T1186) Process Hollowing (T1093) Process Injection (T1055) Replication Through Removable Media (T1091) Scripting (T1064) Service Execution (T1035) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) Startup Items (T1165) Uncommonly Used Port (T1065) User Execution (T1204) Windows Management Instrumentation (T1047) Windows Management Instrumentation Event Subscription (T1084)
8	Boot Integrity	Use secure methods to boot a system and verify the integrity of the operating system and loading mechanisms.	Network Service Scanning (T1046) Firmware Corruption (T1495) Kernel Modules and Extensions (T1215) Code Signing (T1116) Rootkit (T1014) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) Supply Chain Compromise (T1195) System Firmware (T1019)
9	Code Signing	Enforce binary and application integrity with digital signature verification to prevent untrusted code from executing.	AppleScript (T1155) Command-Line Interface (T1059) Network Service Scanning (T1046) LC_LOAD_DYLIB Additions (T1161) Code Signing (T1116) Masquerading (T1036) PowerShell (T1086) Scripting (T1064)

			Service Execution (T1035) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) User Execution (T1204)
10	Credential Access Protection	Use capabilities to prevent successful credential access by adversaries; including blocking forms of credential dumping.	Credential Dumping (T1003) Obfuscated Files or Information (T1027) Network Service Scanning (T1046) Code Signing (T1116) Create Account (T1136) LSASS Driver (T1177) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032)
11	Data Backup	Ensure backup and storage systems are hardened and kept separate from the corporate network to prevent compromise.	Credential Dumping (T1003) Data Destruction (T1485) Data Encrypted for Impact (T1486) Defacement (T1491) Disk Content Wipe (T1488) Obfuscated Files or Information (T1027) Network Service Scanning (T1046) Inhibit System Recovery (T1490) Code Signing (T1116) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032)
12	Data Loss Prevention	Use a data loss prevention (DLP) strategy to categorize sensitive data, identify data formats indicative of personal identifiable information (PII), and restrict exfiltration of sensitive data.	Data from Local System (T1005) Obfuscated Files or Information (T1027) Deobfuscated/Decode Files or Information T1140) Exfiltration Over Alternative Protocol (T1048) Exfiltration Over Command-and-Control Channel T1041) Exfiltration Over Physical Medium (T1052) Network Service Scanning (T1046) Code Signing (T1116) Data Obfuscation (T1001) Data from Removable Media (T1025) Service Execution (T1035) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032)
13	Disable or Remove Feature or Program	Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.	CMSTP (T1191) Command-Line Interface (T1059) Connection Proxy (T1090) Credential Dumping (T1003) Data from Network Shared Drive (T1039) Disabling Security Tools (T1089) Distributed Component Object Model (T1175) Dynamic Data Exchange (T1173) Email Collection (T1114) Execution through API (T1106) Exfiltration Over Alternative Protocol (T1048) Exfiltration Over Other Network Medium (T1011) Exfiltration Over Physical Medium (T1052) Exploitation for Remote Services (T1210) Network Service Scanning (T1046) External Remote Services (T1133) InstallUtil (T1118) LLMNR/NBT-NS Poisoning (T1171) Launch Daemon (T1160) Account Manipulation (T1098) Code Signing (T1116) Communication Through Removable Media T1092) Data from Removable Media (T1025)

			Windows Remote Management (T1028) Remote Desktop Protocol (T1076) Mshta (T1170) Network Share Discovery (T1135) Office Application Startup (T1137) Plist Modification (T1150) Port Knocking (T1205) PowerShell (T1086) Private Keys (T1145) Regsvcs/Regasm (T1121) Remote Access Tools (T1219) Remote Services (T1021) Replication Through Removable Media (T1091) Service Stop (T1489) SSH Hijacking (T1184) Screensaver (T1180) Scripting (T1064) Service Execution (T1035) Signed Binary Proxy Execution (T1218) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) Startup Items (T1165) System Network Configuration Discovery (T1016) Template Injection (T1221) Third-party Software (T1072) Trusted Developer Utilities (T1127) Web Shell (T1100) Windows Admin Shares (T1077)
14	Encrypt Sensitive Information	Protect sensitive information with strong encryption.	Automated Exfiltration (T1020) Brute Force (T1110) Credential Dumping (T1003) Data Encrypted for Impact (T1486) Data Encrypted (T1022) Obfuscated Files or Information (T1027) Email Collection (T1114) Network Service Scanning (T1046) Indicator Removal on Host (T1070) Input Capture (T1056) Kerberoasting (T1208) Automated Collection (T1119) Code Signing (T1116) Data Obfuscation (T1001) Network Sniffing (T1040) Service Execution (T1035) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) Stored Data Manipulation (T1492) System Network Configuration Discovery (T1016) Transmitted Data Manipulation (T1493)
15	Environment Variable Permissions	Prevent modification of environment variables by unauthorized users and groups.	Bash History (T1139) Clear Command History (T1146) Network Service Scanning (T1046) HISTCONTROL (T1148) Indicator Removal on Host (T1070) Code Signing (T1116) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032)
16	Execution Prevention	Block execution of code on a system through application control, and / or script blocking.	AppCert DLLs (T1182) AppInit DLLs (T1103) AppleScript (T1155)

			CMSTP (T1191) Command-Line Interface (T1059) Complied HTML File (T1223) Connection Proxy (T1090) Control Panel Item (T1196) Execution through API (T1106) Execution through Module Load (T1129) Network Service Scanning (T1046) Gatekeeper Bypass (T1144) Group Policy Modification (T1484) Hidden Window (T1143) InstallUtil (T1118) Kernel Modules and Extensions (T1215) LC_LOAD_DYLIB Additions (T1161) Accessibility Features (T1015) Browser Extensions (T1176) Code Signing (T1116) Exploitation for Privilege Escalation (T1068) Rootkit (T1014) Masquerading (T1036) Mshta (T1170) Path Interception (T1034) Plist Modification (T1150) PowerShell (T1086) Regsvcs/Regasm (T1121) Remote Access Tools (T1219) SIP and Trust Provider Hijacking (T1198) Screensaver (T1180) Scripting (T1064) Signed Binary Proxy Execution (T1218) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) Taint Shared Content (T1080) Trusted Developer Utilities (T1127) User Execution (T1204) Windows Management Instrumentation (T1047) Winlogon Helper DLL (T1004) XSL Script Processing (T1220)
17	Exploit Protection	Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring.	AppCert DLLs (T1182) Applnit DLLs (T1103) AppleScript (T1155) CMSTP (T1191) Command-Line Interface (T1059) Complied HTML File (T1223) Connection Proxy (T1090) Control Panel Item (T1196) Execution through API (T1106) Execution through Module Load (T1129) Network Service Scanning (T1046) Gatekeeper Bypass (T1144) Group Policy Modification (T1484) Hidden Window (T1143) InstallUtil (T1118) Kernel Modules and Extensions (T1215) LC_LOAD_DYLIB Additions (T1161) Accessibility Features (T1015) Browser Extensions (T1176) Code Signing (T1116) Exploitation for Privilege Escalation (T1068) Rootkit (T1014)

			Masquerading (T1036) Mshta (T1170) Path Interception (T1034) Plist Modification (T1150) PowerShell (T1086) Regsvcs/Regasm (T1121) Remote Access Tools (T1219) SIP and Trust Provider Hijacking (T1198) Screensaver (T1180) Scripting (T1064) Signed Binary Proxy Execution (T1218) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) Taint Shared Content (T1080) Trusted Developer Utilities (T1127) User Execution (T1204) Windows Management Instrumentation (T1047) Winlogon Helper DLL (T1004) XSL Script Processing (T1220)
18	Filter Network Traffic	Use network appliances to filter ingress or egress traffic and perform protocol-based filtering.	BITS Jobs (T1197) Connection Proxy (T1090) Data from Network Shared Drive (T1039) Obfuscated Files or Information (T1027) Deobfuscated/Decode Files or Information (T1140) Domain Fronting (T1172) Endpoint Denial of Service (T1499) Execution through API (T1106) Exfiltration Over Alternative Protocol (T1048) Exfiltration Over Command and Control Channel (T1041) Exploitation for Remote Services (T1210) Network Service Scanning (T1046) Forced Authentication (T1187) LLMNR/NBT-NS Poisoning (T1171) Code Signing (T1116) Data Obfuscation (T1001) Multi-hop Proxy (T1188) Multilayer Encryption (T1079) Network Denial of Service (T1498) Network Share Discovery (T1135) Port Knocking (T1205) Remote Access Tools (T1219) Remote Services (T1021) Service Execution (T1035) Signed Binary Proxy Execution (T1218) Signed Script Proxy Execution (T1216) Standard Application Layer Protocol (T1071) Standard Cryptographic Protocol (T1032) Standard Non-Application Layer Protocol (T1095) System Network Configuration Discovery (T1016) Third-party Software (T1072) Uncommonly Used Port (T1065) Valid Accounts (T1078) Windows Admin Shares (T1077)
19	Limit Access to Resource Over Network	Prevent access to file shares, remote access to systems, unnecessary services.	Data Encrypted (T1022) Data from Network Shared Drive (T1039) Obfuscated Files or Information (T1027) Execution through API (T1106) Exploitation for Remote Services (T1210) Network Service Scanning (T1046)

			External Remote Services (T1133) Launch Daemon (T1160) Accessibility Features (T1015) Code Signing (T1116) Remote Desktop Protocol (T1076) Hardware Additions (T1200) Network Share Discovery (T1135) Private Keys (T1145) Remote Services (T1021) Service Execution (T1035) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) Standard Non-Application Layer Protocol (T1095) System Network Configuration Discovery (T1016) Uncommonly Used Port (T1065) Windows Admin Shares (T1077)
20	Limit Hardware Installation	Block users or groups from installing or using unapproved hardware on systems, including USB devices.	Exfiltration Over Physical Medium (T1052) Network Service Scanning (T1046) Code Signing (T1116) Data from Removable Media (T1025) Hardware Additions (T1200) Replication Through Removable Media (T1091) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032)
21	Limit Software Installation	Block users or groups from installing unapproved software.	Command-Line Interface (T1059) Network Service Scanning (T1046) Browser Extensions (T1176) Code Signing (T1116) Remote Access Tools (T1219) Remote Services (T1021) Scripting (T1064) Service Execution (T1035) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) Third-party Software (T1072)
22	Multi-Factor Authentication	Use two or more pieces of evidence to authenticate to a system.	Brute Force (T1110) Connection Proxy (T1090) Data from Information Repositories (T1213) Email Collection (T1114) Execution through API (T1106) Network Service Scanning (T1046) External Remote Services (T1133) Input Capture (T1056) Account Manipulation (T1098) Code Signing (T1116) Create Account (T1136) Network Sniffing (T1040) Private Keys (T1145) Remote Services (T1021) Service Execution (T1035) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) Third-party Software (T1072) Two-Factor Authentication Interception (T1111) Valid Accounts (T1078)
23	Network Intrusion Prevention	Use intrusion detection signatures to block traffic at network boundaries.	Brute Force (T1110) Connection Proxy (T1090) Data Encoding (T1132) Data Transfer Size Limits (T1030) Data from Network Shared Drive (T1039)

			Obfuscated Files or Information (T1027) Deobfuscated/Decode Files or Information (T1140) Domain Generation Algorithms (T1483) Exfiltration Over Alternative Protocol (T1048) Exfiltration Over Command and Control Channel (T1041) Exploitation for Remote Services (T1210) Network Service Scanning (T1046) Fallback Channels (T1008) LLMNR/NBT-NS Poisoning (T1171) Code Signing (T1116) Data Obfuscation (T1001) Modify Existing Service (T1031) Multi-Stage Channels (T1104) Multilayer Encryption (T1079) Network Share Discovery (T1135) Remote Access Tools (T1219) Remote File Copy (T1105) Scheduled Transfer (T1029) Service Execution (T1035) Signed Script Proxy Execution (T1216) Spearphishing Attachment (T1193) Standard Application Layer Protocol (T1071) Standard Cryptographic Protocol (T1032) Standard Non-Application Layer Protocol (T1095) System Network Configuration Discovery (T1016) Template Injection (T1221) Uncommonly Used Port (T1065) User Execution (T1204) Web Service (T1102) Windows Admin Shares (T1077)
24	Network Segmentation	Architect sections of the network to isolate critical systems, functions, or resources.	Connection Proxy (T1090) Data from Network Shared Drive (T1039) Obfuscated Files or Information (T1027) Deobfuscated/Decode Files or Information (T1140) Distributed Component Object Model (T1175) Domain Trust Discovery (T1482) Execution through API (T1106) Exfiltration Over Alternative Protocol (T1048) Exfiltration Over Command and Control Channel (T1041) Exploit Public-Facing Application (T1190) Exploitation for Remote Services (T1210) Network Service Scanning (T1046) External Remote Services (T1133) LLMNR/NBT-NS Poisoning (T1171) Account Manipulation (T1098) Code Signing (T1116) Create Account (T1136) Data Obfuscation (T1001) Windows Remote Management (T1028) Remote Desktop Protocol (T1076) Network Share Discovery (T1135) Remote Services (T1021) Runtime Data Manipulation (T1494) Service Stop (T1489) Service Execution (T1035) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) Standard Non-Application Layer Protocol (T1095)

