

# **Global Information Assurance Certification Paper**

# Copyright SANS Institute Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

# Interested in learning more?

Check out the list of upcoming events offering "Advanced Incident Response, Threat Hunting, and Digital Forensics (Forensics at http://www.giac.org/registration/gcfa

# Threat Hunting and Incident Response in a postcompromised environment

### GIAC (GCFA) Gold Certification

Author: Rukhsar Khan, rkhan@rukhsarkhan.de Advisor: Mohammed Haron Accepted: November 28<sup>th</sup>, 2019

#### Abstract

If you give an attacker 100 days to move freely in your compromised environment, the evidence is reasonably strong that your organization is pretty bad at Security

Operations (The future of Security Operations). However, repeatedly sending false positives breach escalation to the forensic team is also problematic. It happens in a lot of large organizations, banks and, government institutions across the globe.

This paper starts with an overview of current significant problems identified in Security Operations and Digital Forensics and Incident Response (DFIR) teams and reasons behind them. Then, we will discuss on the solution that encompasses the MITRE ATT&CK framework (MITRE ATT&CK) along with a robust Cyber Threat Intelligence (CTI). Appropriate data collection sources for data enrichment, including all Cyber Security threat information expressed in the STIX language, will also be covered. Although the solution includes specific commercial and non-commercial products and tools from various vendors and organizations, we are not necessarily in favor of any. The core implementation of the MITRE ATT&CK framework, however, is performed in the IBM Resilient Security Orchestration, Automation, and Response (SOAR) product.

# 1. Introduction

Security Operations Center team (SOC) is responsible for detecting any suspicious and malicious cyber activity in an organization. Once such activity is detected, SOC team generates a security incident report that includes any corresponding information, to hand it over to the Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT). The latter teams' responsibility is to validate the security incident and coordinate the Incident Response (IR) process. If it turned out to be a false-positive, the team is responsible for marking it and then closing it. SOC, CERT and CSIRT teams are also known as Security Operations (SecOps) with the primary goal as to detect and to respond to Cyber Security threats in defending an organization's networked computer environment including their crown jewels.

If SecOps identifies "the organization has been breached, their work is usually finished since they lack the expertise to comprehend a breach fully. So they hand over the incident to a DFIR team, consists of the most skilled and sought-after experts in the Cyber Security industry. DFIR experts can forensically understand and report on the full scope and complete impact of a data breach. Starting with the date, time, and method of the initial compromise, over privilege escalation" (Current Security Operations and DFIR problems) to lateral movement, and accomplishment of the ultimate attack target. It could be of an exfiltration of confidential data or the manipulation of systems or other types of attacks. For discovering this, DFIR experts use many different methods and tools. Evidences are gathered and preserved, to provide the means for its usability during litigation.

In the next chapter will discuss current problems of SecOps and DFIR teams. We will also cover a third discipline which is relatively new in Cyber defense, namely Threat Hunting. Following this, we will introduce a solution based on the MITRE ATT&CK and STIX frameworks underpinned by a sophisticated CTI. In the last chapter, a concrete implementation of the solution can be seen.

## 1.1. SecOps analysis and findings

According to a Forrester report (Forrester Now Tech.), the median breach confirmation time in 2017 was 101 days. So basically it took 101 days for SecOps to confirm a breach and hand it off to the DFIR team. However, DFIR teams are currently often annoyed by the input they receive from SecOps that they frequently request them not to forward anything at all.

One of the primary reasons we have found behind this is the success story "We've identified malware and removed it." Most SecOps organizations move directly to the containment, eradication, and recovery phase of the National Institute of Standards and Technology (NIST) framework without proper scoping an attack.

Firstly, if you don't scope a malware scenario out, you don't know anything about the context. As a result, you have no idea at all in which phase the attacker might be. He might be at the very initial stage of the attack, or he might have already compromised your environment and is about to exfiltrate data. You would be blind to the big picture.

Secondly, if the attacker is an advanced adversary, you can be sure that he's watching your movements. If you begin to remove the threat partially, he might be thinking that you have started a fully-fledged remediation process. And what can be expected from an advanced attacker if he fears to lose his foothold from your compromised environment? If it is, then he is going to start another campaign to strengthen his foothold. That is even worse!

As shown in Figure 1, SecOps needs to improve their capabilities before spending more time and resources in the Detection & Analysis phase. Let me explain later what we mean by this.



If we wanted to express the major reasons why Security Operations is performing poorly in a single headline, we could say that SecOps is scratching only on the surface. There are use cases that range from trivial to complex ones; however, an approach to classify, to categorize and to organize attack scenarios holistically is still lacking.

Also, when it comes to integrating with a CTI solution, SecOps is mostly concentrating on "Isolated Indicators of Compromise (IoC)" only. By "Isolated IOCs," we mean IP addresses, hash values, domain names, etc. that are neither put into a relationship nor is there provided any additional context as part of the CTI. Firstly, isolated IOCs are of little value if no context is supplied. Then, they are changing too rapidly during an attack so that one cannot entirely rely solely on them. The Verizon DBIR 2016 Report stated that 99% of malware hashes seen for just 58 seconds or less.

A robust and actionable CTI can help organizations in providing detailed context around an IOC. E.g. if your IOC is a known bad IP address, related entities like related IP addresses, domain names, email addresses, hash values, malware, products and tools, a Threat Actor and his used Tactics, Techniques and Procedures (TTPs) – tactical intelligence, a Threat Actor and his motivations – strategic intelligence, intelligence reports, etc. shall be provided. Having these kind of real facts helps in staying focused during the analysis without losing traction.

Checking the local relevance – findings – of IOCs adequately is another crucial step during an analysis. Once CTI provided IOCs have been validated in the local context, it's essential to pull in the corresponding timestamps – first-, last-packet –, source-destination relationships, bytes sent, bytes received, protocols and ports used, duration, domain name, etc. Not only is SecOps currently not looking into these kinds of details. They often even don't have the right technology in place that would provide this level of information.

IOCs and local findings, along with all their corresponding context, need expression in a meaningful way. For this, a common expression language is required that allows to seamless data sharing between systems and tools, and to visualizes the relationships between them. OpenIOC and STIX are examples of such an expression language. OpenIOC was developed originally by Mandiant which is now owned by Fireeye whereas STIX is developed by OASIS, which is a non-profit consortium that drives the development of open standards. In other words, STIX is Open Source, and the current version is 2. STIX2 is specified in JSON format whereas its predecessors, STIX 1.1 and 1.2, were defined in XML format.

Unfortunately, most Cyber Security vendors have not yet adopted STIX as their preferred output format. Instead, vendors' native JSON format is still commonly used. This leads to heavy data conversion efforts to use STIX in today's environment. However, vendors have realized the importance of such an expression language and are therefore providing additional tools or have STIX2 compatibility on their roadmap.

## 1.2. DFIR analysis and findings

Major problems that we have encountered in DFIR teams is that, they have to deal with a plethora of tools with uncountable inputs and different output formats that are used manually on command line interfaces.

One of the biggest challenges we have found is the lacking or little integration of the DFIR tool landscape with the organizational infrastructure. Hence, when DFIR teams are conducting a breach analysis, they heavily rely on input from the SecOps and Infrastructure teams related to data collection. This is currently an entirely manual and a time consuming process.

Also, a proper communication and information sharing with the rest of the organization is currently not possible except by means of a ticketing system.

A lot of DFIR teams are also lacking or dealing with poor process driven, standardized procedures for known threat scenarios which prevents them from conducting the breach analysis in a structured and organized way (poor playbooks). Often, enterprises are afraid of funding internal DFIR teams because it's hard to measure their success in a pre-defined timeline. In other words, if a DFIR team is not structured well, there is a high probability that the breach analysis timeline is not predictable. That's why a lot of organizations hire an external DFIR Service Provider that acts as an Incident Response Retainer in case of an emergency.

Forensic tools used by DFIR teams, whether those are commercial products or open source tools, have one thing in common. They are mostly self-contained with no or little integration with 3<sup>rd</sup> party systems. As to the best of our knowledge, neither does Opentext Encase nor Access Data FTK, two well-known commercial products in the forensic field, have a REST API. The same is true for open source tools like Volatility, Plaso, Log2timeline, etc. This is the main reason we have found why DFIR teams are heavily dependent on the data provisioning from SecOps and Infrastructure teams and unable to communicate and share information to the rest of the organization in a standardized way.

It's also difficult to provide a process driven procedures standardization since every breach is unique. However, there are still many common investigation routine tasks which need to be processed while triaging a breach.

## 1.3. Threat Hunting

As the above traditional forensic methods don't allow to respond in a timely manner and at scale, a shift can be observed in the market in the way forensic investigations are conducted today in contrast to "few years ago. Currently, a full-blown deep dive forensic analysis is only done on specific confirmed compromised systems in order to gather additional intelligence. As this doesn't scale across thousands or tens of thousands of endpoints, the new Endpoint Detection and Response (EDR) market has evolved over the last couple of years. Key players like Tanium, Crowdstrike and Carbon Black Response are providing real-time sensors on endpoints in order to quickly gather forensic artifacts via" (Rukhsar Khan, 2019) REST APIs and conduct live response. In our solution we will be leveraging Carbon Black Response for the endpoint sensing and for applying the Threat Hunting technique.

