Utilizing MISP into your Incident reponse plan

Dennis Rand - working at JN Data in Denmark

Cyber Security CrossFitter (incident responder) and Threat intelligence Analyst

JN Data is providing amongst other infrastructure and security services for financial sector

JYSKE BANK · Nykredit · SDC · BEC · bankdata · SILKEBORG DATA

eCrimeLabs

https://www.ecrimelabs.com

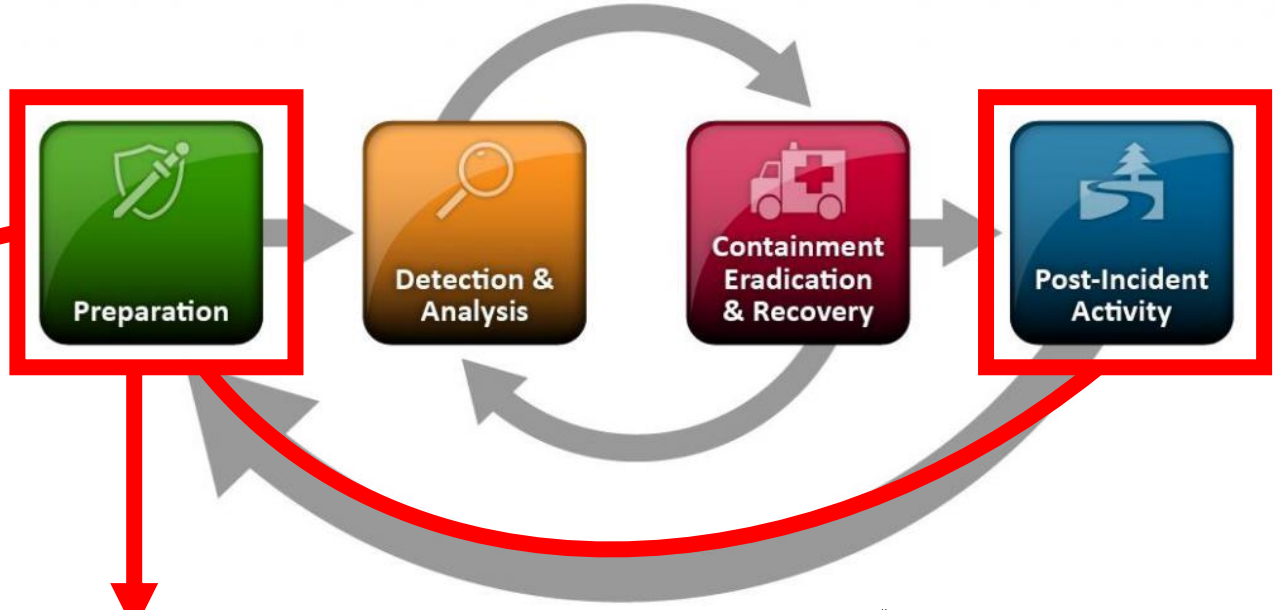
Founder of eCrimeLabs in Denmark,
and active MISP user since 2015