			Third-party Software (T1072) Trusted Relationship (T1199) Windows Admin Shares (T1077)
25	Operating System Configuration	System hardening	Account Discovery (T1087) BITS Jobs (T1197) Bash History (T1139) Clear Command History (T1146) Credential Dumping (T1003) Data from Network Shared Drive (T1039) Exfiltration Over Alternative Protocol (T1048) Exfiltration Over Other Network Medium (T1011) Exploitation for Remote Services (T1210) Network Service Scanning (T1046) File Deletion (T1107) Group Policy Modification (T1484) HISTCONTROL (T1148) Hidden Users (T1147) Inhibit System Recovery (T1490) Install Root Certificate (T1130) Accessibility Features (T1015) Account Manipulation (T1098) Code Signing (T1116) Communication Through Removable Media (T1092) Create Account (T1136) Remote Desktop Protocol (T1076) LSASS Driver (T1177) Masquerading (T1036) Network Share Discovery (T1135) Password Filter DLL (T1174) Query Registry (T1012) Remote Services (T1021) Service Stop (T1489) SIP and Trust Provider Hijacking (T1198) Scheduled Task (T1053) Service Execution (T1035) Setuid and Setgid (T1166) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) Sudo (T1169) Sudo Caching (T1206) Third-party Software (T1072) Trusted Relationship (T1199) Windows Admin Shares (T1077) Winlogon Helper DLL (T1004)
26	Password Policies	Set and enforce secure password policies for accounts.	Account Discovery (T1087) Brute Force (T1110) Credential Dumping (T1003) Data from Network Shared Drive (T1039) Exploitation for Remote Services (T1210) Network Service Scanning (T1046) Forced Authentication (T1187) Keberoasting (T1208) Keychain (T1142) Code Signing (T1116) Credential in Registry (T1214) LSASS Driver (T1177) Network Share Discovery (T1135) Pass the Ticket (T1097) Password Filter DLL (T1174) Password Policy Discovery (T1201)

			Private Keys (T1145) Remote Services (T1021) SSH Hijacking (T1184) Service Execution (T1035) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) Third-party Software (T1072) Trusted Relationship (T1199) Valid Accounts (T1078) Windows Admin Shares (T1077)
27	Pre-compromise	This category is used for any applicable mitigation activities that apply to techniques occurring before an adversary gains Initial Access, such as Reconnaissance and Resource Development techniques.	Acquire Infrastructure (T1583) Active Scanning (T1595) Compromise Accounts (T1586) Compromise Infrastructure (T1584) Develop Capabilities (T1587) Gather Victim Host Information (T1592) Gather Victim Identity Information (T1589) Gather Victim Network Information (T1590) Gather Victim Org Information (T1591) Search Victim-Owned Websites (T1594) Stage Capabilities (T1608)
28	Privileged Account Management	Manage the creation, modification, use, and permissions associated to privileged accounts, including SYSTEM and root.	Access Token Manipulation (T1134) Account Discovery (T1087) Bypass User Account Control (T1088) Command-Line Interface (T1059) Connection Proxy (T1090) Credential Dumping (T1003) Data from Network Shared Drive (T1039) Distributed Component Object Model (T1175) Domain Trust Discovery (T1482) Execution through API (T1106) Exploit Public-Facing Application (T1190) Exploitation for Remote Services (T1210) Network Service Scanning (T1046) File Permission Modification (T1222) Firmware Corruption (T1495) Group Policy Modification (T1484) Input Capture (T1056) Keberoasting (T1208) Account Manipulation (T1098) Code Signing (T1116) Create Account (T1136) Credential in Registry (T1214) Windows Remote Management (T1028) Remote Desktop Protocol (T1076) LSASS Driver (T1177) Modify Existing Service (T1031) Modify Registry (T1112) Network Share Discovery (T1135) Pass the Hash (T1075) Pass the Ticket (T1097) PowerShell (T1086) Private Keys (T1145) Process Injection (T1055) Remote Services (T1021) SSH Hijacking (T1184) Scheduled Task (T1053) Scripting (T1064) Service Execution (T1035) Signed Binary Proxy Execution (T1218)

			Signed Script Proxy Execution (T1216) Software Packing (T1045) Standard Cryptographic Protocol (T1032) Sudo (T1169) Sudo Caching (T1206) T1501 (T1501) Third-party Software (T1072) Valid Accounts (T1078) Video Capture (T1125) Windows Admin Shares (T1077) Windows Management Instrumentation (T1047)
29	Privileged Process Integrity	Protect processes with high privileges that can be used to interact with critical system components; i.e. Process Injection	Authentication Package (T1131) Credential Dumping (T1003) Network Service Scanning (T1046) Code Signing (T1116) LSASS Driver (T1177) Process Injection (T1055) Security Support Provider (T1101) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032)
30	Remote Data Storage	Use remote security log and sensitive file storage where access can be controlled better to prevent exposure of intrusion detection log data or sensitive information.	Data Encrypted (T1022) Obfuscated Files or Information (T1027) Network Service Scanning (T1046) Indicator Removal on Host (T1070) Input Capture (T1056) Automated Collection (T1119) Code Signing (T1116) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) Stored Data Manipulation (T1492) Third-party Software (T1072)
31	Restrict File and Directory Permissions	Restrict access by setting directory and file permissions that are not specific to users or privileged accounts.	Bash History (T1139) Clear Command History (T1146) Connection Proxy (T1090) Control Panel Item (T1196) Credential Dumping (T1003) Data from Network Shared Drive (T1039) Disabling Security Tools (T1089) Dylib Hijacking (T1157) Network Service Scanning (T1046) File Deletion (T1107) File Permission Modification (T1222) Indicator Removal on Host (T1070) Account Manipulation (T1098) Code Signing (T1116) Create Account (T1136) Logon Script (T1037) Masquerading (T1036) Modify Existing Service (T1031) NTFS File Attributes (T1096) Path Interception (T1034) Plist Modification (T1150) PowerShell (T1086) Private Keys (T1145) Process Injection (T1055) Rc.common (T1163) Remote Services (T1021) Runtime Data Manipulation (T1494) Service Stop (T1489) SIP and Trust Provider Hijacking (T1198)

			SSH Hijacking (T1184) Scheduled Task (T1053) Scripting (T1064) Service Execution (T1035) Signed Binary Proxy Execution (T1218) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) Startup Items (T1165) Stored Data Manipulation (T1492) Sudo (T1169) System Time Discovery (T1124) T1501 (T1501) Taint Shared Content (T1080) Time Providers (T1209)
32	Restrict Library Loading	Prevent abuse of library loading mechanisms in the operating system and software to load untrusted code.	Network Service Scanning (T1046) Code Signing (T1116) LSASS Driver (T1177) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032)
33	Restrict Registry Permissions	Restrict the ability to modify certain hives or keys in the Windows Registry.	Disabling Security Tools (T1089) Network Service Scanning (T1046) Code Signing (T1116) Logon Script (T1037) Modify Existing Service (T1031) Modify Registry (T1112) Service Stop (T1489) SIP and Trust Provider Hijacking (T1198) Scripting (T1064) Service Execution (T1035) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) System Time Discovery (T1124) Time Providers (T1209)
34	Restrict Web-Based Content	Restrict use of certain websites, block downloads / attachments, block JavaScript, restrict browser extensions, etc.	Command-Line Interface (T1059) Complied HTML File (T1223) Connection Proxy (T1090) Control Panel Item (T1196) Data Compressed (T1002) Obfuscated Files or Information (T1027) Domain Generation Algorithms (T1483) Exfiltration Over Alternative Protocol (T1048) Network Service Scanning (T1046) Browser Extensions (T1176) Code Signing (T1116) Create Account (T1136) Credential in Registry (T1214) Drive-by Compromise (T1189) Mshta (T1170) NTFS File Attributes (T1096) Scripting (T1064) Service Execution (T1035) Signed Binary Proxy Execution (T1218) Signed Script Proxy Execution (T1216) Spearphishing Attachment (T1193) Spearphishing Link (T1192) Spearphishing via Service (T1194) Standard Application Layer Protocol (T1071) Standard Cryptographic Protocol (T1032) Third-party Software (T1072) Trusted Relationship (T1199)

			Uncommonly Used Port (T1065) User Execution (T1204) Web Service (T1102)
35	Software Configuration	Implement configuration changes to software (other than the operating system) to mitigate security risks associated to how the software operates.	Obfuscated Files or Information (T1027) Dynamic Data Exchange (T1173) Exfiltration Over Alternative Protocol (T1048) Network Service Scanning (T1046) File Deletion (T1107) Install Root Certificate (T1130) Code Signing (T1116) Office Application Startup (T1137) PowerShell (T1086) Query Registry (T1012) Scripting (T1064) Service Execution (T1035) Signed Script Proxy Execution (T1216) Spearphishing Attachment (T1193) Spearphishing Link (T1192) Standard Cryptographic Protocol (T1032) Startup Items (T1165) User Execution (T1204)
36	SSL / TLS Inspection	Break and inspect SSL / TLS sessions to look at encrypted web traffic for adversary activity.	Connection Proxy (T1090) Obfuscated Files or Information (T1027) Domain Fronting (T1172) Exfiltration Over Alternative Protocol (T1048) Network Service Scanning (T1046) Code Signing (T1116) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) Video Capture (T1125)
37	Threat Intelligence Program	A threat intelligence program helps an organization generate their own threat intelligence information and track trends to inform defensive priorities to mitigate risk.	Exploitation for Credential Access (T1212) Exploitation for Defense Evasion (T1211) Exploitation for Privilege Escalation (T1068) Exploitation of Remote Services (T1210)
38	Update Software	Perform regular software updates to mitigate exploitation risk.	AppInit DLLs (T1103) Application Shimmin (T1138) Bypass User Account Control (T1088) Credential Dumping (T1003) DLL Side-Loading (T1073) Execution through Module Load (T1129) Exploit Public-Facing Application (T1190) Exploitation for Credential Access (T1212) Exploitation for Defense Evasion (T1211) Exploitation for Remote Services (T1210) Network Service Scanning (T1046) Firmware Corruption (T1495) Browser Extensions (T1176) Code Signing (T1116) Drive-by Compromise (T1189) Exploitation for Privilege Escalation (T1068) Office Application Startup (T1137) Pass the Hash (T1075) Scripting (T1064) Service Execution (T1035) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) Startup Items (T1165)

			Supply Chain Compromise (T1195) Third-party Software (T1072)
39	User Account Control	Configure Windows User Account Control to mitigate risk of adversaries obtaining elevated process access.	Bypass User Account Control (T1088) Network Service Scanning (T1046) Code Signing (T1116) Pass the Hash (T1075) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) Trusted Relationship (T1199)
40	User Account Management	Manage the creation, modification, use, and permissions associated to user accounts.	Access Token Manipulation (T1134) Account Discovery (T1087) BITS Jobs (T1197) Brute Force (T1110) Bypass User Account Control (T1088) Command-Line Interface (T1059) Data from Information Repositories (T1213) Disabling Security Tools (T1089) Exploitation for Remote Services (T1210) Network Service Scanning (T1046) File Deletion (T1107) Group Policy Modification (T1484) Launch Daemon (T1160) Launchctl (T1152) Code Signing (T1116) Create Account (T1136) Remote Desktop Protocol (T1076) Local Job Scheduling (T1168) Man in the Browser (T1185) Modify Existing Service (T1031) Pass the Hash (T1075) Pass the Ticket (T1097) Private Keys (T1145) Remote Services (T1021) Service Stop (T1489) Scheduled Task (T1053) Scripting (T1064) Service Execution (T1035) Shortcut Modification (T1023) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) T1501 (T1501) Third-party Software (T1072) Trusted Relationship (T1199) Valid Accounts (T1078) Web Shell (T1100) Windows Management Instrumentation (T1047) Windows Management Instrumentation Event Subscription (T1084) Winlogon Helper DLL (T1004)
41	User Training	To reduce the risk of successful spear-phishing, social engineering, and other adversarial techniques that involve user interaction.	Credential Dumping (T1003) Data from Information Repositories (T1213) Exfiltration Over Alternative Protocol (T1048) Network Service Scanning (T1046) Graphical User Interface (T1061) Input Capture (T1056) Browser Extensions (T1176) Code Signing (T1116) LSASS Driver (T1177) Man in the Browser (T1185) Masquerading (T1036)

			Plist Modification (T1150) Service Execution (T1035) Signed Script Proxy Execution (T1216) Spearphishing Attachment (T1193) Spearphishing Link (T1192) Spearphishing via Service (T1194) Standard Cryptographic Protocol (T1032) System Network Configuration Discovery (T1016) Template Injection (T1221) Third-party Software (T1072) Trusted Relationship (T1199) Two-Factor Authentication Interception (T1111) User Execution (T1204) Valid Accounts (T1078) Video Capture (T1125)
42	Vulnerability Scanning	Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them.	Exploit Public-Facing Application (T1190) Exploitation for Remote Services (T1210) Network Service Scanning (T1046) Code Signing (T1116) Service Execution (T1035) Signed Script Proxy Execution (T1216) Standard Cryptographic Protocol (T1032) Supply Chain Compromise (T1195)

To visualize the end result of this strategy using the MITRE ATT&CK framework, below are the breakdown of the priorities on how to achieve both defense-in-depth and cyber resiliency for budgeting.