"The idea behind Threat Hunting is to shift from a reactive IR model to a proactive approach. In Security Operations, a detection team hands off an alert" (Operationalizing the MITRE ATT&CK framework for Security Operations, Threat Hunting and DFIR) to a CERT or CSIRT team which reactively kicks off the IR process for validating the incident and responding to it, in case it's a true incident. The goal with Threat Hunting is to proactively engage a team and hunt for known adversaries including their applied TTPs in an organization's networked computing environment. There are multiple different approaches to Threat Hunting. This paper is not intended to introduce the various forms of Threat Hunting.

In our solution we will be starting the hunt engagement by consuming high-quality initial triage results generated by the CERT or CSIRT team for level-1 analysis. These results will already be augmented by a sophisticated CTI which will be further leveraged by the Threat Hunting team in order to remain focused. We will apply different Threat Hunting techniques and support the CERT/CSIRT team in scoping the attack and limiting the capabilities of an intruder. This will mainly be based on live response with Carbon Black Response EDR in order to provide quick results.

# 2. Solution

Based on the experience within the last decade, dozens of large customers and new emerged market technologies such as Security Information and Event Management (SIEM), EDR, a sophisticated CTI, and advanced tools for computer and network forensics, it is clear that Security Operations, Threat Hunting and DFIR teams need to converge. This is necessary in order to detect and respond to incidents quickly and efficiently, compared to attackers operating their automated attack ecosystems. All three disciplines need to coexist in achieving goals to allow collaboration as well as orchestration, automation and response in single platform. Certainly, See our solution in Figure 2.

- Secops, Threat Hunting and DFIR need to converge. The preferred tool should be SOAR.
- Security Operations and Threat Hunting need a holistic approach to analyze known Threat Scenarios with better CTI – strategic & tactical – and sophisticated data collection sources – e.g. endpoint sensing, flows, etc.
- DFIR needs to better integrate their forensic tools and procedures with the organizational infrastructure.

#### Figure 2: Solution – Claim

It should be noted that a SOAR platform is purpose-built for IR in Security Operations. However, we believe that many features are also well suited for supporting Threat Hunting and DFIR teams. To name a few, workflows, playbooks and orchestration techniques can help the latter teams in order to stay focused and provide quick results. Taking ownership of routine tasks through automation techniques a SOAR platform can further help these teams to free up valuable resources for the more sophisticated and manual tasks required during a Threat Hunting engagement or forensic investigation. Both teams will additionally require to leverage an EDR solution especially for data collection from the endpoint. DFIR teams also need to use a lot of additional forensic tools which can often be integrated with the SOAR platform.

In order to qualify Cyber Security threats and drastically reduce the median breach confirmation time, Security Operations and Threat Hunting teams need "holistic approach to analyze known threat scenarios. Also, they need to start an investigation on the right foot. This is why they need a better CTI that is providing comprehensive strategic and tactical intelligence and giving them context around their IOCs. In addition to this, sophisticated data collection sources need to be implemented. E.g. endpoint sensing and flows are absolutely essential as they provide the means to understand the IOCs in context of their local relevance" (Solution draft). All in all, the goal for SecOps should be to provide high quality results that are consumable by a Threat Hunting and DFIR team.

A Threat Hunting team should support a SecOps team in further scoping an attack by conducting individual TTP analysis and developing additional intelligence. Very importantly, a Threat Hunting team should also be able to identify an ongoing attack and advise the SecOps team how to restrict the capabilities of the attacker. DFIR needs to better integrate their forensic tools and procedures – playbooks and workflows – with the organizational infrastructure.

All of these are part of our solutions, however before we go into the details, we need to introduce the MITRE ATT&CK framework, some useful MITRE resources, sophisticated CTI of the providers Recorded Future and STIX.



Figure 3 is showing the MITRE ATT&CK framework (MITRE ATT&CK). MITRE institute spent many years in analyzing the global high-profile breaches and categorizing them into individual TTPs. Currently, there are 11 tactics of the ATT&CK Matrix for Enterprise, starting off with Initial Access up to Command and Control, down to individual techniques. Every technique describes adversarial procedures and methods. You can also see on the right top corner, on how the ATT&CK Matrix for Enterprise maps to the Cyber Kill Chain. It fits into the last three phases and therefore a post-compromise matrix. A Pre-ATT&CK Matrix available that maps to the pre-compromise phases of the Cyber Kill Chain.



Persistence Privilege Escalation Defense Evasion Credential Access Discovery Lateral Movement Execution Collection Exfiltration Command and Control

#### ATT&CK Matrix for Enterprise

The full ATT&CK Matrix below includes techniques spanning Window	ws, Mac, and Linux platforms and	I can be used to navigate through the knowledge ba	ise.
		· · · ·	

					•	•				
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command an Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographi Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-Stage Channels
	I SASS Driver	Component Firmware	File System Permissions	DCShadow	Input Promot	Ouery Registry	Replication Through	Man in the Browser		Multi-hon Provy

#### Figure 3: Holistic approach – MITRE ATT&CK framework

The MITRE ATT&CK framework is a TTP-based, behavioral threat model. The goal is to detect and mitigate adversarial behaviors based on the individual TTPs as opposed to IOC-based detection and mitigation. As we learned before, IOCs are changing too rapidly but behaviors of an attack scenario can't change entirely. That's why MITRE ATT&CK is entirely concentrating on detection behaviors. This does not mean that we will not be looking at IOCs at all. We will start the investigation based on known IOCs that are relevant for our environment but after some initial triage tasks we will shortly switch to the behavioral model.

1	- ė (	
		"data": {
		"risk": {"rules": 7}.
		"counts": []
		"entity", ["id", "in-03 184 220 20" 1
		"metrica" ( )
		ideation : { asm : #SISISS }
		Intellard : https://app.recordedituture.com/iive/sc/entity/ipssas.is4.220.29 ,
		"timestamps": { "IastSeen": "2018-11-15118:00:48.2622"},
		"threatLists": [],
		"analysthotes": [],
		"riskyCIDRIPs": [],
		"relatedEntities": [
		ł.
		"type": "RelatedMalwargCategory",
		"entities": []
		],
		"type": "RelatedHash",
		"entities": []
		"type": "RelatedEmailAddress",
		"entities": []
		},
		4
		"type": "RelatedIpAddress",
		"entities": []
		f
		"type": "RelatedThreatActor",
		"entities": [
		"count": 1.
		"entity": {
		"id": "GJnFk",
		"name": "AIVD".
		"tume": "Organization"
		"count": 1.
		"entity": /
		"id": "L37nw-".
		"name". "APT28 Fancy Bear"
		"type", "Organization"
		olike , ordaursacrou
		Thime T. The Land Tenner Domain Name T
		Type: <u>merateunterne</u> chomainname,
		entities : []
		}r Ellen − U. – UN-N-res-Me-Nersen − U.
		{"type": "RelatedMalware"},
		"type": "RelatedProduct",
		"entities": []

- 1. Provide real facts
- 2. Inform an organization on the ATT&CK tactics and techniques on which to focus.
- Beginning the analysis on the right foot is crucial. Else you quickly lose focus and waste all your time.

Figure 4: Cyber Threat Intelligence – Recorded Future

So, for beginning the analysis on the right foot it is crucial to have an excellent and robust CTI in place that provides real facts and "informs an organization on the ATT&CK tactics and techniques on which to focus" (MITRE MTR170202). In our solution we are leveraging CTI from Recorded Future. See Figure 4.

This CTI is related to an IP address entity of the value 93.184.220.29. The term entity is equivalent to the term indicator which means that this is the IOC we are starting our investigation with. As you can see further down in the CTI there are multiple related entities to this indicator like related hashes, related email addresses, related IP addresses and most importantly for now a related Threat Actor – APT 28, a well-known Russian Threat Group – which we have learned should be part of a robust and actionable CTI. Based on the provided Threat Actor our next step is to map the CTI out to the MITRE ATT&CK Matrix. In our example we have two related Threat Actors, namely AIVD and APT28. Since MITRE is providing known Threat Actors and their used TTPs as part of the ATT&CK framework, you can simply map out TTPs based on the Threat Actor name.