JN DATA

Use the statistical data

fraud-tactics

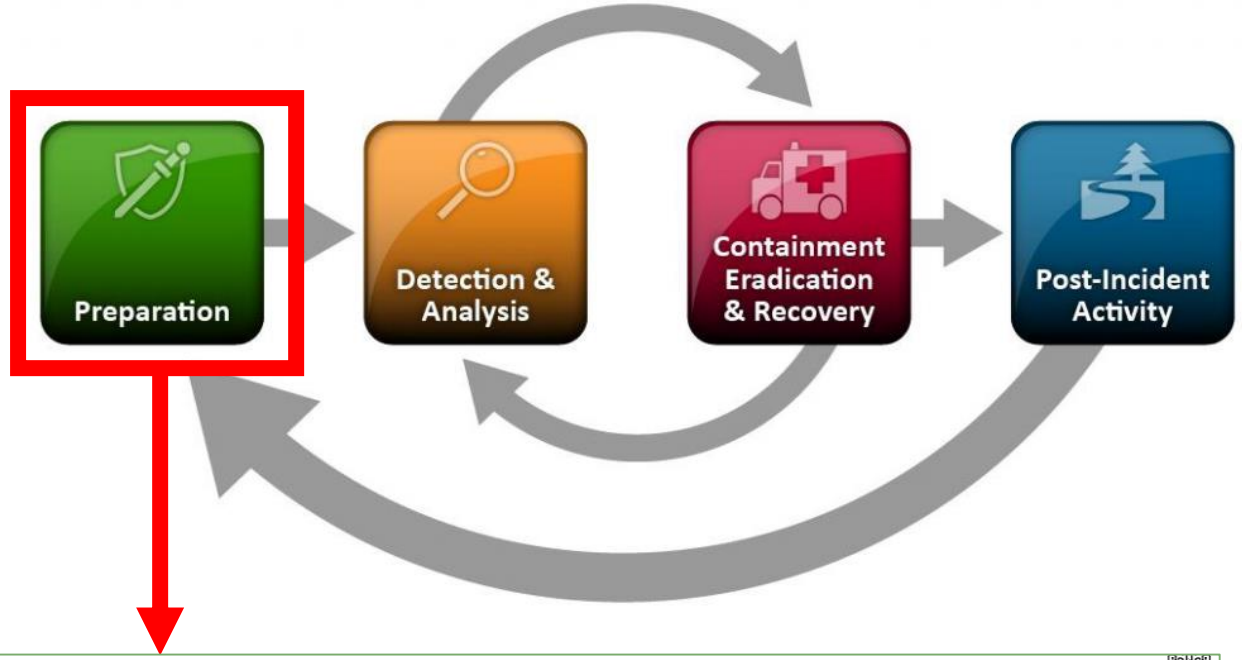
Initiation (7 items)	Target Compromise (4 items)	Perform Fraud (4 items)	Obtain Fraudulent Assets (4 items)	Assets Transfer (4 items)	Monetisation (6 items)
Phishing	Malware	CxO Fraud	Compromised Account Credentials	Fund Transfer	Fund Transfer
Spear phishing	ATM Black Box Attack	Business Email Compromise	Compromised Intellectual Property (IP)	Fund Transfer	ATM Explosive Attack
ATM Shimming	Account-Checking Services	Insider Trading	Compromised Payment Cards	Cryptocurrency Exchange	ATM Jackpotting
ATM skimming	Account-Checking Services	Scam	Compromised Personally Identifiable Information (PII)	SWIFT Transaction	Money Mules
POS Skimming					Prepaid Cards
Social Media Scams					Resell Stolen Data
Vishing					