BEST PRACTICES

- Asset and Inventory Management (AIM)
- AD Hardening (CIS)
- Operating System Configuration (CIS)
- Data Backup (3-2-1-1 rule)
- Update Software
- Application Control
- Network Segmentation (IEC62443)
- Business Continuity and Disaster Recovery Plans (BCP/DRP)

INVESTMENT TOOLS

- Multi-Factor Authentication (MFA)
- Web Application Firewall (WAF)
- Filter Network Traffic (FW)
- Privileged Account Management (PAM)
- Data Loss Prevention (DLP)
- User and Entity Behaviour Analytics (UEBA)
- Endpoint Detection and Response (EDR)
- Security Information and Event Management (SIEM)

CYBER SECURITY PROGRAM

- Governance and Risk Compliance
- Threat and Vulnerability Management
- Patch Management
- Security Awareness
- Incident Response Management
- Architecture and Countermeasure Engineering
- Cyber Threat Intelligence

MITRE ATT&CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

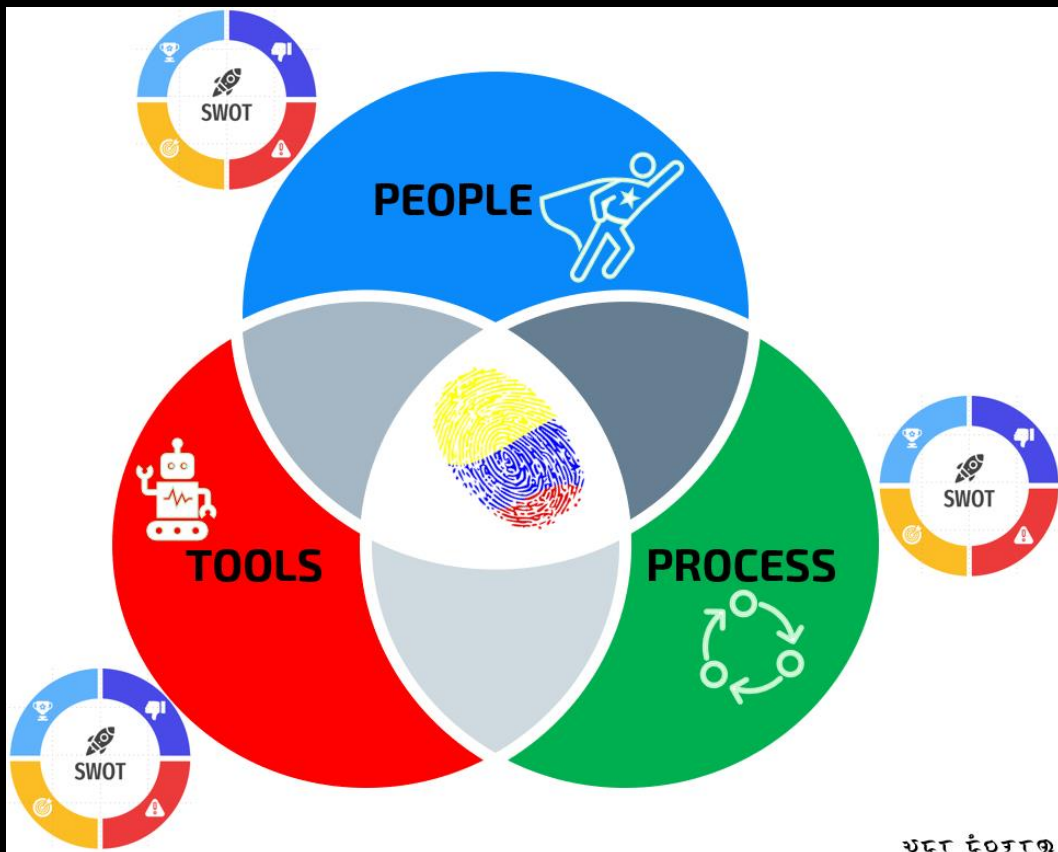
[help](#) [changelog](#) [theme ▾](#)

Create New Layer	Create a new empty layer	▾
Open Existing Layer	Load a layer from your computer or a URL	▾
Create Layer from other layers	Choose layers to inherit properties from	▾
Create Customized Navigator	Create a hyperlink to a customized ATT&CK Navigator	▾

CHAPTER 2

SWOT ANALYSIS ON PEOPLE, PROCESS, AND TOOLS

As the great military strategist Sun Tzu once wrote in his book “The Art of War” – “If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”



Cybersecurity was originally derived from military warfare, the CISO is the commander-in-chief who should know his overall defenses; from people, processes, and arsenals for him to effectively defend the organization's business and valuable assets.

- **Strength** – competitive advantage of the people, process, and tools within the cybersecurity operations.
- **Weakness** – limitations of the people, process, and tools within the cybersecurity operations.
- **Opportunity** – chances to strengthen the weaknesses of the people, process, and tools to the cybersecurity operations.
- **Threat** – potential risks or challenges to achieve the chances to reinforce the people, process, and tools within the cybersecurity operations.

The data provided below were just an example and should be taken as a guide and not as-is.

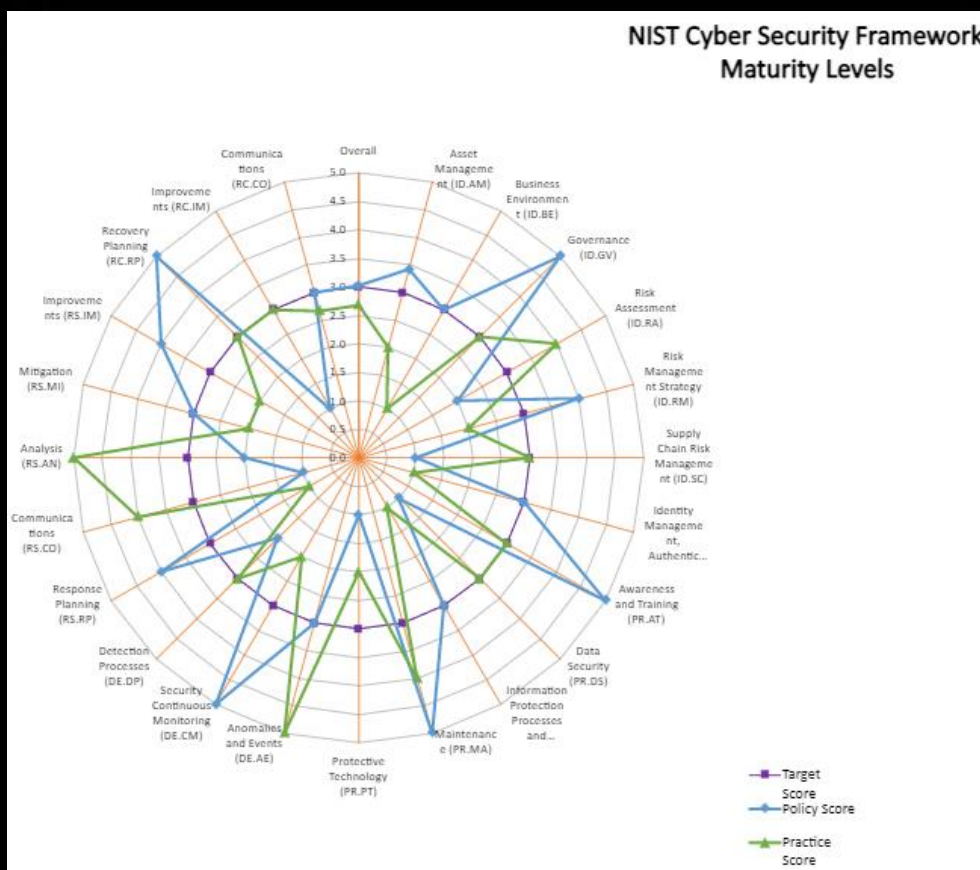
SWOT	PEOPLE	PROCESS	TOOLS
Strength	Experienced Engineers	GRC Policies	Inventory and Asset Management
	Good communication skills	DFIR Plan and Playbooks	XDR
	Strong leadership	TVM Playbook	Risk Register and Patch Tracking
	Self-driven professionals	VAPT Program	Scanner and Tester
	Proactive Analysts	CIS Benchmark	Identity and Access Management
Weakness	Burn-out	Bureaucratic process	No ticketing system
	Lack of R&D experience	Absence of security assessment questionnaire	Not properly use of CTI platform
	Too technical but less on presentation skills	Lack of security controls and policies	Absence of Asset and inventory tool
	Reactive attitude	No proper channel for disseminating intelligence	Complex EDR solution to operate
	Absence of adversarial mindset	No crisis management plan	Not fully implemented WAF on external facing assets
Opportunity	Sharpen presentation skills	Conduct SWOT analysis	Tighten application control
	Cross-training among team	Adopt purple teaming	Implement MFA
	Conduct technical tabletop exercise within the CyOps team	Conduct scenario-based tabletop exercise with stakeholders	Recalibrate use cases for detection and prevention tools
	Attend cyber range or capture the flag	Use risk registry for tracking unpatched assets and tech-stacks	Operationalize threat hunting program
	Conduct bi-yearly team building	Assess overall CyOps posture with NIST or MITRE framework	Refer to CIS hardening best practices
Threat	Short turnover	Further damage during incident breach	No visibility of the network anomalous traffic
	Skills shortage of experienced analysts	Supply chain monitoring and audit	Prone to DDOS attack
	Fast-faced threat landscape to cope	Untracked residual risk	High risk of Ransomware breach
	Accidental manager but no prior operational experience	Untracked inherited risk	Sensitive data leak exposures
	Insider threat	Supply chain risk	Data loss

CHAPTER 3

CYOPS MATURITY ASSESSMENT

The CISO has 3 personas in the author's opinion and observations which the majority may subconsciously not be aware of as their mindsets have shifted to business focus only and delegated everything to the next high-ranking officer. And in many companies, they split these roles instead of just a single point of failure; Technical (TISO), Business (BISO), and Strategic (SISO) information security officer.

The purpose of this assessment and the succeeding maturity measurements is not to reinvent the wheel but reintroduce their existence and to be utilized by the CISO according to the 3 roles mentioned. Thus, the blind spots are addressed during their first 90 days when joining an organization or building the cybersecurity operations (CyOps) and achieved industry compliances like ISO 27001 and others.



Download link: [NIST-CSF-Maturity-Tool-v2.0.xlsx](#)

Sha-256 Hash: e26ae5d616ec12aff89033ba5761098cf3c76f1ee9429638882b48fa9100285e

Malware Check: [VirusTotal](#) -

[e26ae5d616ec12aff89033ba5761098cf3c76f1ee9429638882b48fa9100285e](#)

CHAPTER 4

OPERATIONALIZING DFIR PROGRAM IN IT AND ICS/OT

It is a known strategy that when a CISO hires for a digital forensics and incident response (DFIR) analyst, is they look for a principal calibre; not just a level 3 security operations center (SOC). The experiences and mindsets are very much distinct. Building the DFIR program from scratch is not an easy task. It is even more pressured if the requirement is to operationalize it during your first 90 days of joining the company. Without prior experience in creating the following: IR plan, IR playbooks, tabletop exercise (TTX), threat modeling, compromise assessment, IR maturity assessment, project management, and business cases for procuring security solutions.