layer x +	·	mmegranoso/attabt-havig	aron yen ren prinsky								5 H	MITRE ATT&CK <sup>TM</sup> Navigator
						selection cont	=+, ×,	layer controls	`⊞ ⊄	D ₹,1:	Ž ♥, O Ⅲ 🧏	chnique controls 🕺 💁 , 🔟 , 🔍 , 🕅
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery		Threat (	Groups		Exfiltration	Command And Control
10 items	33 items	58 items	28 items	63 items	19 items	20 items	APTI	vie	w select	deselect	9 items	21 items
Drive-by Compromi	ise AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	APT16	vis	w select	deselect	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing	g CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window	APT17	vie	w select	deselect	Data Compressed	Communication Through
Application	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Discovery	APT18	vis	w select	deselect	Data Encrypted	Removable Media
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Browser Bookmark Dis	C APT19	vie	select	deselect	Data Transfer Size Limits	Connection Proxy
Replication Through	h Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Disc	0	<u></u>	- Joneca	deserved.	Exfiltration Over Alternativ	Custom Command and Control Protocol
See Suphishing Attac	hmanic Data Exchange	Application Shimming	Bypass User Account	CMSTP	Credentials in Registry	Network Service Scann	ii AP128	<u>V16</u>	w select	deselect	Protocol	Curtom Contographic
Spearphishing Link	Execution through API	Authentication Package	Control	Code Signing	Exploitation for Credential	Network Share Discove	APT29	vie	w select	deselect "	d Exfiltration Over Comman and Control Channel	d Protocol
Spearphishing via Se	Execution through Module	BITS Jobs	DLL Search Order Hijacking	Compiled HTML File	Access	Network Sniffing		Sorty	vare		Exfiltration Over Other	Data Encoding
Supply Chain Comp	Load	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Password Policy Disco	V SPAKA KAT	VIE	w select	deselect	Network Medium	Data Obfuscation
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model	Hooking	Peripheral Device Disco	04H RAT	vie	w select	deselect	Exfiltration Over Physical	Domain Fronting
Valid Accounts	Graphical User Interface	Change Default File	Extra Window Memory	Hijacking	Input Capture	Permission Groups Dis	ADVSTORESHE	iLL <u>vie</u>	select	deselect	Medium	Fallback Channels
	InstallUtil	Association	Injection	Control Panel Items	Input Prompt	Process Discovery	ASPXSpy	vie	select	deselect	Scheduled Transfer	Multi-hop Proxy
	Launchetl	Component Firmware	File System Permissions	DCShadow	Kerberoasting	Query Registry	Agent hts	vie	select	deselect		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Weakness	Deobfuscate/Decode Files or Information	Keychain	Remote System Discov	ngeneiber			desclose		Multiband Communication
	LSASS Driver	Create Account	Hooking	Disabling Security Tools	LLMNR/NBT-NS Poisoning	Security Software Disco	<sub>p</sub> Arp	vie	w select	deselect		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Image File Execution Options Injection	DLL Search Order Hijacking	Network Sniffing	System Information	Autolt backdoo	or vie	w select	deselect *	<u> </u>	Port Knocking
	PowerShell	Dylih Hijacking	Launch Daemon	DLL Side-Loading	Password Filter DLL	System Network	Taint Sh	ared Content				Remote Access Tools
	Regsvcs/Regasm	External Remote Services	New Service	Exploitation for Defense Evasion	Private Keys	Configuration Discove	ry Third-pa	arty Software				Remote File Copy
	Regsvr32	File System Permissions	Path Interception	Extra Window Memory Injection	Securityd Memory	System Network	Window	s Admin Shares				Standard Application Layer
	Rundll32	Weakness	Plist Modification	File Deletion	Two-Factor Authentication	Connections Discovery	/ Window Manage	is Remote ment				Protocol
	Scheduled Task	Hidden Files and Directories	Port Monitors	File Permissions Modification		System Owner/User Discovery						Standard Cryptographic Protocol
	Scripting	Hooking	Process Injection	File System Logical Offsets		System Service Discove	ery					Standard Non-Application
	Service Execution	Hypervisor	Scheduled Task	Gatekeener Bynass		System Time Discovery	, ,					Layer Protocol
	Signed Binary Proxy Execution	Image File Execution Options	Service Registry Permissions	Hidden Files and Directories	1							Uncommonly Used Port
	Signed Script Proxy Execution	Injection	Weakness	Hidden Users	-							Web Service
	Source	Nernel Modules and Extensions	Setuid and Setgid	Hidden Window								
	Space atter Filename	Launch Agent	SID-History Injection	HISTCONTROL								
	Third-party Software	Launch Daemon	Startup Items	Image File Execution Options								
	Trap	Launcheti	Sudo	Injection								



Figure 5 introduces a free tool from MITRE, the ATT&CK Navigator, that visualizes all the TTPs of one of the ATT&CK matrices, depending on which matrix you have loaded. In our example we have loaded the ATT&CK Matrix for Enterprise. This tool allows us to select a Threat Actor. Since our CTI indicates APT28 as a related Threat Actor and this specific Threat Actor is available in the ATT&CK framework, we can simply select it and the ATT&CK Navigator highlights all the related TTPs. This allows us to learn how the Threat Group is operating. If we right-klick on a TTP we can select to view the corresponding technique details. This opens a new browser tab which is linked back to the MITRE website. Every TTP has a unique id, some high-level information on the corresponding procedures and methods, examples out of the wild, detection and mitigation advise and a whole universe of further detailed references to known global high-profile breach reports. We call this the human readable version of the ATT&CK framework.

In our solution we are splitting the TTP provided information into multiple stages, namely *Stage 1 Analysis*, *Stage 2 Analysis* and *Stage 3 Analysis*. We will later describe what we exactly mean by this.

In contrast to the human readable version of the ATT&CK Matrix the entire framework is also available in machine code, more precisely in STIX2 format. As mentioned earlier, STIX2 is a specific JSON formatting. Based on Figure 6 and Figure 7 let's see what STIX2 is about.

STIX is a great language that can express and describe a Cyber Security threat or incident by breaking down its complex and obfuscated elements into individual structured objects and put those objects into a relationship. You can then visualize the relationships in a graph.

STIX2 defines twelve STIX Domain Objects (SDOs), namely Attack Pattern, Campaign, Course of Action, Identity, Indicator, Intrusion Set, Malware, Observed Data, Report, Threat Actor, Tool and Vulnerability. In addition to these, two additional STIX Relationship Objects (SROs) are defined which can put the SDOs in a specific kind of relationship. SRO names are Relationship and Sighting. Following is an enumeration of all the domain objects provided by MITRE ATT&CK as part of their framework:

- 1. MITRE TTPs = Attack Pattern SDO
- 2. MITRE Mitigation = Course of Action SDO
- 3. MITRE Intrusion Set = Intrusion Set SDO
- 4. MITRE Malware = Malware SDO
- 5. MITRE Tool = Tool SDO
- 6. MITRE Identity = Identity SDO
- 7. MITRE Relationship = Relationship SRO

 STIX 2 defines twelve STIX Domain Objects (SDOs):

 Object
 Name
 Description

 MITRE TTPs
 Attack Pattern
 A type of Tactics, Techniques, and Procedures (TTP) that describes ways threat actors attempt to compromise targets

Local definition	Campaign	Campaign	A grouping of adversarial behaviors that describes a set of malicious activities or attacks that occur over a period of time against a specific set of targets.
MITRE mitigation	Course of Action	Course of Action	An action taken to either prevent an attack or respond to an attack.
Local definition	Identity	Identity	Individuals, organizations, or groups, as well as classes of individuals, organizations, or groups.
CTI	Indicator	Indicator	Contains a pattern that can be used to detect suspicious or malicious cyber activity.
MITRE Intrusion Set	ム 示 後 ム Intrusion Set	Intrusion Set	A grouped set of adversarial behaviors and resources with common properties believed to be orchestrated by a single threat actor.

#### STIX Patterning

[ipv4-addr:value = '93.184.220.29' OR ipv4-addr:value = '152.199.19.161' OR ipv4-addr:value = '13.107.4.50' OR ipv4-addr:value = '68.232.34.200' OR ipv4-addr:value = '23.37.43.27' OR ipv4-addr:value = '23.184.221.240']
[network-traffic:dst\_ref.type = 'domain-name' AND network-traffic:dst\_ref.value = 'example.com'] REPEATS 5 TIMES WITHIN 1800 SECONDS

[windows-registry-key:key = 'HKEY\_CURRENT\_USER\\Software\\CryptoLocker\\Files' OR windows-registry-key:key = 'HKEY\_CURRENT\_USER\\Software\\Microsoft\\CurrentVersion\\Run\\CryptoLocker\_0388']

[email-message:from\_ref.value MATCHES '.+\\@example\\.com\$' AND email-message:body\_multipart[\*].body\_raw\_ref.name MATCHES '^Final Report.+\\.exe\$']

[artifact:mime\_type = 'application/vnd.tcpdump.pcap' AND artifact:payload\_bin MATCHES '\\xd4\\xc3\\xb2\\xa1\\x02\\x00\\x04\\x00']

Figure 6: Structured Threat Information Expression (STIX) (Source: https://oasis-open.github.io/cti-documentation/stix/intro)

An Attack Pattern SDO describes the TTPs a Threat Actor is using in order to compromise a target. A Course of Action SDO gives instructions on how to respond to the attack. An Intrusion Set SDO provides all the context around a Threat Actor or Threat Group, their motives, the way they are operating, etc. A Malware SDO expresses a malware variant that is used to compromise a target. A Tool SDO describes a tool that can be utilized in order to compromise a system. An Identity SDO simply describes an individual, an organization or a group. A Relationship SRO creates relationships of a specific type between SDOs in order to express that relationship. E.g. an Identity Set is using specific malware, a Course of Action mitigates an Attack Pattern, an Identity is targeted by a tool, etc.

Other SDOs or the Sighting SRO which are not provided by MITRE ATT&CK need to get derived from other sources. E.g. the Indicator SDO can come from a CTI feed. Contextual objects like Report SDOs, Threat Actor SDOs and Tool SDOs can also be delivered as part of a robust and actionable CTI.