mitre-mobile-attack | mitre-attack | mitre-pre-attack

Initial access (11 items)	Execution (33 items)	Persistence (59 items)	Privilege escalation (28 items)	Defense evasion (67 items)	Credential access (20 items)	Discovery (22 items)	Lateral movement (17 items)	Collection (13 items)	Command and control (22 items)	Exfiltration (9 items)	Impact (14 items)
Spearphishing Attachment	PowerShell	Registry Run Keys / Startup Folder	Scheduled Task	Deobfuscate/Decode Files or Information	Input Capture	File and Directory Discovery	Remote File Copy	Input Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
External Remote Services	Scheduled Task	Scheduled Task	Startup Items	Masquerading	Credential Dumping	Application Window Discovery	AppleScript	Data from Local System	Standard Application Layer Protocol	Data Compressed	Data Encrypted for Impact
Spearphishing Link	CMSTP	External Remote Services	Valid Accounts	Software Packing	Credentials in Files	Browser Bookmark Discovery	Application Deployment Software	Screen Capture	Uncommonly Used Port	Data Encrypted	Defacement
Valid Accounts	Exploitation for Client Execution	Hidden Files and Directories	Access Token Manipulation	CMSTP	Private Keys	Peripheral Device Discovery	Distributed Component Object Model	Automated Collection	Fallback Channels	Exfiltration Over Command and Control Channel	Disk Content Wipe
Drive-by Compromise	Regsvr32	Startup Items	Accessibility Features	DLL Side-Loading	Account Manipulation	Process Discovery	Exploitation of Remote Services	Clipboard Data	Remote File Copy	Exfiltration Over Physical Medium	Disk Structure Wipe
Exploit Public-Facing Application	Rundll32	Valid Accounts	AppCert DLLs	Hidden Files and Directories	Bash History	System Network Connections Discovery	Logon Scripts	Data Staged	Communication Through Removable Media	Scheduled Transfer	Endpoint Denial of Service
Hardware Additions	Scripting	.bash_profile and .bashrc	AppInit DLLs	Obfuscated Files or Information	Brute Force	Account Discovery	Pass the Hash	Data from Removable Media	Connection Proxy	Data Transfer Size Limits	Firmware Corruption
Replication Through Removable Media	User Execution	Accessibility Features	Application Shimming	Regsvr32	Credentials in Registry	Domain Trust Discovery	Pass the Ticket	Audio Capture	Custom Command and Control Protocol	Exfiltration Over Alternative Protocol	Inhibit System Recovery
Spearphishing via Service	AppleScript	Account Manipulation	Bypass User Account Control	Rundll32	Exploitation for Credential Access	Network Service Scanning	Remote Desktop Protocol	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Other Network Medium	Network Denial of Service
Supply Chain Compromise	Command-Line Interface	AppCert DLLs	DLL Search Order Hijacking	Scripting	Forced Authentication	Network Share Discovery	Remote Services	Data from Network Shared Drive	Data Encoding		Resource Hijacking
Trusted Relationship	Compiled HTML File	AppInit DLLs	Dylib Hijacking	Valid Accounts	Hooking	Network Sniffing	Replication Through Removable Media	Email Collection	Data Obfuscation		Runtime Data Manipulation
	Control Panel Items	Application Shimming	Exploitation for Privilege Escalation	Access Token Manipulation	Input Prompt	Password Policy Discovery	SSH Hijacking	Man in the Browser	Domain Fronting		Service Stop
	Dynamic Data Exchange	Authentication Package	Extra Window Memory Injection	BITS Jobs	Kerberoasting	Permission Groups Discovery	Shared Webroot	Video Capture	Domain Generation Algorithms		Stored Data Manipulation
	Execution through API	BITS Jobs	File System Permissions Weakness	Binary Padding	Keychain	Query Registry	Taint Shared Content		Multi-Stage Channels		Transmitted Data Manipulation
	Execution through Module Load	Bootkit	Hooking	Bypass User Account Control	LLMNR/NBT-NS Poisoning	Remote System Discovery	Third-party Software		Multi-hop Proxy		
	Graphical User Interface	Browser Extensions	Image File Execution Options Injection	Clear Command History	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Windows Admin Shares		Multiband Communication		

MITRE ATT&CK™



"Threat data can also be used in prioritization of vulnerabilities"

"If there is an exploit mentioned or publicly available, you should prioritize patching this; No matter what CVSS score or Risk level it is marked with"

Metasploit exploits with CVE assigned feed

Event ID	1350
UUID	5c6eea3c-fe10-43d3-902b-237d9742046f
Creator org	eCrimeLabs
Owner org	eCrimeLabs
Email	tip@ecrimelabs.net
Tags	+
Date	2019-02-21
Threat Level	Undefined
Analysis	Completed
Distribution	Your organisation only
Info	Metasploit exploits with CVE assigned feed
Published	Yes (2019-02-22 06:10:07)
#Attributes	1777
First recorded change	2019-02-21 18:13:16
Last change	2019-02-21 18:13:16
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Related Events

2018-09-09 (846) 2018-09-06 (1283) 2018-08-08 (21) 2018-08-01 (213) 2018-07-25 (1065) 2018-07-25 (1225) 2018-05-15 (175) 2018-01-31 (35) 2018-01-25 (1084) 2018-01-16 (864) 2017-12-04 (60) 2017-11-27 (1159) 2017-10-05 (1070) 2017-09-28 (163) 2017-06-20 (97) 2017-04-11 (500) 2017-03-31 (140) 2016-12-16 (1061) 2016-11-17 (644) 2016-11-07 (326) 2016-08-25 (1121) 2016-08-17 (1105) 2016-04-28 (377) 2016-04-22 (298) 2016-04-18 (968) 2016-01-12 (195) 2015-12-28 (476) 2015-09-28 (652) 2015-09-18 (353) 2015-08-24 (88) 2015-08-21 (742) 2015-08-10 (923) 2015-08-05 (349) 2015-06-30 (247) 2015-06-15 (236) 2015-06-11 (150) 2015-03-10 (662) 2015-01-11 (151) 2014-11-21 (115) 2014-11-13 (340) 2014-11-12 (1154) 2014-10-30 (1074) 2014-10-23 (429) 2014-10-09 (739) 2013-02-08 (568) 2012-04-16 (929)

Collapse...