This program is the alter-ego of the CISO in technical aspects. The “Marines” in the cybersecurity world. Advisor to the defense-in-depth strategy. In some organizations, this is separate from the SOC and instead belongs to the computer emergency response team (CERT) together with the cyber threat intelligence (CTI). DFIR analyst is all-in-one in many cases – the SOC, threat hunter, threat intel, forensics, application engineer, application red teamer, technical project manager, and defense strategist. The organization should treasure if they lucky enough to find a unicorn.

In establishing a DFIR capability, the best practices is to align the program with the SP 800-61 Rev. 2, Computer Security Incident Handling Guide for the enterprise IT and SP 800-82 Rev. 2, Guide to Industrial Control Systems (ICS) Security for the OT.

Whilst there are plenty of IR plan templates that can be searched over the Internet, it is good to have a RACIS matrix (responsibility, accountability, consulted, informed, support) under the “Roles and Responsibility” section and get a buy-in among the stakeholders to make sure the everyone is clear on their respective jobs when a breach happens.

It is also important to adopt the NIST framework as a model to well define each incident phase from Detection to Reporting so it would be clear and organized during the crisis management inside the cyberwar room. At the end of the day, the key performance indicator (KPI) of a DFIR is time and speed in all matters.

Since it is common for enterprise IT to have a reference on the IR playbook, below is a sample template for OT cybersecurity IR that can be modified and used according to the ICS's unique environment. Nothing is a one-size-fits-all solution, and no one can tell that they are an “expert” in the OT world. Hence, delusional .

ICS/OT Incident Response

Playbook Objective

This playbook covers quick guide for handling specific cybersecurity related incidents:

- Denial of Control Action
- Control Devices Reprogrammed
- Spoofed System Status Information
- Control Logic Manipulation
- Safety Systems Modified
- Malware on Control Systems
- Vulnerability Scanner Incidents
- Penetration Testing Incident
- CCTV Attack
- Cyber-Intrusions
- Wireless Telegraph Hacking

The main objective is to improve the speed and efficiency of response actions and decisions to minimize the impact of a cyber incident on business functions and Data Center operations. Below are the targeted devices running on both Windows and Linux Operating Systems for this IR playbook.

- HMI
- Data Historian
- BMS
- EMS
- SCADA
- RTU
- CCTV
- *Edge for IIoT devices*
- *PLC (microcontroller - I/O's) – refer to the PCAP or NetFlow for network forensics.*

Notification and Support

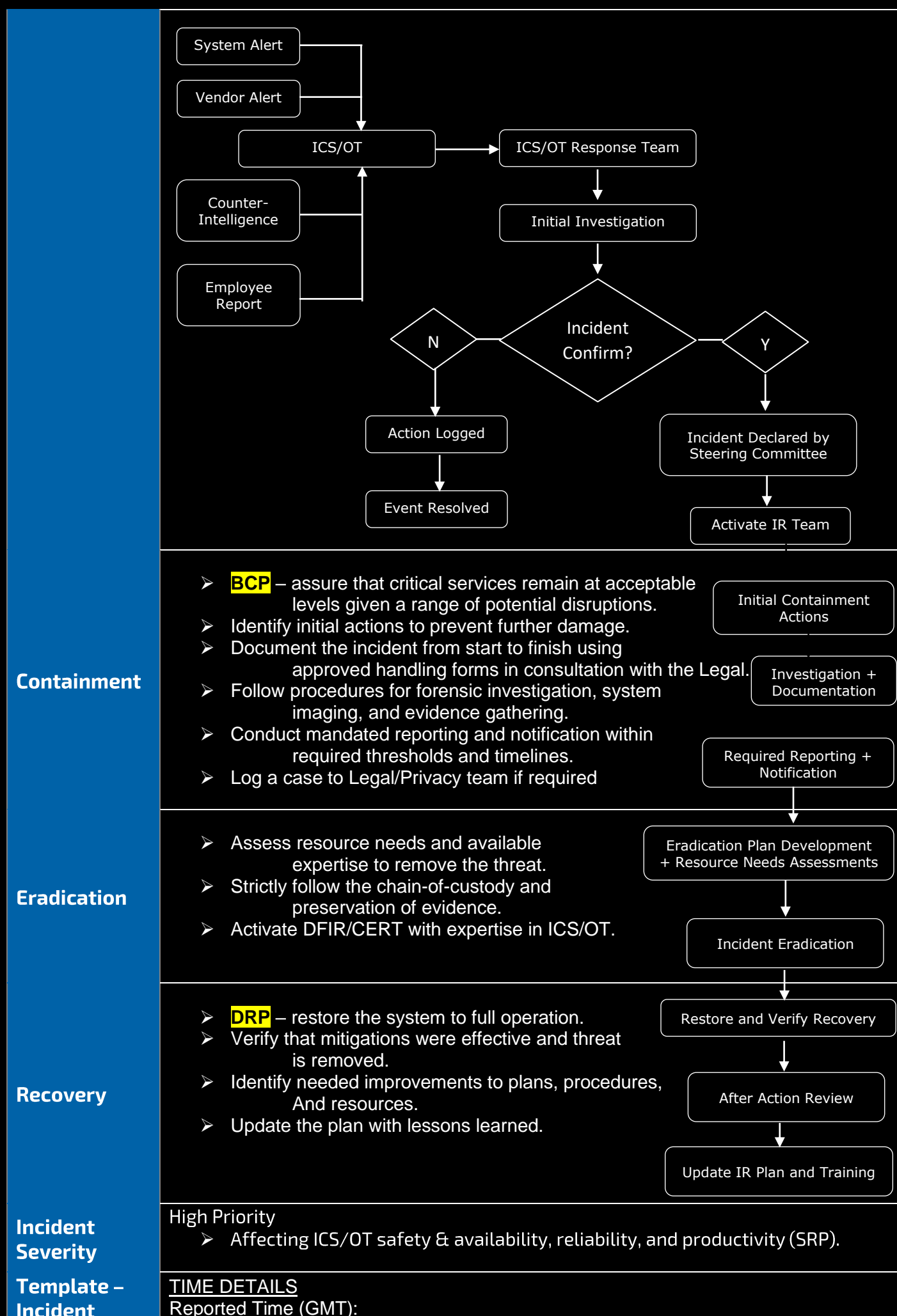
- Global HelpDesk
- Global Leadership, Local ICS/OT Director and Functional Team
- OEM Designated Support Engineer
- Vendor Service Provider
- Legal Team
- Public Relations Officer
- CERT Director
- SOC Director
- CISO
- IR Retainer
- Steering Committee

Preparation


- Staff expertise in handling cybersecurity incidents inside the ICS/OT – both CyOps and Control Engineer.
- 24/7 availability for critical staff.
- Updated contact list for response personnel and partners.
- Compile key documentation of Business-Critical networks and systems.
- Identify response partners and establish mutual assistance agreements.
- Updated technical response procedures for Incident Handling.
- Updated BCP and DRP
- Cyber War Room
- User Awareness and Training

Detection & Analysis

- Track and assess threat and vulnerability intelligence.
- Report cyber threats and suspicious activity alerts to the IR and ICS/OT director.
- Declare and classify the cyber incident.
- Alert and activate the CERT and/or IR team.



Investigation Summary Report	Method of detection:
	Notification source:
	Event Time (GMT):
	<u>SUMMARY</u>
	Threat Type: TITLE HERE
	Receiver:
	Sender:
	<u>ANALYSIS</u>
	-
	<u>RECOMMENDED ACTION</u>
	-

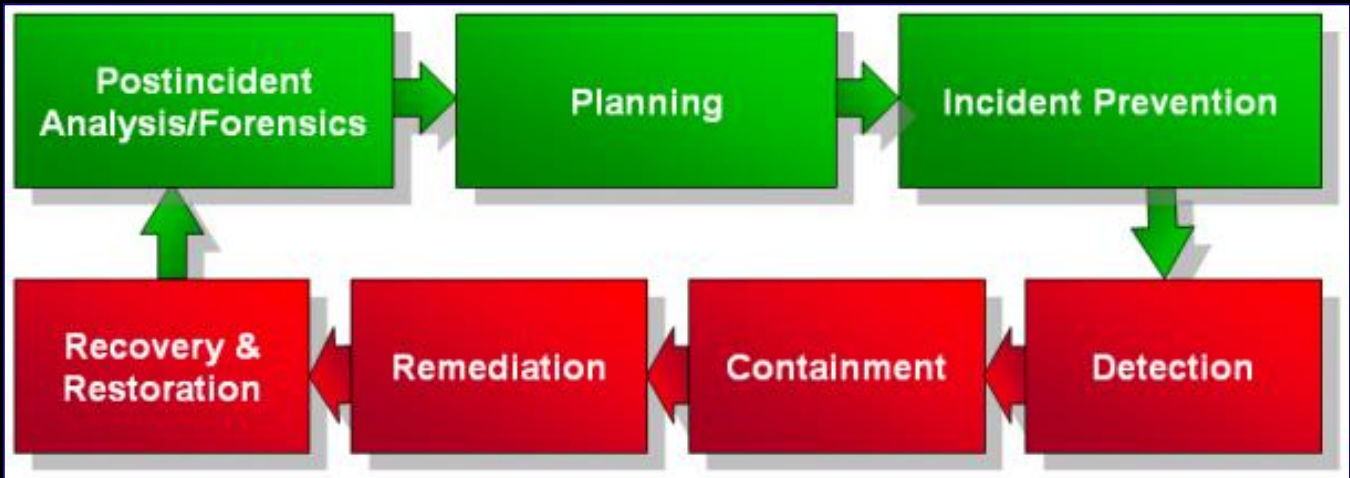


It is highly advised that using this template needs a thorough counterchecking with the OT cybersecurity and must be aligned with their BCP and DRP. Thus, it is highlighted on the workflow diagram.

Another good reference for developing IR in ICS is from the US-CERT which can be downloaded here: [Developing an Industrial Control Systems Cybersecurity Incident Response Capability \(cisa.gov\)](https://www.cisa.gov/developing-an-industrial-control-systems-cybersecurity-incident-response-capability).

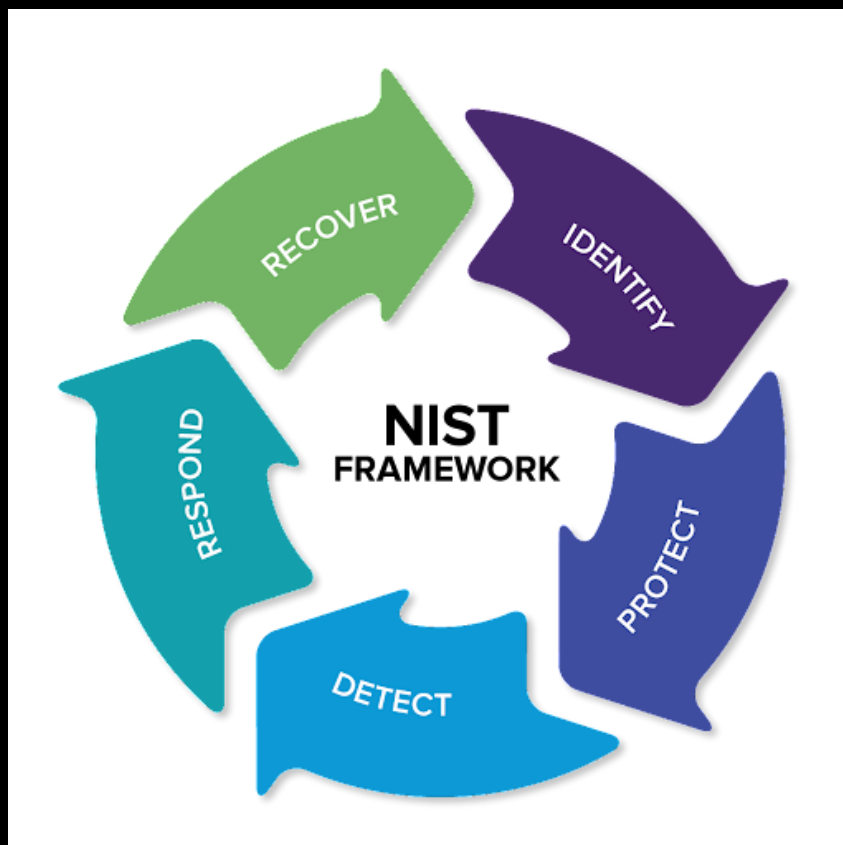
A16	Information security incident management	
A16.1	Management of information security incidents & improvements	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.
A16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.
A16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.
A16.1.3	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.
A16.1.4	Assessment of and decision on information security events	Information security events shall be assessed, and it shall be decided if they are to be classified as information security incidents.
A16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.
A16.1.6	Learning from information security incidents	Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.