MITE	RE malware	Balware	Malware	A type of TTP, also known as malicious code and malicious software, used to compromise the confidentiality, integrity, or availability of a victim's data or system.
t	— Qradar	Coserved Bata	Observed Data	Conveys information observed on a system or network (e.g., an IP address).
Cyber Observable Object	CTI	Report	Report	Collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including contextual details.
"end": "2018-11-2/14;3:123:638 +0100", "type": "network-traffic", "start": "2018-11-27 14;31:23:638 +0100"	СТІ	Threat Actor	Threat Actor	Individuals, groups, or organizations believed to be operating with malicious intent.
"dst_ref": "2", "src_ref": "1", "protocols": [ "tco"	CTI ITRE tool	<b>K</b> Tut	ΤοοΙ	Legitimate software that can be used by threat actors to perform attacks.
], "dst_packets": 15, "src_packets": 17, "dst_byte_count": 4054,	Qradar	Vulnerability	Vulnerability	A mistake in software that can be directly used by a hacker to gain access to a system or network.
"src_byte_count": 1972 },	S	TIX 2 defines	two STIX Relatio	nship Objects (SROs):
"1": { "type": "ipv4-addr",		Object	Name	Description
"value": "192.168.150.203" ), "2": { "type": "ipv4-addr", "value": "216.58.207.34"	relationship	Relationship	Relationship	Used to link two SDOs and to describe how they are related to each other.
}	definition	50 Sighting	Sighting	Denotes the belief that an element of CTI was seen (e.g., indicator, malware).

Figure 7: Structured Threat Information Expression (STIX) continued (Source: https://oasis-open.github.io/cti-documentation/stix/intro)

Observed Data and Vulnerability SDOs can be created from data collected from an internal Cyber Security defense system like a SIEM, Vulnerability Management system, EDR system, etc. that has matched against a CTI provided indicator in order to express the local relevance. Putting an Indicator SDO into a relationship with an Observed Data SDO is done by the special Sighting SRO.

When operationalizing MITRE ATT&CK and STIX a defending organization can develop SDOs and SROs by leveraging the STIX2 Python APIs (Oasis Open) which are available for free. Let's take a closer look at the Indicator SDO. In order to express a suspicious or malicious IOC with all its context a CTI provider can use STIX patterning which is defined in its own document (Oasis Open). As seen in Figure 6, STIX patterning allows you to narrow down suspicious or malicious behavior very granularly. In Figure 7 you can further see how the local relevance of an IOC expressed by an Indicator SDO is defined by a Cyber Observable Object (Oasis Open) that is part of the Observed Data SDO. Cyber Observable Objects can be far more comprehensive in order to specify any kind of local findings.

In Figure 8 you can further see SDOs put into relationships. A small example in the right top corner is showing how an indicator indicates a Campaign which is in turn attributed-to a Threat Actor and targets a Vulnerability. A graph could look like the one in the middle of this illustration if more context is available.



Figure 8: Structured Threat Information Expression – Relationship types (Source: <u>https://oasis-open.github.io/cti-documentation/stix/intro</u>)

# 3. Implementation

This section details on how we implemented our solution. "As mentioned earlier, our core implementation of the MITRE ATT&CK framework is performed in the IBM Resilient SOAR platform" (Implementation – Overview – steps 0-6). In order to converge Security Operations, Threat Hunting and DFIR in this single platform we have defined three stages, namely *Stage 1 Analysis*, *Stage 2 Analysis* and *Stage 3 Analysis*. *Stage 1 Analysis* corresponds to a SecOps Level-1 IR team, *Stage 2 Analysis* to a Threat Hunting team and *Stage 3 Analysis* applies to a DFIR team. See Figure 9.

Only the items that we have colored red are the ones that we have integrated with IBM Resilient as part of this writeup. These are Recorded Future Threat Intelligence, IBM QRadar SIEM with Wincollect and Sysmon for the endpoint sensing, IBM QRadar Network Insights (QNI) for creating network flows (Internet Protocol Flow Information Export (IPFIX)), A10 SSL interception proxy for intercepting and decrypting SSL traffic, Carbon Black Response as the EDR and Volatility for deep dive forensics. Except for Volatility all our integrations are based on REST APIs. For better understanding our implementation we have given some items of the Stage 1 Analysis unique step numbers. These are the steps that we will demonstrate on the following diagrams. Other system and tool integrations will follow later.

### Stage1 Analysis – L1 (Secops):

- Recorded Future Threat Intelligence (steps 0.2, 5)
- SIEM Qradar events Wincollect - Sysmon (steps 2-6)
- QNI Flows (steps 7-10)
- A10 SSL interception
- proxy Analysis I 2 (Threat Hun
- Stage2 Analysis L2 (Threat Hunting):
  - CB Response
- Stage3 Analysis L3 (DFIR):
  - Volatility
  - Plaso, Log2timeline, etc.
  - Qradar Incident Forensics, PCAP
  - Google Rekall Agent Server
  - Cuckoo Sandbox



## 3.1. Stage 1 Analysis – L1 SecOps

### 3.1.1. Find Recorded Future matched destination IPs and load CTI – steps 0-6

**Figure 9: Solution continued** 

Figure 10 on the next page is visualizing how we are initially detecting destination IP addresses that have matched against the Recorded Future (RF) CTI and what actions we are taking in order to get context. As a prerequisite for this solution to work properly we are first loading the complete MITRE ATT&CK Matrix for Enterprise into a Postgres database named test. To accomplish this, we have written a script that leverages the MITRE TAXII server (step 0.1). Secondly, we are integrating QRadar with Recorded Future by taking advantage of the available Recorded Future app. This app can be configured in a way that it loads RF provided Risklists into QRadar Reference Sets (step 0.2). By defining an RF risk score we were able to limit the number of objects – IP addresses, hash values, domain names, etc. – that are loading into these reference sets. E.g. we configured 65 which corresponds to a high-risk score. We also specified a time interval for updating the reference sets hourly.

Within QRadar we have created rules that point to the reference sets. If any local-to- remote network traffic that matches against an IP address object in a reference set has been identified, the rule fires an alarm which is called offense in the QRadar terminology. An offense contains all the related event<sup>1</sup> and flow data that has been recorded according to the configured rule specification. An offense also includes a list of source and destination IP addresses that have been identified as part of the offense. We are escalating this offense automatically into Resilient which is represented as a new incident (step 1).

Rukhsar Khan, rkhan@rukhsarkhan.de

<sup>&</sup>lt;sup>1</sup> Event data is equivalent to log data in the QRadar nomenclature



Figure 10: Steps 0-6 – Functions diagram on Steps 0-6 – Functions diagram

The offense escalation process is only taking high-level information from the QRadar offense into the Resilient incident. If the analyst needs to enrich the original incident by additional information, he can simply take advantage of Resilient's automation feature that re-queries the QRadar Ariel<sup>2</sup> database and loads the additional information into the incident.

	🗊 🖍 https://qradar.rukhsarkhan.de/console	e/core/jsp/DojoGenericList	.jsp?appName=QRadar&p	ageId=ReferenceSets
	🗋 Add 🖙 Edit 🗟 View Contents 🚳 Delete 🛛 RF	- IP Q		
Recorded Future for QRadar	Name	Туре	Number of Elements	Associated Rules
	RF - Ip - Current C&C Server	IP	590	1
·i;i·	RF - Ip - Cyber Exploit Signal: Medium	IP	1	1
Recorded Future	RF - Ip - Historical Bad SSL Association	IP	95	1
Configuration	RF - Ip - Historical Botnet Traffic	IP	35	1
	RF - Ip - Historical C&C Server	IP	220	1
	RF - Ip - Historical Honeypot Sighting	IP	5,997	1
	RF - Ip - Historical Multicategory Blacklist	IP	5,708	1
	RF - Ip - Historical Open Proxies	IP	680	1
	RF - Ip - Historical Positive Malware Verdict	IP	5,260	1
	RF - Ip - Historical Spam Source	P	338	1
	RF - Ip - Historical SSH/Dictionary Attacker	IP	5,312	1
	No - Ip - Historical Threat Researcher	IP	836	1
	RF - Ip - historically Linked to APT	IP	30	1
Te Wizard	ally Linked to Cyber Attack	IP	1,838	1
Rule Wizard: Rule Test Stack Editor	ally Linked to Intrusion Method	IP	16,300	1
White tests do you wish to perform on incoming events? Test Group 174	ally Reported as a Defanged IP	P	1,355	1
Type to filter	ally Reported by DHS AIS	IP	1,466	1
when the local network is one of the following networks     when the destination network is one of the following networks     when the IP protocol is one of the following networks	ally Reported by Insikt Group	IP	32	1
when the Event Payload contains this string     when the source port is one of the following ports	ally Reported in Threat List	IP	8,831	1
<ul> <li>when the destination port is one of the following ports</li> <li>when the local port is one of the following ports</li> </ul>	ot Host	IP	1	1
when the termice points one of the following IP addresses     when the destination IP is one of the following IP addresses     when the destination IP is one of the following IP addresses	ossible Bogus BGP Route	IP	2	1
when the local IP is one of the following ID addresses Rule (Click on an underlined value to edit it)	s s	IP	48,385	1
Invalid tests are highlighted and must be fixed before rule can be saved. Apply Recorded Future P match on events which are detected by the Local vsyst	tem s Packet Source	IP	14,189	1
COM and when any of Source IP. Destination IP are contained in any of RE - Ip - Current C&C Server - IP. RF - IP - Current C&C Server - IP. RF - Ip - Current C&C Server - IP. RF - Ip - Current C&C Server - IP. RF - Ip - Current C&C Server - IP. RF - Ip - Current C&C Server - IP. RF - Ip - Current C&C Server - IP. RF - IP - Current C&C Server - IP. RF - IP - Current C&C Server - IP. RF - IP - CURRENT C&C Server - IP. RF - IP - CURRENT C&C Server - IP. RF - IP - CURRENT C&C Server - IP. RF - IP - CURRENT C&C Server - IP. RF - IP - CURRENT C&C Server - IP. RF - IP - CURRENT C&C Server - IP. RF - IP - IP. Server - IP. RF - IP. Server - IP. Server - IP. RF - IP. Server	e Delivery	IP	22	1
Server - IP, KF - Ip - Historical Honeypot Signifig - IP, KF - Ip - Historical Multicategory Blacklist - IP, KF - Ip - Historical Department of the Server - IP, RF - Ip - Historical Server - IP, RF - Ip - Histo				
Please select any groups you would like this rule to be a member of Common and the selection of the selectio				
Notes (Enter your notes about this rule) Recorded Future IP match		Figure 11: Step	0.2 – QRadar ro	eference set load