Related Feeds

CIRCL OSINT Feed (1)
The Botvrij.eu Data (2)
Metasploit exploits with CVE assigned (54)

https://www.ecrimelabs.com/blog/2019/9/2/using-threat-data-in-your-vulnerability-management-strategy

https://feeds.ecrimelabs.net/data/metasploit-cve

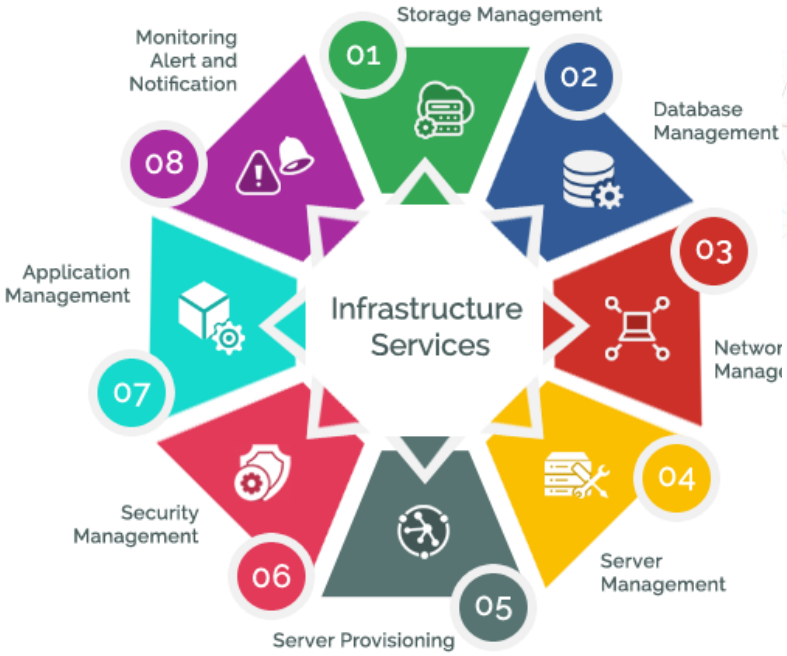
JN DATA

Be an incident responder superhero

Using your MISP as a SOAR platform

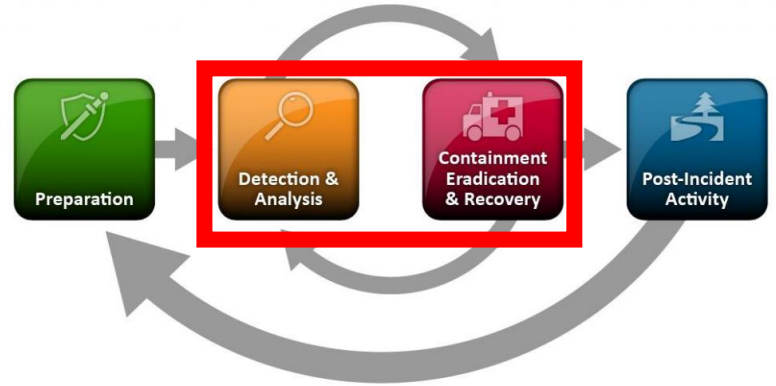
JN DATA

Challenge → Services + Governance x customers



On-Premises	IaaS Infrastructure as a Service	PaaS Platform as a Service	SaaS Software as a Service
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