A16.1.7	Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence.
---------	------------------------	---



Screenshot taken from US-CERT

Lastly, if the organization is applying for an ISO 27001 compliance, below are the basic requirements that need to be produced to pass the certification as of March 2022.



CHAPTER 5

OPERATIONALIZING NEXGEN-SOC

Security operations center or SOC is the first level of defense for detection and response. They validate the alerts to categorize events versus real incidents. Triage on the severity of the impact based on the asset's criticality and escalate to different levels depending on their scope of work and capabilities. SOC follows the IR plan and playbooks that the DFIR established. And most of the SOC set-up are 24x7 models for continuous monitoring.

This is also the entry point of many of the IT professionals who wanted to shift their careers to cybersecurity. Level 1 usually does not require having any security certifications but having the willingness to learn and operational mindset are better than someone who has certifications but with a reactive attitude. A nail needs to be hammered before it digs deeper.

SOC also consumes any relevant threat intelligence from the CTI team to action through either for threat hunting or countermeasures such as blacklisting and detection capabilities with security information and event management (SIEM) or endpoint detection and response (EDR) solutions for proactive measures.



Building a SOC is expensive as an organization needs to consider putting up a spacious cyber control room and renting an office intended only for that team with the follow-the-sun model. That is why many start-up companies or even small and medium enterprises, the DFIR program is enough with on-call support during incidents to meet the minimum budget expenditures. Unless they are applying for cyber insurance then they may want to do case studies of a managed security service providers (MSSP) for outsourced SOC.

When looking for a standard framework for hiring cybersecurity analysts based from skillset, here is the extensive guidance from CISA – [NICE Cybersecurity Workforce Framework Work Roles | National Initiative for Cybersecurity Careers and Studies \(cisa.gov\)](https://www.cisa.gov/nice).

The next generation SOC is a cyber threat intelligence (CTI) driven operation as mentioned earlier. Unlike the typical SOC who just plays a “whack-a-mole” game and is IOC-centric. Today in a very fast pacing sophisticated attack from APTs and state-sponsored threat actors, SOC should be on top of the game at least even during their shift hours as adversaries from different directions never sleep even until they achieved their goals.

It is a given fact that no security solutions are 100% bulletproof even they bragged about their artificial intelligence (AI) and machine learning (ML) technology. Many times, the even “known” malware is “unknown” to them and hence the reason why organizations are still being a breach.

THREAT INTELLIGENCE-DRIVEN SOC (aka NexGen-SOC)			
“Threat Hunting Known-Unknowns”			
➤ CTI = Context + Attribution + Action ➤ Context – clear picture of the urgency, relevance, and priority to the organization. ➤ Attribution – this answers the Why and the Who behind the threat. ➤ Action – SOC to prioritize most valuable and relevant IOCs associated with the threat.			
	TACTICAL (No Context & Attribution)	OPERATIONAL (Applies Context & Attribution to Enable Action)	STRATEGICAL (Provides Context & Attribution to Enable Action)
DESCRIPTION	IOCs provided through CTI Platform's API integrated within the SIEM and SOAR	CTI to provide TTPs associated with APTs for effective Threat Hunting and Mitigations – this includes the artifact that has not been identified by the tools for enhancement	CTI to provide Bi-Monthly or Ad-Hoc basis on the organization Threat Landscape.
USE CASE	Updated and automated IOC feeds to SIEM and SOAR for real-time detection & prevention.	SOC analysts get notified of the latest threats relevant to organization for both APT and TTPs. Zero Day or unidentified malware by organization tools.	SOC/IR leaders to review and have better understanding on the APT's motivation, tradecraft, and sophistication. Make more informed business decision and provide alignment on SOC program's strategy and real-world risk.
BENEFITS	<ul style="list-style-type: none"> Automated and constantly updated in near-real time. Less or no false-positive alerts. 	<ul style="list-style-type: none"> Guide SOC analysts' actions. Driven by near-real time threat, collaboration and expert analysis Informed on the latest/emerging threats. 	<ul style="list-style-type: none"> Empowers SOC team and leadership decision-making Help communicate the urgency of Cyber-Security issues to the CISO and leadership.



Another emphasis on this NexGen-SOC is a shift of the mindsets not only the analyst but the lead or manager itself. These roles are somehow still technical on high-level and not just traditional managing shift rotation, workloads, training budget allocations, and planning team-building. They should be the first ones who are stepping-in in on the cyber battlefield and the last ones stepping out. They should lead by examples so the analysts would be inspired on catching “known-unknowns” to reduce the dwell-time.

These are the new “Spartans” of this era. The frontliners of cybersecurity. Only the brave!

CHAPTER 6

XDR BUSINESS CASES

There is too much hype currently popping up regarding the endpoint security solution that most of the vendors are now adopting – the Extended Detection and Response (XDR). Some of them are in the cloud (SaaS) and some on-premises. Some are network appliance dependent for network detection and response (NDR) capabilities, and some are just agent-based that covers the network traffic analysis (NTA).

Endpoint detection and response (EDR) is not yet obsolete. Its features are focused mainly on the exploits and anomalous activities residing on the host itself. Whilst the NDR takes care of the anomalous traffic on the network for detection and prevention.

Other organizations prioritized security information and event management (SIEM) over EDR and NDR but then realizes soon the absence of prevention, response, remediation, and recovery –which are containment and forensics to be specific. This is even security orchestration and automated response (SOAR) solutions are relying too upon.

Thus, the XDR tries to address both network and endpoint security solutions to have complete visibility during breach investigations with a bonus of users and entity behavioral analytics (EUBA). In short, hybrid.

In more than 7 years of solid experience of the author on conducting proof-of-concept (POC) to different EDR and a few XDR solution providers in the market for the digital forensics and incident response (DFIR) program, he has built a solid business and use cases to debunk the vendor's marketing ads through thorough testing and continuous red teaming even after the acquisition.

This business and use cases are meant to be the guiding principle for the organizations who are looking into the XDR solution and explicitly being advised to test them by running the customized exploits, live ransomware, zero-day exploits, leaving of the land binaries and scripts (LoLBAS), and network-based attacks – on an isolated host in case of false-negative or missed detection and prevention.

Note that this high-level business and use cases are mapped with the SP 800-61 revised 2 of the NIST framework.

ID	FEATURES	DESCRIPTION
1	PRODUCT ADAPTABILITY	Multi-Platform Support both IT and OT (Embedded OS, Win7, Win10, Win11, Linux, MacOS, iOS, Android)
		System Performance and Resource Utilization (CPU, Memory, Disk, Network)
		Ease of Deployment & Upgrade (supported by Intune, GPO, SCCM, JAMF, Ansible, etc.)
		Cloud Console Management (SaaS)
		Intuitive (user-friendly and one-click solution)
		Multi-Integration Support and Able to Co-Exist with Other Security Solution (AV, EPP, DLP, etc.)
2	PROTECTION From THREATS	Advanced Threat Prevention (AI, ML)
		Always on Protection (Online and Offline)
		Built-In Threat Intelligence (OSINT and Commercial)
		Quarantine Malicious Non-PE Files (MS-Office, PDF, ISO, Zip, 7zip, Images, Video, etc.)
		Device Control
3	DETECTION Of THREATS	Behavioural-Based Detection of Threats
		Signature-based Detection of Threats (Built-In NextGen AV)
		Real-Time Monitoring System Activity
		Static Analysis
		Sandbox Analyzer for Dynamic Analysis
		Fuzzy Hashing
		Unusual Files and Registry Entries
		LoLBaS / LoLBin
		Fileless Malware
		Stegware
		Polymorphic Malware
		Metamorphic Malware
		Ransomware
		Data Wiper
		File Integrity Monitoring
		User and Entity Behavioural Analytics
		Network Anomalous Activities (Data Exfiltration, Lateral, Movement, Privileged Escalation)
4	RESPONSE To THREATS	Endpoint Visibility and Control (Asset Inventory)
		Dynamic Process Termination
		Forensics Capability - Full Memory Acquisition
		Forensics Capability - Full Disk Data Acquisition
		Forensics Capability - Memory Dump Analysis
		Forensics Capability - Data Dump Analysis
		Network Containment
		Process Containment
		Download and Manually Analyse the File
5	RECOVER from INCIDENTS	Run On-Demand AV
		Revert Changes in Registry Edit
		Revert Changes on Files
		Revert Changes on System
6	ADDITIONAL FEATURES	Supports YARA Rules
		Supports Sigma Rules
		Unmanage Asset Auto-Discovery

		Built-In Automated Response with Playbook
		Built-In Vulnerability Management
7	SUPPORT On STANDARD SUBSCRIPTION	24x7 On Call Support
		24x7 On Email Support
		One Time Service Cost

During the proof of concept (POC) of the prospective XDR solution, it is good to test and validate them through the tactics, techniques, and procedures (TTPs) mapped below from the MITRE ATT&CK framework (v.10).

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Network Information (T1039) Active Scanning (T1043)	Compromise Accounts (T1078)	Valid Accounts (T1078) Trusted Relationship (T1078) Supply Chain Compromise (T1195) Replication Through Removable Media (T1195) Phishing (T1195) Hardware Additions (T1195) External Remote Services (T1195) Exploit Public-Facing Application (T1195) Drive-by Compromise (T1195)	Windows Management Instrumentation (T1047) User Execution (T1028) System Services (T1028) Software Deployment Tools (T1028) Shared Modules (T1028) Scheduled Task/Job (T1049) Native API (T1049) Inter-Process Communication (T1049) Exploitation for Client Execution (T1049) Deploy Container (T1049)	Valid Accounts (T1078) Server Software Component (T1078) Scheduled Task/Job (T1049) Task Scheduler (T1049) Office Application Startup (T1049) Modify Authentication Process (T1049) Hijack Execution Flow (T1049) External Remote Services (T1049) Create or Modify System Process (T1049) Container Administration Command (T1049) Command and Scripting Interpreter (T1049)	Valid Accounts (T1078) Scheduled Task/Job (T1049) Process Injection (T1055) Hijack Execution (T1049) Event Triggered Execution (T1049) Escape to Host (T1049) Domain Policy Modification (T1049) Create or Modify System Process (T1049) Boot or Logon Initialization Script (T1049) Browser Extensions (T1049) Access Token Manipulation (T1049) Abuse Elevation Control Mechanism (T1049) BITS Jobs (T1049) Account Manipulation (T1049)	XSL Script Processing (T1055) Virtualization/Sandbox Evasion (T1055) Steal or Forge Kerberos Tickets (T1055) Steal Application Access Token (T1055) OS Credential Dumping (T1055) Network Sniffing (T1055) Modify Authentication Process (T1055) Signed Script Proxy Execution (T1055) Signed Binary Proxy Execution (T1055) Rootkit (T1055) Process Injection (T1055) Priv. Obj. Desc. (T1055) Obfuscated Files or Information (T1055) Modify System Image (T1055) Modify Registry (T1055) Modify Cloud Compute Infrastructure (T1055) Modify Authentication Process (T1055) Masquerading (T1055) Indicator Removal on Host (T1055) Impair Defenses (T1055) Hijack Execution Flow (T1055) File and Directory Permissions Modification (T1055) Exploitation for Defense Evasion (T1055) Domain Policy Modification (T1055) Deploy Container (T1055) Deobfuscate/Decode Files or Information (T1055) Build Image on Host (T1055) BITS Jobs (T1055) Access Token Manipulation (T1055)	Unsecured Credentials (T1055) Steal or Forge Kerberos Tickets (T1055) Steal Application Access Token (T1055) OS Credential Dumping (T1055) Network Sniffing (T1055) Modify Authentication Process (T1055) Forge Web Credentials (T1055) Exploitation for Credential Access (T1055) Brute Force (T1055) Adversary-in-the-Middle (T1055)	Virtualization/Sandbox Evasion (T1055) System Network Connections Discovery (T1055) System Network Configuration Discovery (T1055) Query Registry (T1055) Process Discovery (T1055) Network Share Discovery (T1055) Network Service Scanning (T1055) Container and Resource Discovery (T1055) Cloud Storage Object Discovery (T1055) Cloud Service Dashboard Discovery (T1055) Cloud Infrastructure Discovery (T1055)	Use Alternate Authentication Material (T1055) Taint Shared Content (T1055) Software Deployment Tools (T1055) Replication Through Removable Media (T1055) Remote Services (T1055) Remote Service Session Hijacking (T1055) Lateral Tool Transfer (T1055) Exploitation of Remote Services (T1055)	Email Collection (T1055) Data from Network Shared Drive (T1055) Taint Shared Content (T1055) Data from Information Repositories (T1055) Data from Cloud Storage Object (T1055) Browser Session Hijacking (T1055) Automated Collection (T1055) Adversary-in-the-Middle (T1055)	Web Service (T1055) Remote Access Software (T1055) Proxy (T1055) Protocol Tunneling (T1055) Non-Standard Port (T1055) Non-Application Layer Protocol (T1055) Multi-Stage Channels (T1055) Ingress Tool Transfer (T1055) Fallback Channels (T1055) Encrypted Channel (T1055) Dynamic Resolution (T1055) Data Obfuscation (T1055) Data Encoding (T1055) Application Layer Protocol (T1055)	Transfer Data to Cloud Account (T1055) Scheduled Transfer (T1055) Softlifting Over Physical Medium (T1055) Exfiltration Over Other Network Medium (T1055) Exfiltration Over C2 Channel (T1055) Exfiltration Over Alternative Protocol (T1055) Data Transfer Size Limits (T1055)	System Shutdown/Reboot (T1055) Service Stop (T1055) Resource Hijacking (T1055) Disk Wipe (T1055) Data Manipulation (T1055) Data Encrypted for Impact (T1055)