<sup>2</sup> Ariel is the name of the QRadar log/event database

Rukhsar Khan, rkhan@rukhsarkhan.de © 2019 The SANS Institute From the list of all the suspicious destination IP addresses that have been detected by QRadar as part of an offense we want to load the RF matched destination IP addresses into the Resilient incident. For this we are re-querying QRadar from within Resilient (steps 2-3) and loading the retrieved RF matched destination IP addresses into the incident's Artifacts (step 4) tab. An artifact in the Resilient context is an IOC. We have configured to trigger another automation that accomplishes an IP lookup for every newly created RF matched IP addresses artifact (step 5) in order to load the detailed CTI with all the IOC context in our test database (step 6).

**Figure 11** is visualizing the loading of objects by the RF app provided risklists into QRadar reference sets. Reference sets have a Name, Type, Number of Elements and Associated Rules column. The associated rule is also shown on the right side of this illustration.

					Summary Display 🔻	Events 🔍 Flows	Actions V 🖨 Print	Send to Res	
Magnitude			Status	Rele	evance 6	Severity 5		Credibility 4	
	Quick execution of a series of suspicious commands		Offense Type	e Sou	rce IP				
Description	containing Process Create		Event/Flow c	ount <u>84 e</u>	events and 82 flows in 17 categ	ories			
iource IP(s)	<u>192.168.150.203</u> (192.168.150.203)		Start	Nov	26, 2018, 5:00:00 PM				
estination IP(s)	Local (10) Remote (18)		Duration	1h 2	10m 25s				
letwork(s)	Multiple (3)		Assigned to	Una	ssigned				
		All A			(				
All Oper	Incidents - Edited T -	Save As 👻 🍪 (Shared)							Selected -
All Oper	isposition: Confirmed, U	Save As	e 🖸					More	Selected •
All Oper Incident D	isposition: Confirmed, U	Save As  Chared) Name: "9697"  Status: Active	e Ø					More.	Selected •
All Oper Incident D 1 result SI	how 100 •	Save As  Chared) Name: "9697"  Status: Active Description	e C Date Discovered	Next Due Date	⇔ Date Created	\$ Owner	\$ Phase	More	Selected • • Columns • Status

Figure 12: Step 1 – Qradar offense escalation

The QRadar offense escalation into Resilient is further illustrated in Figure 12. As you can see, the offense has a unique number which in our example is 9697. The source IP - or potential victim IP - address is 192.168.150.203. There is a total of 18 remote destination IP addresses, 84 events and 82 flows recorded as part of this offense. Once this offense is escalated into Resilient, either automatically or manually by clicking on the Send to Resilient button on the right top corner of the offense, this offense becomes an incident in the Resilient SOAR platform. When the incident is created, the name and description of the incident are derived from a field mapping configuration in the QRadar Resilient app. This app is installed on QRadar and is required to escalate QRadar offenses to Resilient.

scription flows and 2224 events in 20 categories: Quick execution o ch containing Process Create	MITRE: T1059/Command-Line Interface + Activity field Make integrity provisioning MITRE: T1016/Network Configuration Discovery MITRE: T1059/Command-Line Interface MITRE: T1082/System Information Discovery
asks Details Breach Notes Members Ne utomotive MITRE ATT&CK QRadar Events utfifacts	RECORDED FUTURE: Destination IP match from QRadar re-query Action Status Workflow Status Close Incident Delete Incident
Search Q	Add Artifact Table Graph Artifact Type: All Date Created: All - Has Attachment: All
how 25 💌	

Figure 13: Step 2 – RECORDED FUTURE: Destination IP match...

In order to trigger the re-query from Resilient to QRadar we have provisioned the **RECORDED FUTURE: Destination IP match from QRadar re-query action which constitutes** step 2 and can be seen in Figure 13.

Layouts	Rules	Scrip	ts	Workflows	Functions	Message Destinations	Phases &								
Rules / F	RECORDED	FUTU	RE: De	estination IP	match from QI	Radar re-query									
	Display Na	me *	REC	ORDED FUT	URE: Destination	on II									
	Object 1	уре	Incid	lent											
	Condit	ions	Add	conditions ir	n which to invo	ke the rule. Add New									
Activitie	es														
	Orde	ered	Order	ed Activities	will be invoked	d in the order specified be	elow. They in								
	Workf	lows	Workf	flow Activities	s are started a	fter all Ordered Activities	complete.	ules	Scripts	Workfl	ows	Functions	Message Destinations	Phases & Tasks	Incident T
			REC	CORDED FUT	URE: Destination	on IP match from QRadar re	-query ×	RFC	ORDED FU	TURE: De	estinati	on IP match f	rom QRadar re-query		
	Destinat	ions	Trans	action Data	is posted to M	essage Destinations after	all Ordered								
			Selec	ct Destination	IS				Nan	ne * 🛛 🖡	RECOR	DED FUTURE	: Destination IP match from	n QRadar re-query	
									API Name	• <b>0</b>	ecorde	d_future_destir	nation_ip_match_from_qrad	lar_requery	
									Descrip	tion T	This wo destina Qradar	orkflow re-que tion IPs that a Offense esca	ries the QRadar databases are related to the source alation that match against source alating source alation	se for finding all the IP provided by the or at the Recorded Futur	iginal e TI.
									Object Ty	pe *	Incide	ent			
												_			

Figure 14: Steps 2-3 - Rule / Workflow

Rukhsar Khan, rkhan@rukhsarkhan.de

 $\mathbf{O}$ 

5 @ M 

This action is provisioned by a menu-item rule, also known as a semi-automation. A semiautomation requires user intervention to trigger the automation. In contrast to this a full automation is provisioned by an automatic rule that specifies one or more match conditions. If the match condition is true, the automation is triggered without user intervention.

Figure 14 is further elaborating on steps 2-3. On the left side of this illustration we can see that the rule RECORDED FUTURE: Destination IP match from QRadar re-query is calling a workflow. The workflow has only a single function. Functions have a pre-process script, a function processor and a post-process script.

```
inputs.ariel_sql_query = "select destinationip from events where inoffense(" +
    incident.properties.qradar_id + ") and qidname(qid) = 'Recorded Future IP
    match' GROUP BY destinationip START PARSEDATETIME('" + str(incident.
    discovered_date) + "') STOP PARSEDATETIME('now')"
    inputs.incident_id = incident.id
    inputs.source_ip = incident.properties.source_ip_address
    inputs.typ_flag = ''
```

Figure 15: Steps 2-3 – Pre-process script

The pre-process script above defines an input variable name (inputs.ariel\_sql\_query) and a corresponding value which in our case is a select statement for querying the QRadar Ariel database. Our select statement is simply searching for all destination IP addresses that are part of the incident's offense ID (incident.properties.qradar\_id) AND have a qidname equal to "Recorded Future IP match". Qidname is the name of the QRadar event, so we are matching only on events that have matched against the RF CTI. The query time range is further limited to the discovered date of the incident until now. Now is an Ariel Query Language function that specifies the current time. This input parameter is now taken into a function processor. A function processor is a Python script that can provide 3<sup>rd</sup> party system APIs and is able to integrate with these. In our example we have a function processor with the QRadar Python APIs. We are using this function processor to process our input parameter (select statement) and provide us with a corresponding result set.

```
1 for entry in results.events:
2 if entry is None:
3 break
4 else:
5 row = incident.addArtifact("IP Address", entry.destinationip, "Provided by
RECORDED FUTURE TI match")
```

Figure 16: Steps 2-3 – Post-process script

The result set is formatted as a JSON string and is eventually taken as input into our postprocess script (see Figure 16). The post-process script in our example is simply iterating over the result set and is creating an IP address artifact with the description "Provided by RECORDED FUTURE TI match" for every included destination IP address (see Figure 17). Resilient workflows, pre- and post-process scripts, function processors, the REST API and much more are described in detail under the IBM Resilient Developer portal (IBM Resilient Developer portal).