Ensure coverage

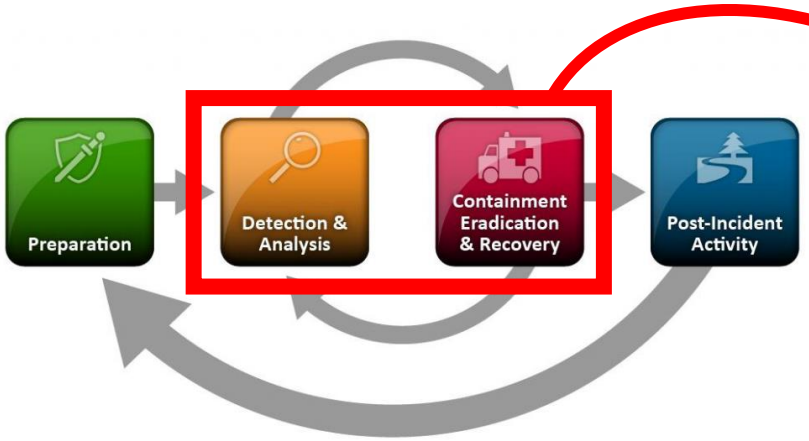


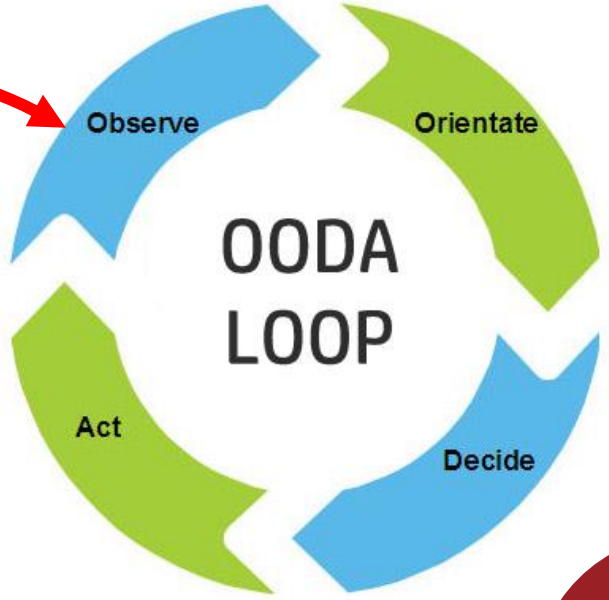
Network

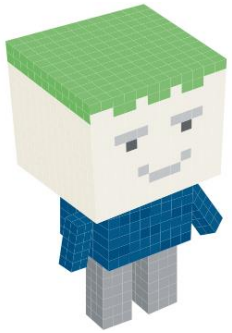
Endpoints

Logs

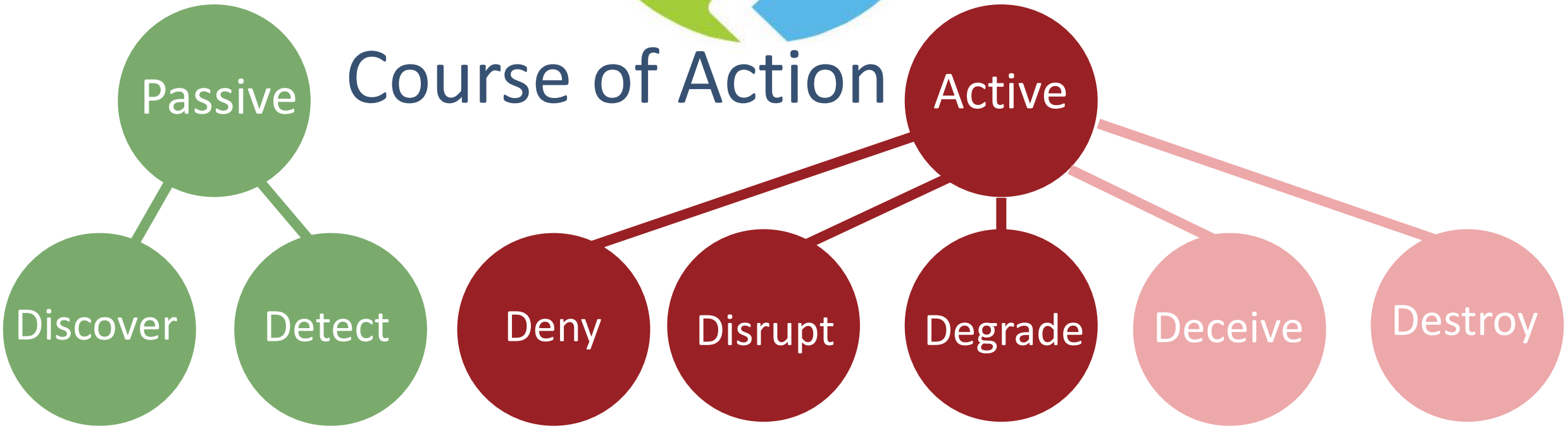
3 is the best,
2 is a minimum







Course of Action



https://github.com/MISP/misp-taxonomies/tree/master/course-of-action

Tagging to the rescue

Name	
jndata:incident-classification=alert	IDS=True, Published=False
jndata:incident-classification=block	IDS=True, Published=True
jndata:incident-classification=false-positive	