The printable (xls) and raw (json) versions of this map are downloadable from the author's github: [strainerart/xdr_usecases: Extended Detection and Response \(XDR\) Use Cases \(github.com\)](https://github.com/strainerart/xdr_usecases: Extended Detection and Response (XDR) Use Cases)

CHAPTER 7

DIGITAL FORENSICS TOOL BUSINESS CASES



Few emerging Forensics investigators nowadays merely rely on the popularity of the tools and by default, commercial toys are the first choice. Sadly, the managers and leaders do not challenge this decision-making on both use cases and return of investment (ROI) to the company.

Before, it is understood that the court of law only accepts a certain tool because of the capabilities of preserving evidence. But today, even free and open-source software (FOSS) and freeware have that feature too. Hence, everything falls on the standard methodologies of forensics investigations – identification, preservation, analysis, documentation, and reporting.

Based on the author's experience on the different forensics tools used – below are the use cases that an organization can utilize to test against different vendors for acquisition with a great value aside from the yearly subscription.

ID	FEATURES
1	Acquisition and Analysis
2	Preview and Acquire Disk Image
3	Memory Forensics
4	Cloud Forensics
5	Network Forensics
6	Built-In threat Intelligence to Identify Known IOCs
7	Registry Analysis
8	Web Browser Analysis
9	Identify Steganography
10	Extensive Automation and Scripting
11	Automatic Report Generation
12	Web and Email Artifacts
13	Social Media Artifacts
14	Backend Database
15	Database Forensics
16	Examine all Major Filesystems
17	Examine Digital Evidence from Windows
18	Examine Digital Evidence from MacOS
19	Examine Digital Evidence from Linux
20	Bruteforce Password Protected Files
21	Integrated Tools and Viewers
22	Full Text Search with Multi-Lingual Capabilities
23	Integrated AI/ML Tools for Image and Video Analytics

CHAPTER 8

OPERATIONALIZING CTI PROGRAM

When we asked a consultant or security vendors about how to operationalize a cyber threat intelligence (CTI) program, most if not all, will tell you about the “maturity” of your cybersecurity.

When I was tasked and given an opportunity to build the program from scratch from the author’s first experienced, it was not the case from what many “experts” were claiming. From asset intelligence to security risk scorecard (SRS) up to the web application firewall (WAF), all are existing including 5 different CTI platforms from both IT and OT – and yet it was not that successful in general.

On the second time I operationalized CTI with a different organization, there were no tools but only the people and process were established with the help of the open-source intelligence (OSInt). Incorporate the program to the zero-day exploited vulnerabilities under the threat and vulnerability management (TVM), and DFIR.

So, to debunk the response template from those security consultants and vendors, the “maturity” that an organization need is not the tools but the people’s “mindset” with less bureaucracy on the process especially when the defense readiness condition arises to level 4 (DefCon 4); an imminent threat is on-going.

Just imagine that your organization is under coordinated attack with both distributed denial of service (DDoS) on your public-facing assets and ransomware has been detected by your EDR solution; the CTI requested to block the geographical IP address from a communist country and your firewall engineers asked you to raise a ticket for change? Emergency response cannot be later or tomorrow but now. That is how and why the CTI program is failing even proper communication and coordination are in place, at least in the author’s real-life corporate operational experienced.

A good e-book that an aspiring CTI analyst could start reading is the security-intelligence-handbook-third-edition.pdf. It gives a clear insight into the actionable intelligence for different stakeholders strategically, operationally, tactically, and technically. From the last time I read the hard copy of the second edition, it was vendor-neutral.

Getting someone who can operationalize the CTI program in a 30 to 90 days timeline is a tough but fulfilling challenge. Someone who has exposure to the red and blue teaming roles and is conversant in communication and presentation skills is perfect for this role. It is good if the candidate has a

military background but for someone who has done being an attacker and defender in the corporate industry is even better as they know the ins and outs of an adversary's mind in the cyber world.

Lastly, a good CTI program should have a weekly global awareness campaign that is relevant to the organization. It should provide context and recommended actions for the related stakeholders. Here are some of the references that an analyst can start with to cover all aspects of threat intelligence; strategic, operational, technical, and tactical.

TOP THREAT ACTORS TARGETING ICS/SCADA

ADVERSARY	ATTACK VECTOR	TARGETED INDUSTRY	OPERATION	MALWARE LINK	EXPLOITED CVE
Black Art123	Spear Phishing	Energy	Ransomware-as-a-Service	WiperCrypto	CVE-1234-567

TOP 10 EXPLOITED CVEs RELEVANT TO XYZ COMPANY

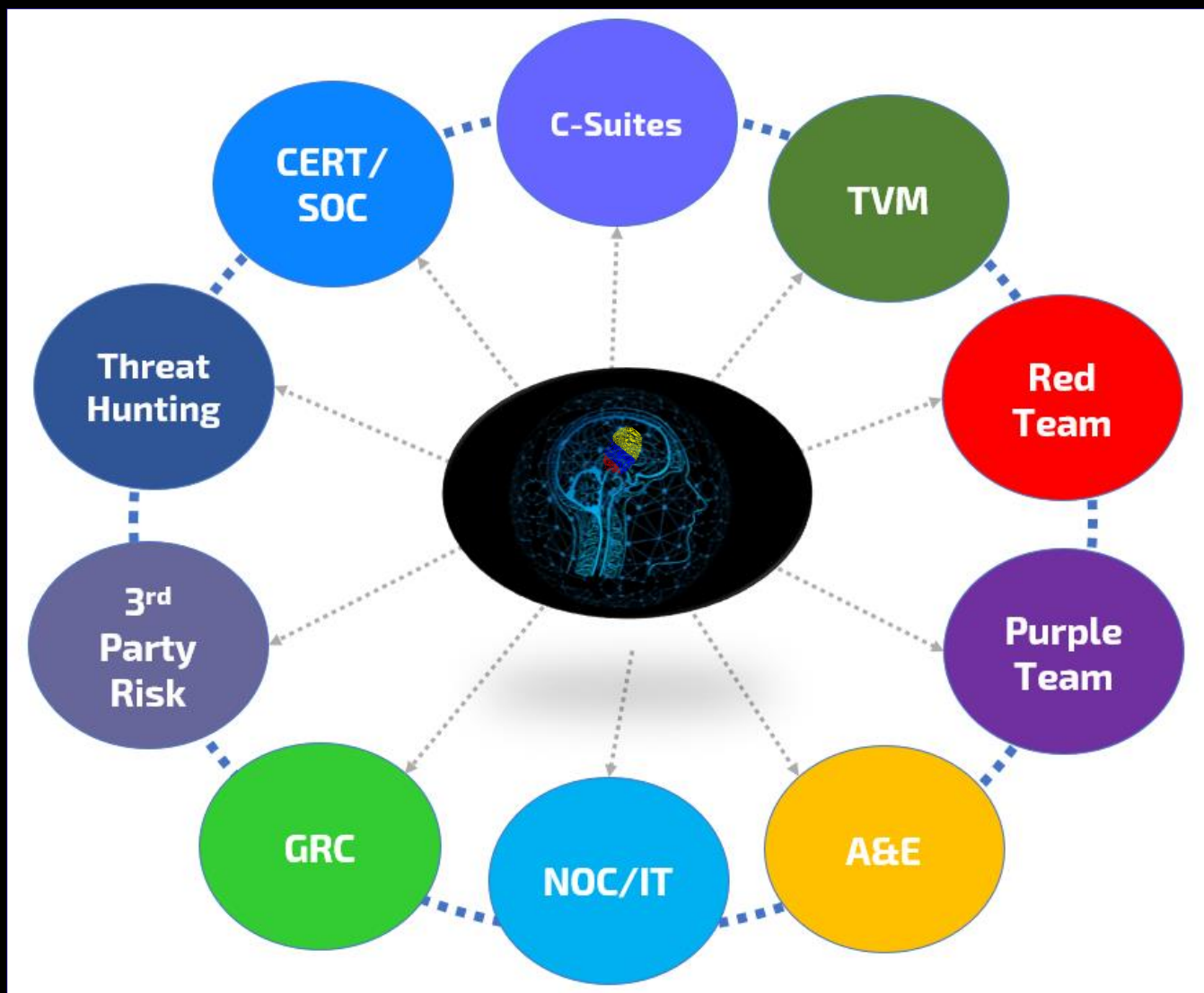
VULNERABILITY ID	THREAT TYPE	DESCRIPTION	NUMBER of EXPOSED ASSETS	DOMAIN	THREAT ACTOR LINK
CVE-4321-765	Remote Code Execution	Log21x exploitation	1,978	ICS/SCADA	White JEN456

The analysts should add the mitigation strategy aside from giving the links of the software patch to make it actionable for relevant parties.

Adding the relevant security breaches to the weekly global awareness for both the IT and OT will add value to the CTI program, especially if the analyst will include the type of defense readiness condition (DefCon) level for the SOC and DFIR's threat hunting. If the organization has Red Team or Purple Teaming program, this is also a good source of their adversarial emulation exercise.

An internal portal for CTI is also one good indicator and visibility of the program that gives continuous awareness on the global threat landscape in cybersecurity for both the IT and OT.

To be more precise on who are the stakeholders or beneficiaries of the CTI program, here are the ranges of its functionalities that covers the strategic, operational, technical, and tactical.



To reiterate, CTI is not just about managing a platform and sharing indicators of compromise (IOCs) and indicators of attack (IOAs) to the SOC team. It is knowing the unknown by deep diving in both the dark and shallow web to prepare the organizations against advanced persistent threats (APTs) through countermeasures and DFIR, reducing risk against exploited vulnerabilities and zero-days through the TVM, and compromise or breach assessments through threat hunting. Many call this “counter-intelligence”.



CHAPTER 9

CTI PLATFORM BUSINESS CASES

Cyber threat intelligence (CTI) solution providers will claim that they covered everything and that they are on top of the game among other competitors, Similar to the EDR and XDR solutions, many will brag that they are the best security vendors, and they are number 1 in the market. But, these CTI providers are just reactive as security advisories and news sites of providing breaches, common vulnerability and exploit (CVE) that prospective customers make-believe that they are really proactive.



Many tend to forget about the basic pillars of information and communication technology (ICT) – the people, process, and tool. And this is just a tool but behind that is the dedicated and tireless human who uses techniques on crawling the information for you from both the shallow and dark web.

When scouting for a CTI solution for investment, whether for integrating with the SIEM, SOAR, EDR, XDR, security operations, and other reasons; here are the factors to be considered for a minimum business and use cases must have needed to help the program fulfil its critical mission and vision on vendor selections through facilitating a proof-of-concept (POC) or proof-of-value (POV) instead of blindly choosing a tool that is based on hearsays, paid surveys, and fancy marketing presentations.