Summary		Descrip	tion									
ID Phase	3152 Stage1 Analysis	96 flows a match co	nd 141 eve ntaining Pro	nts in 18 ca ocess Create	itegories: Qu e	ick executi	ion of a series of	suspicious comn	nands pre	ceded by Red	corded Fut	ure IP
Severity Date Created Date Occurred Date Discovered		Tasks Automo Artifa	Details tive MITI cts	Breach RE ATT&CK	Notes QRadar I	Members Events	News Feed	Attachments	Stats	Timeline	Artifacts	Edit
Compromised Incident Type	MITRE	Search		0		9 D	3.184.220.29 vetails	9				Graph ent: All
People Created By Owner Members	<ul> <li>account functional</li> <li>account functional</li> <li>There are no members.</li> </ul>	Show Ty	25 v pe Address	<ul> <li>○ Va</li> <li>8</li> </ul>	alue	0	Created E Valu Typ	ad         11/27/2018 21           By         account function           ue         93.184.220.25           De         IP Address           Dn         Provided by R	:48 onal ECORDED F	UTURE TI match	>	ions
Related Incide	nts		P Address	9	3.184.220.2		Relate	As specified in	the artifact t	ype settings (curr	ently Relate)	
No related incident	S.		9 Address: Sc	purce 1	92.168.150.	203 11	/26/2018 21:14	As specified	in the artifa	ict type sett ▼	Û	

Figure 17: Step 4 – Result

Next, an automatic rule is triggered as part of step 5 if the following match condition is true: If an Artifact is created AND the Type is equal to IP Address AND its Description is equal to "Provided by RECORDED FUTURE TI match". As this condition is true in our example, a JSON message is sent to a queue named RF lookup on the Resilient message bus that triggers an action processor. See Figure 18.

Display Name	RECORDED FUTURE: TI lookup and	
Object Type	Artifact	
Conditions	Add conditions in which to invoke the rule. Clear All	
	All Any Advanced example: 1 OR (2 AND 3)	
	Type	+ 🛍
	Description v is equal to v Provided by RECORDED FUTURE TI match	+0
Activities	Artifact is created V	+ 🗈
Ordered	Ordered Activities will be invoked in the order specified below. They include: Add Tasks, Run Script, and Set Field. Add New	
Workflows	Workflow Activities are started after all Ordered Activities complete.	
	Select Workflows	

Figure 18: Step 5 – Automatic rule – RECORDED FUTURE: TI lookup...

In contrast to a function processor that is used when you want to write changes back into the Resilient platform efficiently, an action processor can be used when you need to trigger a script but do not necessarily need to write changes back into Resilient. As step 5 doesn't require this, we have chosen to call an action processor script by this rule. This script performs an IP lookup operation against the Recorded Future Connect API (Recorded Future)

in order to search for the detailed CTI for the two RF matched destination IP addresses 81.7.11.83 and 93.184.220.29 and loads the result set into the Postgres test database (step 6).

Figure 19 is displaying some details on the stored CTI for entity 93.184.220.29 (IOC). As you can see, the evidenceDetails key has a list of multiple rules that are providing intelligence around the IOC. Later in our solution we will be concentrating on the key relatedIpAddress because we want to verify the local relevance of all the provided related IP addresses for this IOC.



Figure 19: CTI – RECORDED FUTURE example JSON

### 3.1.2. Produce STIX bundle and fill data table – steps 7-10

As part of this solution "we are expressing the CTI provided IOCs in STIX Indicator SDOs and their local relevance in STIX Observed Data SDOs. We are further generating Sighting SROs in order to visualize that we sighted IOCs in the local context. We are also leveraging the Identity SDO in order to specify Recorded Future as an organization that we are receiving indicators from" (Operationalizing the MITRE ATT&CK framework for Security Operations, Threat Hunting and DFIR). In order to put the Identity SDO into a relationship with other SDOs we are making use of the Relationship SRO. For generating a visualized graph, we are finally creating a STIX bundle. A STIX bundle packages multiple STIX SDOs and SROs into a single entity which can be loaded into a STIX Visualizer (Oasis Open).

Figure 20 is illustrating with steps 7-10 how we are achieving the above goal. Step 7 is first of all re-querying QRadar in order to receive flow details on the previously RF matched IP addresses. These flow details are required to provide context around the local relevance. We are expressing the local relevance in a STIX Observed Data SDO and the RF matched IP addresses in an Indicator SDO. As QRadar currently doesn't provide result sets in STIX format, we need to convert the received QRadar JSON of step 8 into STIX. For this we are using a free IBM Python library called STIX Shifter (Github) that we have customized to our needs. We are then loading the flow details into a data table available in the Resilient incident (step 9). In step 10 we are further loading the STIX bundle into our Postgres test database.



# 3.1.3. Verify Related entities – only relevant Related IPs, hashes and domain names – steps 11-15

Figure 21 is illustrating steps 11-15 of our solution. Taking benefit of our actionable CTI, the goal is to verify the related IP addresses, hashes and domain names of the RF matched destination IP address 93.184.220.29 that have been part of its corresponding CTI. We are verifying all these related entities "against the QRadar Ariel database and are only considering the ones that have a local relevance, i.e. local-to-remote network traffic that matched against a related entity" (Operationalizing the MITRE ATT&CK framework for Security Operations, Threat Hunting and DFIR). Finally, we are taking those matching related entities into the Resilient incident's Artifacts tab.



Figure 21: Steps 11-15 – Functions diagram

On the top left corner of Figure 22 we can see that a menu-item rule under the name RECORDED FUTURE: Verify Related Indicators "that relates to an incident artifact has been provisioned. Once we trigger this action against an IP address artifact another window pops up (bottom left) where we have to define a start and end time for the QRadar query. We are no longer specifying the query start time as the incident discovered date as we want to extend our search window to a selective value" (Implementation – Related IP Addresses – steps 11-15) that allows us to go beyond the incident discovered date.

As you can see on the right side of this figure all the Related IP addresses and Related domain names are shown up. If related hash values were also part of the local findings, they would also show up in the Resilient Artifacts tab.



Figure 22: Steps 11-15 – RECORDED FUTURE: Verify Related Indicator...

### 3.1.4. "Create STIX knowledge and Its relevance graph – steps 16-21

Once we have all the relevant information handy, we eventually want to generate two graphs, a STIX knowledge and a relevance graph.

In order to generate the knowledge graph, we are first checking whether a related Threat Actor (step 16) has been provided as part of the CTI, and if yes, we are mapping it out to the MITRE Intrusion Set (step 17). Next we are searching recursively what tools and malware are utilized by that specific Intrusion Set. Then we are creating a STIX file that includes all the identified Tool SDOs and Malware SDOs along with the Intrusion Set SDO, all provided by MITRE. Next, we are further leveraging the CTI in extracting reports and generating a Recorded Future Identity SDO along with Report SDOs and loading these into the same STIX file. Finally, we are loading the STIX file that is representing the knowledge graph into the Attachments tab of our Resilient incident (step 18). See Figure 23 below" (Implementation – STIX knowledge and relevance graph – steps 16-21).



The goal with the knowledge graph is to consolidate as much as possible knowledge around a specific Intrusion Set or Threat Actor in a single graph. This allows us to learn very quickly how the Threat Actor is operating.

The goal with the relevance graph is to see at a single glance which CTI provided IOCs and their related entities do have a local relevance, how these are related to each other and what is the local context around these. The relevance graph is generated by pulling in and merging the previously created individual STIX bundles that are stored in our Postgres test database to a single larger bundle (steps 19-20). We also include a mapping of the relevant domain names and hash values to the corresponding Observed Data SDOs.

IP Add	ress 93.184	.220.29	11/27/2018 2	21:48	As specified	in the artifact typ	oe setti 💌	Ť.	xecution	of a series	of susp	icious d						A
IP Additant and	end time for the A	8.150.203 Action/Que	11/27/201	Add to QF	Radar Refere ECORDED F riel Query ED FUTURE	nce Set UTURE: Build	knowledg	IP address	Description 1683 flows a match conta Tasks Automotive Artifact	n nd 3500 events in : ning Process Crea Details Breach MITRE ATT&C S	21 categorie ate Notes XK QRad	s: Quick exer Members ar Events	cution	MITRE: T1059/Con Make Integrity provi MITRE: T1016/Net MITRE: T1059/Con MITRE: T1059/Con MITRE: T1082/Syst RECORDED FUTU RECORDED FUTU Action Status Workflow Status Close Incident Delete Incident	mand-Line Interface sioning work Configuration mand-Line Interface term Information Dis IRE: Destination IP IRE: QRADAR: Buil	e + Activit Discovery e covery <u>match fror</u> d Relevan	y field n QRadar ce Graph	re-
															Prove /	u under t	TUIUTU	C
			Drag file	e here		I	Up Maximum file	load File e size: 25 MB	Search	٩				Artifact Type: All	Date Created:	All → H	as Attach	Gr
earch C	C Show Task Atlachment	5	Drag file	e here	l	Jploaded By: All	Up Maximum file I Date (	Noad File e size: 25 MB Created: All	Search	Q				Artifact Type: All	Date Created:	All → H	as Attach	Gr
earch C	고 ) I Show Task Atlachment	s tupi	Drag file	e here	e Added	Jploaded By: All	Up Maximum fik Date (	oload File e size: 25 MB Created: All s	Search	٩				Artifact Type: All	Date Created:	NI - H	as Attachi	Gr
Search C Type d	Snow Task Attachment Name Knowledge graph 93.184.220.29.txt	م ب للوا <u>acc</u>	Drag file oaded By :ount function	e here	e Added 29/2018	/ploaded By: All	Up Maximum file I Date ( Actio	Noad File e size: 25 MB Created: All s	Search	Q				Artifact Type: All	Date Created:	NI + H	as Attach	Gr

Figure 24: Steps 16-21 – Build knowledge and relevance graph

The knowledge and relevance graphs are both generated by triggering a corresponding menuitem rule in the Resilient platform and for each of these two actions a separate file is loaded in the incident's Attachment tab. See Figure 24 above.