jndata:incident-classification=hunting	IDS=True, Published=False
jndata:incident-classification=incident	IDS=True, Published=False

Thank you for local tags, added in MISP 2.4.110

ALERT: Passiv - trigger alerts through SIEM/Log management (Event not need to be published)

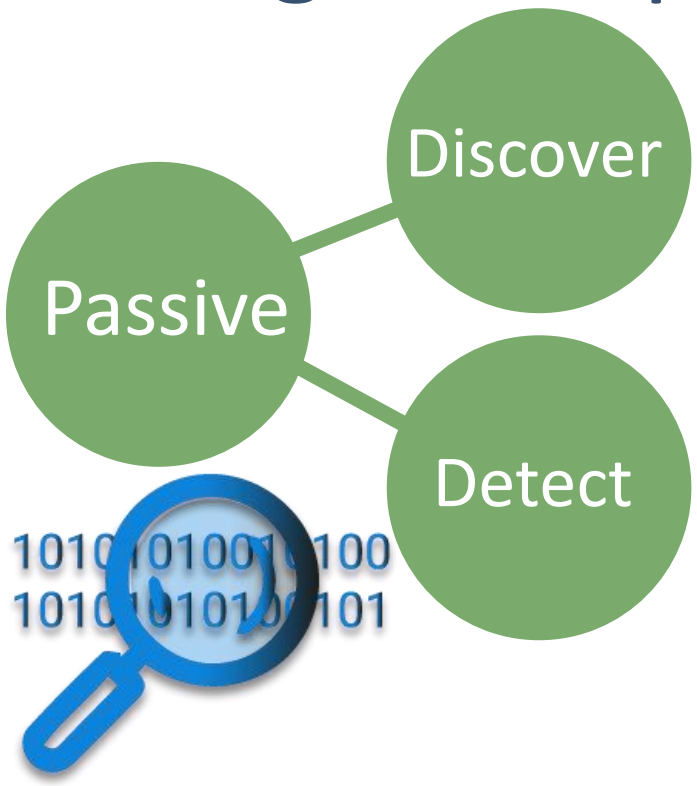
BLOCK: Active - Blocking in Firewalls, Proxies, etc. (Event published)

INCIDENT: Passive/Active (Event does not need to be published)

HUNTING: Do a retrosearch for attributes (Event not need to be published)