ID	FEATURES	DESCRIPTION
1	Evaluated Threat Intelligence	Balances both machine learning and human analysts
		Validates threats against a standardized information model
		Delivers only intelligence on specific threats to the organization
2	Strategic Threat Intelligence	Connects threat information directly to business operations
		Uses non-technical language to explain cyber risk
		Helps identify how best to direct cyber-related resources
3	Operational Threat Intelligence	Delivers insights on how threat actors conduct attacks
		Offers in-depth reports on tactics, techniques & procedures
		Provides specific threat mitigation recommendations
4	Comprehensive Threat Intelligence	Consolidates many threat data sources into one
		Provides insight into organization active threats via the Dark Web

		Includes external threats such as partners and supply chain
5	Personalized Threat Intelligence	Creates a tailored risk profile based on organization
		Alerts only to threats relevant to organization
		Provides specific mitigation recommendations
6	Practical Threat Intelligence	An immediate intel operation without additional staff
		Easy and affordable to implement without extra overhead
		Integrates with existing cybersecurity environment
		Integration - API that connects to SOAR, EDR and SIEM for tactical and technical intelligence
		Phishing Sites & Phishing Kits
		Brute Force Credentials Stuffing Tools
		Accounts for Sale / Credential Leak
		Leaked Documents
		Malicious Mobile Applications
		Malicious Desktop Applications
		Carding as a Service
		Fraudulent Tutorials & Services
		Fake VIP Accounts
		Leaked Codes
		Doppelganger Domains (Typosquatting)
		Threat Actors Tracking
		Most Active Threat Actors
		Latest and Exploitable CVEs including Zero-Day
		Command & Control
		Top 10 Cyber Attacks
		Negative Social Media Mention
		Takedown Services
		Third Party Monitoring

CHAPTER 10

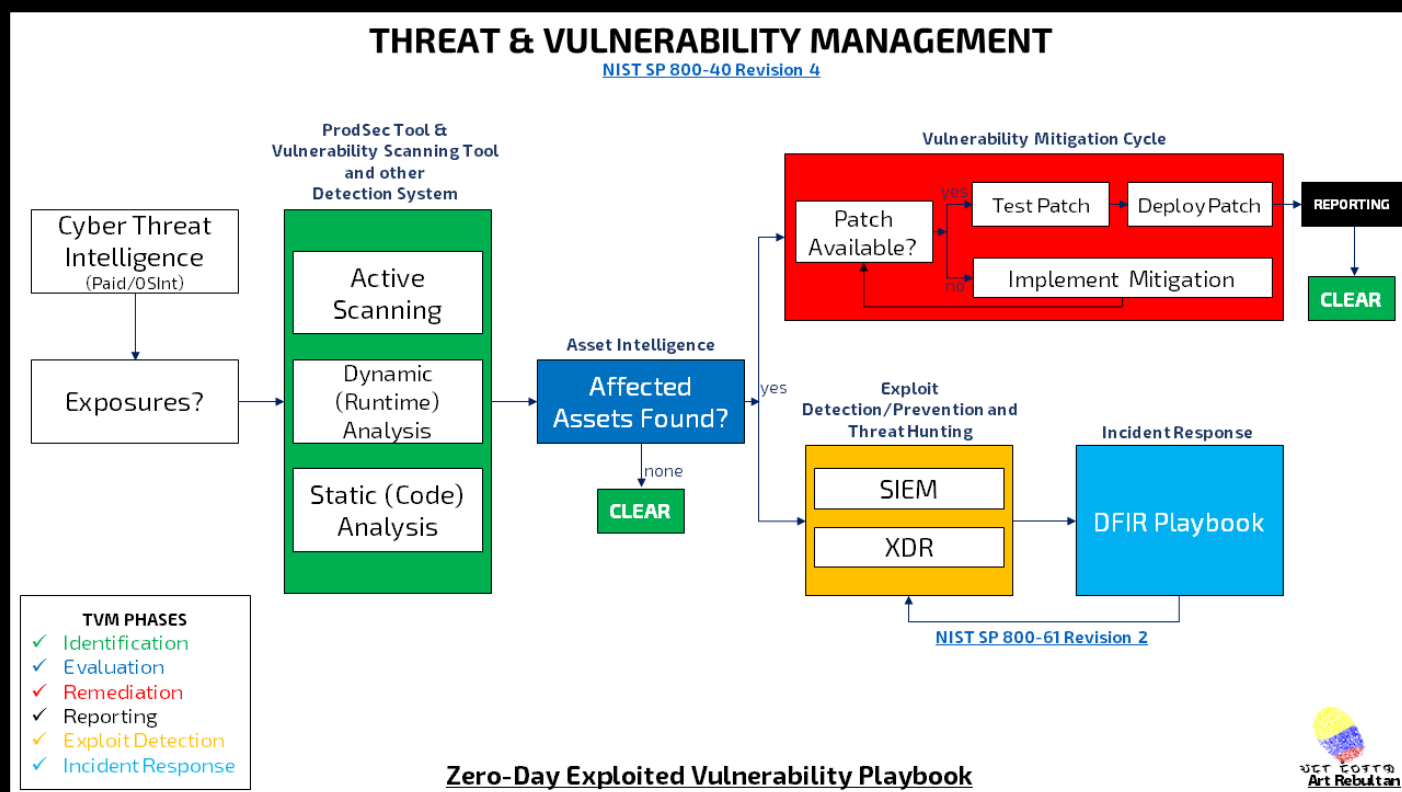
OPERATIONALIZING TVM PROGRAM

Reducing risk – as simple as that; the very mission of the threat and vulnerability management (TVM) program. Accountable for the risk registry for the current, inherited, and residual risks. Ensuring that all exploited assets that are accessible to the Internet and internal devices with communication to the untrusted network are prioritized to be remediated against risk exposures.

Whilst technology is good to have, best practices are for the organizations to solidify the people and process first which the NIST have published a guide that TVM program could adopt, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4-draft.pdf>.

Another important entity that is beneficial to the CISO and the TVM director is the process of handling Zero-Day exploits like Log4j vulnerability where many of the organizations across the globe were caught in surprise and did not handle risk mitigation well.

The Center for Internet Security (NIS), [Log4j Zero-Day Vulnerability Response](#), and some government security advisors released a similar workflow below.



Notice on the playbook above, 6 domains were working and coordinated together to mitigate similar risks more effectively. Thus, this visualizes the defense-in-depth on the people, process, and tools in the exemptions of the network segmentation or the overly hyped “zero trust”.

1. CTI gathers strategic, operational, and technical intelligence for internal sharing and defense readiness condition level (DefCon).
2. Product security and TVM itself refer to any asset exposures from various scanning tools or configuration management database (CMDB).
3. Patch management team to test the software version update or upgrade in non-production first if the patch is available prior to deployment in the production hosts.
4. SOC for continuous monitoring and threat hunting of the IOAs and backlisting of IOCs in the network. They may also work with the Architecture and Engineering for countermeasures on the WAF as the first layer of defense against remote code executions (RCE).
5. DFIR or CERT is on standby for any breach or compromised hosts to carry on the IR playbooks for containment, eradication, remediation, and recovery for business-as-usual (BAU).

The organization may utilize free and open-source software (FOSS) for this program targeting the IT network if they have enough budget to get acquire a security solution like risk-based vulnerability management (RBVM) tools.

1. [OpenVAS - Open Vulnerability Assessment Scanner](#)
2. [Burp Suite - Application Security Testing Software](#)
3. [OWASP ZAP](#)
4. [Tsunami Network Scanner](#)
5. [Nmap Security Scanner for Linux/Mac/Windows](#)

Although NMAP is being used even by the red teamers for scanning an OT device, it is highly advised to use the non-intrusive parameters and should only be tested thoroughly first in non-production before jeopardizing the safety and availability, reliability, and productivity in the ICS network.

CHAPTER 11

OPERATIONALIZING INTERNAL BUG BOUNTY HUNTING PROGRAM

The sole objective of the internal bug bounty hunting initiative is to encourage responsible reporting within the organization's community of suspected vulnerabilities or flaws in the whole IT services, security, and application systems that may potentially affect the company's critical assets.

The different firms have different business cases. Here are the few considerations to buy-in with the C-Suites instead of straight going to the external bug bounty hunting for start-ups or SMEs:

1. Faster and continuous vulnerability identification.
2. Improve product security.
3. Cost efficient is equal to low investment with high return of investment (ROI).
4. Confidential source code stays within the organization.
5. Attract diverse expert audience within the company.
6. Build security-centric community.
7. Provide 360 asset visibility.



In some instances, there could be agony from the stakeholders and product owners about this program, it is very important to establish a scope and limitations:

1. Mutual non-disclosure agreement policy between the employer and the employees. Usually, this is by default under the confidentiality clause being signed upon joining the company.
2. No assets shall be jeopardized in any way of their confidentiality, integrity, availability, safety, reliability, and productivity (CIA/SRP) for both hardware and software.
3. All systems should remain up and running whether static or dynamic site.
4. All contents should remain unchanged either video, graphical, text, or codes.

In all activities in cybersecurity, having a drawback is no exemption like below:

1. Time consuming.
2. Resource constraints.
3. Analyst's burn-out.



Thus, here are some of the recommendations that can be applied to make this work:

1. The bug hunter itself should present the findings and show that it is reproducible. The program can borrow the same methodology from the external bug bounty platform or government CERTs.
2. Build a dedicated volunteer team or champion who is passionate about vulnerability assessment and penetration testing aside from within the cybersecurity team itself. An intern could also be an option.

Also, a standard reporting template should be imposed so the turn-around is quick and the findings are easily proved whether it's a false-positive or accurate.

Metrics and rewards are important spices of the bug bounty hunting program. This is the guiding expense value of the organization whether it is monetary based, a "swag", a recognition through certificate, or a company-wide announcement just to boost the morale of the bug hunter.

Here is a sample of where the program could start, and it can be modified according to the budget.

CVSS SEVERITY LEVEL	CVSS SCORE RANGE	SEVERITY MULTIPLIER	MONETARY REWARD
Informational	0	0	0
Low	0.1 – 3.9	25	\$2.50 – \$97.50
Medium	4.0 – 6.9	50	\$200 – \$345
High	7.0 – 8.9	75	\$525 – \$667.50
Critical	9.0 – 10.0	100	\$900 – \$1,000

Finally, the reporting structure and service level agreement (SLA) for remediation is also mandatory for this program. Else, the known bugs will just become an inherited risk or residual in the future. Again, it will be another cause of breach to the organization.

SEVERITY OF FINDINGS	DAYS TO FIX AFTER VALIDATION
Informational	None – risk registry
Low	1 Month
Medium	7 to 14 Days
High	3 to 4 Days
Critical	24 Hours



Picture credit to Scott Adams

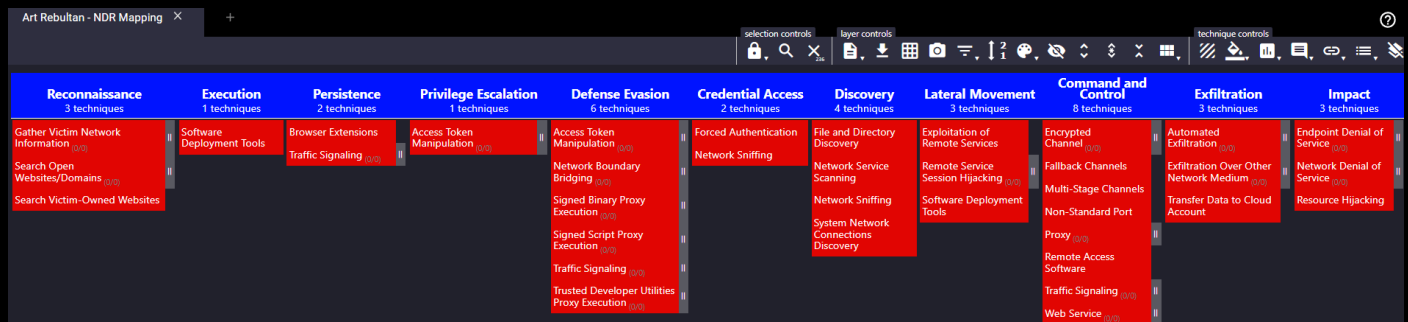
CHAPTER 12

ANNEX

Network Detection and Response (NDR) Business Cases

In a high-level visualization when a vendor demonstrates their SIEM and XDR tools, an analyst would not know that many of the network-based attacks will not be covered by those solutions unless you know what exactly the use case is.

Mapping the lists through the MITRE ATT&CK framework would provide the organization with a clear understanding of what their gaps really are. Thus, every penny spent on the budget allocated for the tools are worth the investments rather than dimly acquiring the technology based on popularity.



To download or view the JSON and XLSX files of this image, visit the author's GitHub page here: [Network Detection and Response \(NDR\) use cases.](#)

The baseline is good enough to test all bits and bytes of the NDR solution's providers so the analyst would not go wrong and will just focus on the vendor's support and investment cost.