Figure 25 and Figure 26 are showing the two graphs, which need to get loaded into the STIX Visualizer by manually downloading the incident attachments to the file system of the local machine.



Figure 25: Steps 16-21 – knowledge graph



Figure 26: Steps 16-21 – relevance graph

All the nodes in the STIX Visualizer are a graphical representation of their corresponding STIX Domain or Relationship Object. If you klick on a node, the SDO or SRO details are shown on the right side of the browser tab. We have selected the Intrusion Set – APT28 – node in the knowledge graph. We can see an extract of the node details that are part of the Intrusion Set SDO provided by MITRE.

The way we have built the relevance graph is as follows:

- Create a Recorded Future Identity SDO as the root node of the tree.
- Create Indicator SDOs based on the RF matched destination IP addresses found in QRadar, which BTW have increased over time during our analysis.
- For every Indicator SDO, create a STIX pattern that searches for the Indicator IP address or any of its related IP addresses. E.g. ipv4-addr:value='93.184.220.29' OR ipv4-addr:value='205.185.216.42'. See Figure 27.
- Create Observed Data SDOs for every source-destination IP address relationship that is related to the Indicator SDO or any of its related IP addresses.
- Create a Sighting SRO in order to put an Indicator SDO into a sighting relationship with all its corresponding Observed Data SDOs.



Figure 27: Relevance graph – Indicator SDO

By clicking through the Observed Data SDOs of IOC 93.184.220.29 and its related IP addresses, we quickly found some suspicion (see Figure 28). The source-destination relationship 192.168.150.203  $\rightarrow$  205.185.216.4 (right column) is showing that the source IP has sent more than 4 MB in 3910 flows in about 150 milliseconds. This definitely needs some closer look. More specifically we need to understand what exactly has been sent and whether that was legitimate network traffic or a malicious data exfiltration.

	Selected Node
ld:	observed-data 6cb40327-641f-4c57-9725- c11b348db58f
Type:	observed-data
Flow End Time:	2018-11-28 22:44:33:619 +0100
Object Type	: network-traffic
Flow Start Time:	2018-11-28 22:42:38:124 +0100
Protocols:	tcp
Destination Packets:	464
Source Packets:	452
Destination Byte:	269772
Source Byte	: 41310
Source IP:	192.168.150.203
Destination IP:	93.184.220.29
Last observed:	2018-11-28 22:44:33:619 +0100
Created by:	identity0b3eb29a- d3de-4ff8-9246-6609d6c40fbd
First observed:	2018-11-28 22:42:38:124 +0100
Number	132.0

Figure 28: Relevance graph – Observed Data SDOs

25

"As we have learned, all the TTPs potentially used by a known MITRE Intrusion Set are put into relationship by the Relationship SROs that are provided as part of the ATT&CK framework. Since we have loaded the complete framework in STIX2 format in our Postgres test database, we can identify these TTPs recursively by verifying the relationships of the Intrusion Set" (Resilient Workflows and Playbooks).

A SOAR tool like IBM Resilient can further help us by providing workflows and playbooks in order to trigger additional automation actions and giving instructions to an analyst. Depending on which Intrusion Set / Threat Actor has been identified, a generic workflow can call another workflow in order to satisfy the analysis requirements implemented for the corresponding TTPs. E.g. Figure 29 is illustrating how a generic workflow named MITRE is calling the workflow MITRE: APT28 after identifying APT28 as the Threat Actor. The MITRE: APT28 workflow extract can be seen on the right side of this illustration. This workflow combines the creation of task instructions (e.g. MITRE: T1003/Credential Dumping, MITRE: T1056/Input Capture) that are provided to the analyst in the form of a playbook and the calling of another workflow named MITRE: T1059/Command-Line Interface (top right) that is triggering an automation script for additional data collection and enrichment for satisfying TTP # T1059 requirements.



Figure 29: MITRE workflow calls APT28 workflow

Figure 30 "is further elaborating on how the playbook that is eventually providing task instructions to the analyst teams looks like. Some initial triage task instructions are listed under the *Stage 1 Analysis* phase of the incident which are processed by the Security Operations team. Once completed, the incident is handed off to the Threat Hunting team for scoping the attack and developing further intelligence. As you can see, all the TTP task instructions regarding APT28 have been loaded into the *Stage 2 Analysis* phase of this playbook" (Resilient Playbook and automated actions for Threat Hunting and DFIR).

MITE	RE: Build k	knowledge graph and chee	ck the relevant Threat Actor	Complete and	Tasks				
etails	Notes Memb	pers Attachments			Task Name		Owner	Due Date	
etails					Edit Stage1 Anal	/sis - Security Ope	rations		
Owner Due Date		Unassigned	Creator Date Initiated	Rukhsar Khan 02/18/2019 14:36	*-MITRE: © FUTURE from QR:	RECORDED : Destination IP match adar re-query	Unassigned 🔻	O No due da	
Date Closed Instructions		02/18/2019 14:37 Steps 16-18: Go to the Artifacts tab, select the individu	al Destination IP addresses and triager the action "N	ITRE: RECORDED FUTURE: Build knowledge (	*-MITRE: D	RECORDED : Verify Related	Unassigned 🔻	⊘ No due d	
		address. The goal here is to map the rela knowledge graph. E.g. if the RF TI is prov	ted entities of the Recorded Future TI feed regarding viding a ThreatActor "APT28" as a related entity, this	uild a Ision-Set	Build relevance graph	Unassigned 👻	O No due d		
		SDO in the MITRE Att&ck matrix. If it find Intrusion-Set. Also, sightings and IntelCa attaches to the Incident. ( <i>This action is j</i>	s a match it recursively searches for all the relevant rds that are provided by Recorded Future CTI are als provided by an Action Processor script that is lis	at specific in a file that (ing) $\bigtriangleup$ and check Actor	Build knowledge graph k the relevant Threat	Unassigned 🕶	⊙ No due d		
		Note the Intrusion-Set name (root object	in the graph, which is the Threat Actor) and answer t	Stage2 Anal	Stage2 Analysis - Threat Hunting				
		Once the Threat Actor has been identified and hand the Stage2 Analysis off to the T	d, all the corresponding TTP instructions will be load hreat Hunting team.	ed into the Stage2 Analysis phase. Now you can	po ahead └──	THREAT HUNTING:	Unassigned <b>v</b>	⊙ No due d	
cident	Fields	(1770)			r interest	T1091/Replication Removable Media	Unassigned 👻	⊘ No due d	
Which Threat Acto been ide	een identified?	AP 128			MITRE:	T1193/Spearphishing ent	Unassigned 🔻	⊙ No due d	
					ſŶ ⊘ <sup>*</sup> MITRE: Link	T1192/Spearphishing	Unassigned 🔻	O No due d	
					C C KITRE: Relations	T1199/Trusted	Unassigned 🔻	O No due o	
						T1078/Valid Accounts	Unassigned 👻	⊙ No due c	
					A * MITRE:	T10E0/Command Line	Uppersigned =	O No duo d	

Figure 30: MITRE Playbook loads TTPs for APT28

## 3.2. Stage 2/3 Analysis

It is important to note that the Threat Actors are watching the endeavors of the Cyber defense community exactly in the same way as we are observing their movements. We expect that they will change their attack vectors once they know that we have identified these. This means that we need to be agile in Incident Response and quickly adapt to changing attack vectors.

Instructions Start the Threat Hunting engagement by beginning with the right preparations:

- 1. Load the Att&ck Navigator and activate the noted Intrusion-Set name (Threat Actor) in order to see all the relevant TTPs.
- Open the two file attachments regading the knowledge and the relevance graph in the STIX visualization tool in seperate browser tabs (file:///C: /cti-stix-visualization-master/index.html)
- 3. Work with the knowledge graph and gather as much knowledge as possible about the Threat Actor/Group, their motivations, their used TTPs, malware and tools.
- 4. Based on the MITRE Att&ck website learn more about the indentified TTP details.
- 5. Read analyst reports provided by Recorded Future and MITRE Att&ck.
- 6. Work with the relevance graph and understand the local findings, their context and based on the acquired knowledge try to identify suspicious relationships. Document suspicious source-destination relationships, domain names and hashes from the relevance graph.
- 7. Trigger the Artifact level action "CB RESPONSE: Threat Hunting" in order to populate the table TTP findings in the "MITRE TTP staging table" tab. 8. Switch to the Carbon Black Response UI and begin to search for corresponding processes to the findings under 6. E.g. work with a search filter
- "ipaddr:93.184.220.29 AND hostname:lenovo\_an AND domain:rapidssl.com" AND alliance\_score\_attackframework:[1 TO \*].
- 9. While conducting Threat Hunting as part of 8, follow the instructions specified in the individual TTP tasks.
- 10. Gather as much intelligence as possible by working through the MITRE TTP staging table.

11. When conducting the specific TTP analysis answer the key investigative questions provided in the TTP tasks. Please also answer the question "Which additional TTPs have been identified" below.

Figure 31: MITRE Threat Hunting preparations

Figure 31 is showing the details of the MITRE: Threat Hunting: Preparations task. The goal of this task is to identify additional TTPs that have been used by an attacker as part of the local compromise. Additional TTP tasks are loaded into the playbook once the question in the left bottom corner "Which additional TTPs have been identified" is answered. However, answering this question requires to first trigger the action CB Response: Threat Hunting demonstrated in Figure 32.

This action pulls in the findings of Carbon Black (CB) Response into a Resilient data table named "MITRE TTP staging table" via an integration with the Carbon Black API for Python (CBAPI). More precisely, we have activated the Threat Intelligence (TI) named "MITRE ATT&CK" within CB Response and configured it to generate alerts whenever some endpoint activity matches this TI.



Figure 32: MITRE TTP staging table - Threat Hunting

This allows the Threat Hunting team to triage the table details and switch to the CB Response UI as required in order to understand the individual TTP details by triggering ad-hoc queries and conducting live response.

Once the Threat Hunting team works through the individual TTP tasks and scopes the attack, it provides additional intelligence to the SecOps and DFIR teams. E.g. if it has identified that the attacker is about to exfiltrate data, they can advise the SecOps team to restrict the capabilities of the intruder. Also, as part of the scoping process the Threat Hunting team narrows down an attack to a few suspicious highly or confirmed compromised systems while scanning thousands or tens of thousands of endpoints.

When a small amount of confirmed compromised systems has been identified, an automated action for creating a memory dump of each of these endpoints helps the Threat Hunting team in handing these images off to the DFIR team. The DFIR team can then go for the deep dive forensic analysis and work on a strategy for a fullyfledged remediation, eradication and recovery process.

Figure 33 shows additional automated actions in IBM Resilient SOAR that aid in further streamlining the security and forensic analysis as well as restrict the capabilities of the intruder. E.g. the action CB RESPONSE: Create memdump creates a memory dump for the selected endpoint, VOLATILITY: Scan memory image allows to analyze the memory dump with the open source tool Volatility, A10:

Activate SSL interception and A10: Deactivate SSL interception enables and disables SSL interception on the A10 SSL interception proxy and the action A10: Block IP address allows to block an IP address as part of the containment process.

Show	25 💌					
	Туре	Value	Created	Relate?		Actions
	IP Address	192.168.150.203	03/21/2019 15:30	As specified in the artifa	ct type sett	<b>±</b>
A	IP Address	93.184.220.29	03/22/2019 09:46	As specified in A10:	Activate SSL interception Block IP address	
A	IP Address	209.197.3.15	03/22/2019 09:46	As spectied in A10:	Deactivate SSL interception	)
	Related domain name	ocsp.verisign.com	03/22/2019 09:51	As specified in MITR	E: RECORDED FUTURE: Build knowledg	ge graph
	Related domain name	ds.download.windowsupdate.com	03/22/2019 09:51	As specified in VOLA	TILITY: Scan memory image	
					VOI ATTI ITY: Scan memory image	×
					Hostname Ienovo_ari	
					Volatility Plugin pallet	Cancel Execute

Figure 33:Additional actions for SecOps, Threat Hunting and DFIR

# 4. Conclusion

Figure 34 Figure 35 summarize what we learned in this publication. Starting the investigation with a robust and actionable CTI is key. As analysts are progressing through the Stage 1 and Stage 2 phases of our solution, they need to stick on the CTI in order to remain focused. We've also learned what MITRE ATT&CK is about. More specifically we got acquainted with the human readable MITRE website in contrast to the MITRE framework provided in STIX2 for integration with an organization's Cyber defense ecosystem.

Robust and actionable Cyber Threat Intelligence
Holistic detection and response framework – MITRE Att&ck
Meaningful IOC expression language – STIX2, OpenIOC

Figure 34: Summary

We also learned that it's vital to do a proper incident or threat identification and scoping in order to understand the big picture, especially before starting with any remediation. Figure 35 is illustrating a six-step IR process communicated by the SANS institute (SANS institute). This process further refines the NIST IR process that we learned about earlier in this publication. As you can see, it especially emphasizes on the importance of the Identification and Scoping phase.



Figure 35: Summary continued

A Threat Hunting team can help an organization in this process. Also, a DFIR team can further help in conducting a deep dive forensic analysis on specific confirmed compromised endpoints and work on a fully-fledged remediation strategy in order to completely wipe out an attacker's foothold from the compromised environment. If an organization can't afford to engage a Threat Hunting or DFIR team, they can revert to a Threat Hunting or DFIR retainer.

30

# 5. References

- Forrester Now Tech. Forrester Now Tech: Security Automation And Orchestration (SAO), Q3 2018
- Github. *IBM/stix-shifter. (n.d.).* Retrieved from https://github.com/IBM/stix-shifter
- IBM Resilient Developer portal. *Resilient. (n.d.). Retrieved from* https://developer.ibm.com/security/resilient/
- MITRE ATT&CK. MITRE ATT&CK<sup>TM</sup>. (n.d.). Retrieved from <u>https://attack.mitre.org</u>
- MITRE MTR170202. *MITRE MTR170202 Finding Cyber Threats with ATT&CKTM Based Analytics*
- National Institute of Standards and Technology. *NIST Computer Security Incident Handling Guide*
- Oasis Open. STIX 2 Python API Documentation stix2 1.1.1 documentation. (n.d.). Retrieved from <u>https://stix2.readthedocs.io/en/latest/</u>
- Oasis Open. STIX Version 2.0. Part 4: Cyber Observable Objects. (n.d.). Retrieved from <u>http://docs.oasis-open.org/cti/stix/v2.0/cs01/part4-cyber-observable-objects/stix</u> v2.0-cs01-part4-cyber-observable-objects.html
- Oasis Open. STIX Version 2.0. Part 5: STIX Patterning. (n.d.). Retrieved from <u>http://docs.oasis-open.org/cti/stix/v2.0/cs01/part5-stix-patterning/stix-v2.0-cs01-</u> <u>part5-stix-patterning.html#\_Toc496717759</u>
- Oasis Open. STIX Viewer. (n.d.). Retrieved from <u>https://oasis-open.github.io/cti-stix</u> visualization/
- Recorded Future. *Recorded Future Connect API. (n.d.). Retrieved from https://api.recordedfuture.com/v2/*
- SANS institute. It's Awfully Noisy Out There: Results of the 2018 SANS Incident Response Survey
- The future of Security Operations. *Rich Mogull, Mike Rothman, Adrian Lane. (n.d.). Research - Papers. Retrieved from <u>https://securosis.com/research/papers/the</u> <i>future-of-security-operations*

Current Security Operations and DFIR problems. Retrieved from <u>https://www.rukhsarkhan.de/blog/current-security-operations-and-dfir-problems</u> Threat Hunting – a relatively new discipline in Cyber defense. Retrieved from <u>https://www.rukhsarkhan.de/blog/threat-hunting-cyber-defense</u> Operationalizing the MITRE ATT&CK framework for Security Operations, Threat Hunting and DFIR. Retrieved from <u>https://www.rukhsarkhan.de/blog</u> Solution draft. Retrieved from <u>https://www.rukhsarkhan.de/blog/solution-draft</u>

Implementation – Overview – steps 0-6. Retrieved from <u>https://www.rukhsarkhan.de/blog/implementation</u>

Implementation – Related IP Addresses – steps 11-15. Retrieved from <u>https://www.rukhsarkhan.de/blog/implementation-related-ip-addresses</u>

Implementation – STIX knowledge and relevance graph – steps 16-21. Retrieved from <u>https://www.rukhsarkhan.de/blog/implementation-knowledge-and-relevance-graph</u>

Resilient Workflows and Playbooks. Retrieved from <u>https://www.rukhsarkhan.de/blog/resilient-workflows-playbooks</u>

Resilient Playbook and automated actions for Threat Hunting and DFIR. Retrieved from <u>https://www.rukhsarkhan.de/blog/resilient-playbook-threat-hunting</u>

# 6. Acronyms and Glossary

Ariel Query Language: This is the name of the QRadar query language which has a SQL-like	Э
syntax	
CBAPI: Carbon Black API for Python28	
CERT: Computer Emergency Response Team2	
CSIRT: Computer Security Incident Response Team	
CTI: Cyber Threat Intelligence1	
DFIR: Digital Forensics and Incident Response1	
EDR: Endpoint Detection and Response5	
IPFIX: Internet Protocol Flow Information Export	
Reference Sets: A QRadar reference set is a reference table that can include objects like IP	
w addresses, hash values, domain names, etc. Reference sets can be populated manually or	
automatically by an app. E.g. the Recorded Future app loads risklists into reference sets. A	L
QRadar rule can then refer to a reference set in order to trigger an offense if for example a	n
IP address or hash value has matched against an entry in the reference set	
REST API: In computing, representational state transfer (REST) or RESTful is an	
architectural style used for web development. Systems and sites designed using this style	
aim for fast performance, reliability and the ability to scale (to grow and easily support	
extra users). To achieve these goals, developers work with reusable components that can be	e
managed and updated without affecting the system as a whole while it is running. Source:	
https://en.wikipedia.org/wiki/ Representational_state_transfer5	
RF: Recorded Future	
Risklists: Recorded Future can provide IOCs as part of a risklist. E.g. an IP risklist can	
contain hundreds or thousands of malicious IP addresses	
SDOs: STIX Domain Objects	
SIEM: Security Information and Event Management	
SOAR: Security Orchestration, Automation and Response	
SKUS: STIX Relationship Objects	
STIX: Structured Threat Information Expression	