Attack Surface Management Business Cases

In the usual threat and vulnerability management (TVM) program, it is important to have complete visibility of the organization's public-facing assets. Unfortunately, this is a challenge in a start-up or SME company.

Whilst open-source intelligence (OSInt) is a good tool to use even with the help of red teaming or penetration testing arsenals, still there will be an unknown asset that is yet to discover. So, the chief information security officer (CISO) or the TVM director may want to explore this technology.

The business and use cases for this may have overlapped with the vulnerability and penetration testing (VAPT) tool or the security risk scorecard (SRS) but it is not to be compared as apple-to-apple which a seasoned analyst can validate and confirm.

ID	FEATURES	DESCRIPTION
1	Create Comprehensive Visibility Through Graph-Based Mapping	Discover assets and cloud resources using a multitude of integrations and techniques. Identify partner and third-party relationships. Examine asset composition, technologies, and configurations in the wild.
2	Know when Assets Change to Stay Ahead of the Threat	Monitor organization's infrastructure in real time to detect changes and exposures. Build a safety net for cloud adoption and digital transformation.
3	Automatically Send Notification of Changes	Send an alert through email for any changes on the organization's risk exposures.
4	Automatically Send Notification of Newly Discovered Assets	Almost real-time notifications.
5	Empower Security Operations to Mitigate Real-World Threats	Automatically apply SecOps expertise and intelligence to our attack surface. Know what's exposed.
6	Checks Software for Vulnerabilities	Provide an accurate CVEs against the tech-stacks with risk scoring and additional threat intelligence.
7	Search Against Exploited Application	Ability to search zero day exploited CVEs and tech-stacks.
8	Identifies Out-Of-Date Software Versions	Continuous monitoring of our tech-stacks.
9	Risk-Based Management	Relevant and Applicability to EDI's environment
		Asset criticality
		Known vulnerabilities
		Any known exploitation code
10	Automated Discovery	Required level of sophistication
		Discover internet-exposed assets (both IPv4 and IPv6)
		Support cloud asset discovery
		Enumerate services running on these assets
11	Generate Report	Enable organizations to import known assets not automatically discovered
		Able to produce comprehensive report with prioritization and recommendation.

12	Replacement to Vulnerability Assessment Tool	Replaces existing external VAPT tool for compliance
13	Additional Threat Intelligence	Additional context and actionable threat intelligence against the risk exposure.
14	FAIR Model	Provide Financial Impact Rating
15	Integration	Integrate with MFA, SSO, Ticketing System, SIEM, SOAR, CTI, etc.
16	Support	24x7 Technical Support on both Email, Call, and Web



Security Risk Scorecard Business Case

Not known to many, this is the cheapest, easiest to operationalize, and the fastest visibility of the return of investment (ROI) from the cybersecurity operations. Given that the process is already in place. This platform is a hybrid of all the security domains – governance and risk compliance (GRC), threat and vulnerability management (TVM), incident response (IR), and cyber threat intelligence (CTI).

Evidently, the business and use cases below would clearly tell the coverage from each cybersecurity program that a good security risk scorecard (SRS) must have. Though there could be some additions, these lists are a strong baseline.

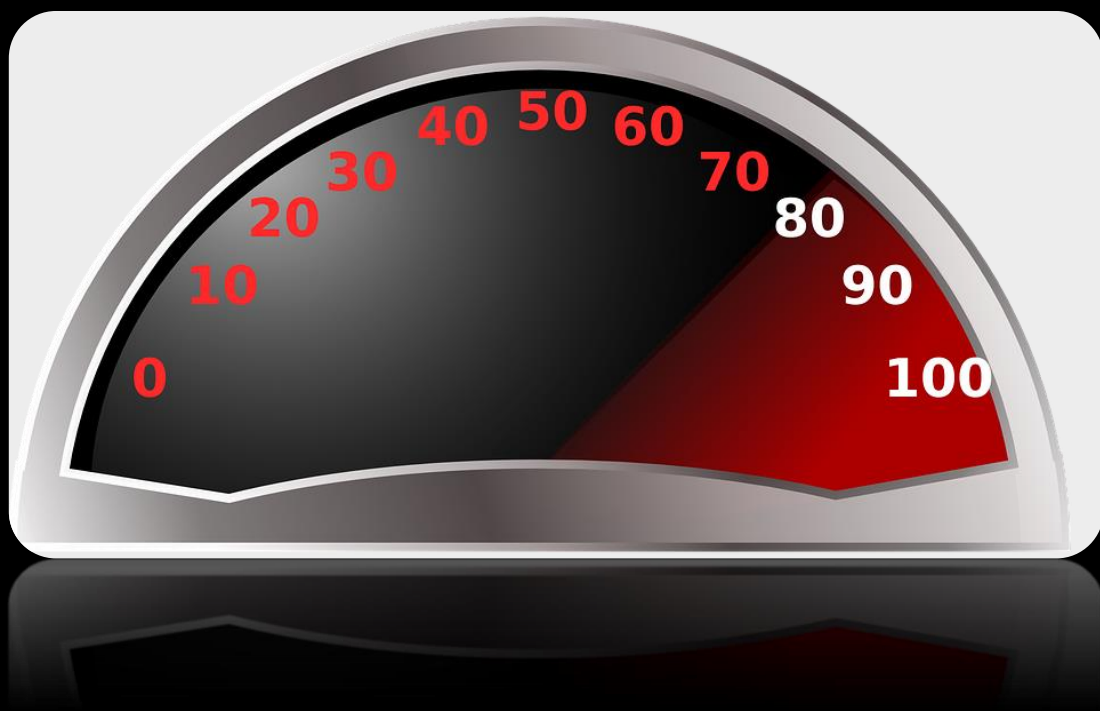
ID	USE CASES	CATEGORY	SAMPLES
1	CAPABILITIES	Risk Assessment Methodology	<div>CVEs</div> <div>TTPs</div> <div>Security Controls (OWASP, SANS, ISO27001, PCI-DSS, CIS)</div> <div>Misconfiguration Scanning (CIA)</div>

			Complete Assessment (Detailed Findings and Recommendations)
			Real-Time Critical Risk Monitoring
			Manual Query Vulnerable Tech-Stacks
		Predictive	Threat Landscape
2	SCOPE	TVM	Patch Management
			Application Security
			CDN Security
			Web Security
			SSL/TLS Strength
			Attack Surface
			DNS Health
			DDOS Resiliency
			Network Security
			Web Ranking
		Security Operations	Credential Management
			Email Security
			IP Reputation
			Fraudulent Apps
			Fraudulent Domains
		GRC	Brand Monitoring (Brand Names)
			Social Mention
			Data Leaked
3	SECURITY RATINGS	Transparency	Providing full and timely openness on the Security Posture findings
		Accurate and Validated	Empirical, data-driven, and based on independently verifiable and accessible information
		Timely and Updated	Up to date
		Model Governance	Provide reasonable notice and explanation on the impact of security rating
		Confidentiality	MNDA
		Independence	Ability to improve the security ratings
4	USABILITY	User-Friendly	Intuitive
5	COMMUNITY SUPPORT	Blogs	Company
			Product
			Cybersecurity and Risk Management

6	RELEASE RATE		Breach Research
		Features and Bug Updates	Frequent
7	3RD PARTY INTEGRATION	Risk Monitoring	Vendors and Suppliers
		API Integration	TVM Platform
			GRC Platform
			Ticketing System
			SSO
8	DISTINGUISHED CUSTOMERS	This signifies Product Maturity	Fortune 500
			ICS/OT
			Telecommunication
			Data Center
			Transportation
			Banking and Finance

Acquiring this tool would give the organization visibility on the external threat landscape. Most of the CISOs use this more often on their presentations with the board of trustees or c-suites. The report generated from the platform is also being used in ISO 27001 and SOC 2 compliance certifications.

This is good to have the technology for business point of view.



IoT Asset and Inventory Intelligence Business Case

Asset and inventory management (AIM) tool could be the top priority to have in both the enterprise IT and industrial control system or operational technology (ICS/OT) cybersecurity. No one can protect the organization holistically without knowing what critical assets they have. Hence, this should have been addressed during the first chapter during the foundation of the CyOps program when mapping everything with the MITRE framework.



A small and start-up company may have budget constraints to acquire this advanced asset intelligence tool but when the time comes, this business and use cases will be handy for facilitating a proof-of-concept or value (POC/POV).

ID	USE CASE	BUSINESS CASE
1	DEPLOYMENT and USER MANAGEMENT	SaaS or On-Prem
		Agentless
		Intuitive
		User-Friendly
2	ASSET and INVENTORY MANAGEMENT (AIM)	Incomplete Asset Inventory
		Inaccurate data and characteristics
		Inability to tune
		Deep risk information
		Unmanaged Asset Discovery
3	THREAT and VULNERABILITY MANAGEMENT (TVM)	Identifying Vulnerabilities
		Threat Intelligence for Prioritizing and Risk Scoring
		Prioritizing Vulnerabilities
		Timely Remediation of Vulnerabilities

		Tracking the Vulnerability Management Process
4	INCIDENT MANAGEMENT (Monitoring, Detection, and Response)	NTA - Passive Anomaly Detection
5	THREAT LANDSCAPE (Internal Attack Surface)	Is the system at risk critical to operations?
		Is the system hardened?
		Is the system likely to be compromised based on contextual data relative to the attack vector?
		Determine if the asset in layer one (SIS) or two (SCADA/Control Engineering), and is it an adjacent network or network attack vector including the layer 3.5 (FW/DMZ/Proxy) asset?
6	REPORTING	Executive Summary
		Technical Summary
		With Remediation Recommendation
7	TECHNICAL SUPPORT MANAGEMENT	Global Regional Support Coverage
		Email Support
		Phone Support
		24x7 Coverage
8	3rd PARTY INTEGRATION	SIEM
		SOAR
		CTI
		MFA/SSO
		Ticketing System

ACKNOWLEDGEMENT

The author would sincerely like to recognize the teammates, leaders, and CISOs that he worked with from the present and previous organizations. They have contributed a lot in many aspects especially for being a mentor. They are the ladder that the author used as a steppingstone to reach the milestones on where he is today.

To the MITRE ATT&CK community who restlessly and continuously collaborate, researching, and testing for malware and adversary's tactics, techniques, and procedures.

The NIST that gives the global organization a solid framework for people, process, and tools in cybersecurity.

For all the vendors whom the author worked with and shared the business and use cases for testing their products and learned from those to further enhance their solution's capabilities.

To all the photographers and graphic designers who are sharing their beautiful craft on the Internet without copyright.

To all the cybersecurity community from different domains who keeps on advocating and mentoring the next generation of cybersecurity professionals that gives hope and confidence.

And to all my friends and families who always believe in me.

With all my heart and soul, thank you!

ABOUT THE AUTHOR

Michael Artemio Go Rebultan, also known as “Art Rebultan” – has 19 years of combined experience as an IT, OT, and Cyber Security professional with a background in PCI-DSS technical audit management, Unix/Linux security, and systems administration, R&D, VAPT, TVM, Risk Management, Counterintelligence.

He acquired these unique experiences from different organizations that he joined – semiconductor, business process outsourcing, academe, retail corporation, data center, a banking corporation, security solutions provider, and energy company. Thus, he wanted to share these with all CISO aspirants including himself.

He is holding a master's degree in IT (MIT) with a concentration in E-Commerce security, a bachelor's degree in computer science (BSCS), a graduate diploma in digital forensics and cyber security (GrDp-DFCS), and a degree in aircraft technician course and spent a year of practice in the aviation industry before jumping to the world of information and communications technology.

As a vow to himself of giving back something to the community, he loves to submit calls for papers in various IT and OT cybersecurity conferences for speaking engagements. He always believes that human knowledge belongs to the world.

Some of the international summits that he presented with are RSA, HITB, ICS Security Week, Paraben, Smart Cybersecurity, Mandiant Cyber Defense, Arab Security, Infosec in the City, and more).

Obviously, he is also devoted on technical writings more of his works are posted here, [Art Rebultan – Medium](#) and [Str@1n3r · GitHub](#). One of the known e-book that he is a co-author with is the [Red Team E-Book Guide by Peerlyst](#).

Art is affiliated with the ISC² Singapore and Rotary Club of Singapore (RCJT). And as a normal person, he is a Krav Maga practitioner, Judoka, Eskrimador, and a license level 2 Freediver.

The **Accidental CISO**



Survival Kit

Version 1 – March 2022