FALSE-POSITIVE: Exclude data from above, without having to delete

Using the capabilities during an incident

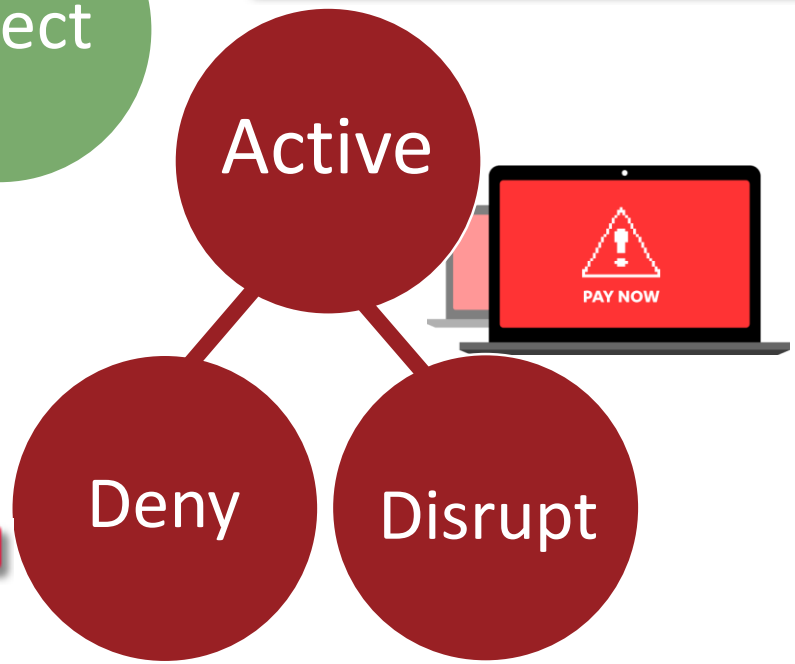


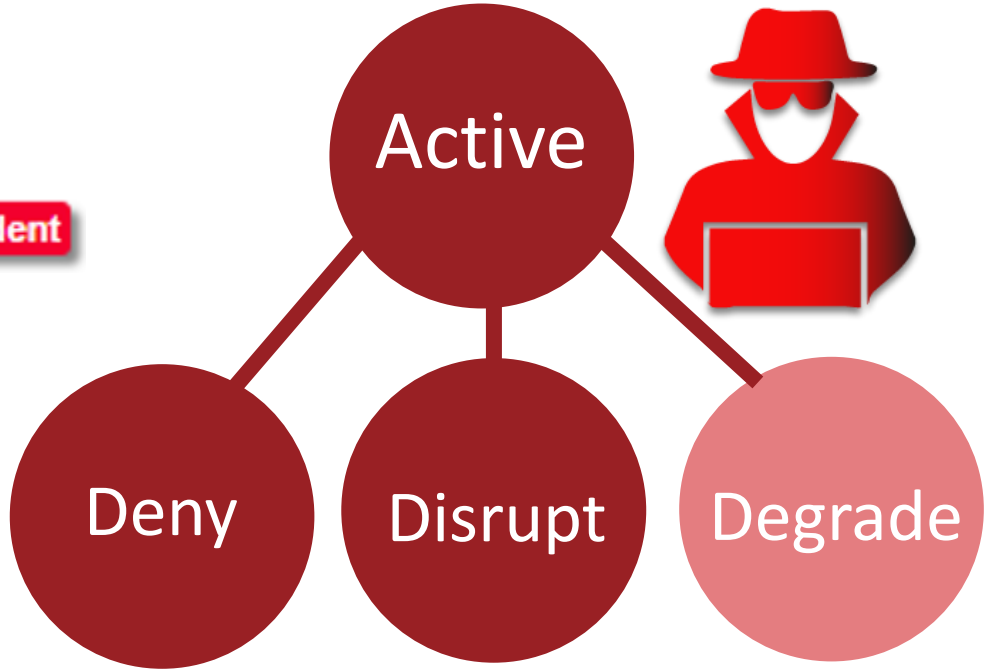
jndata:incident-classification=alert

jndata:incident-classification=hunting

jndata:incident-classification=incident

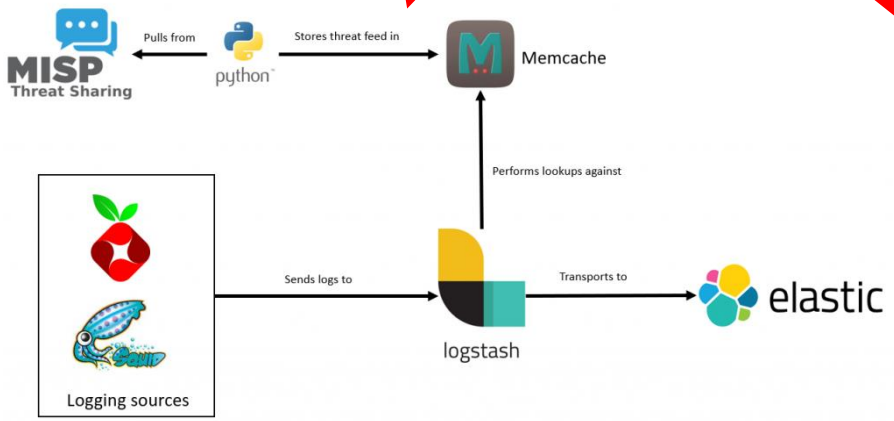
jndata:incident-classification=incident



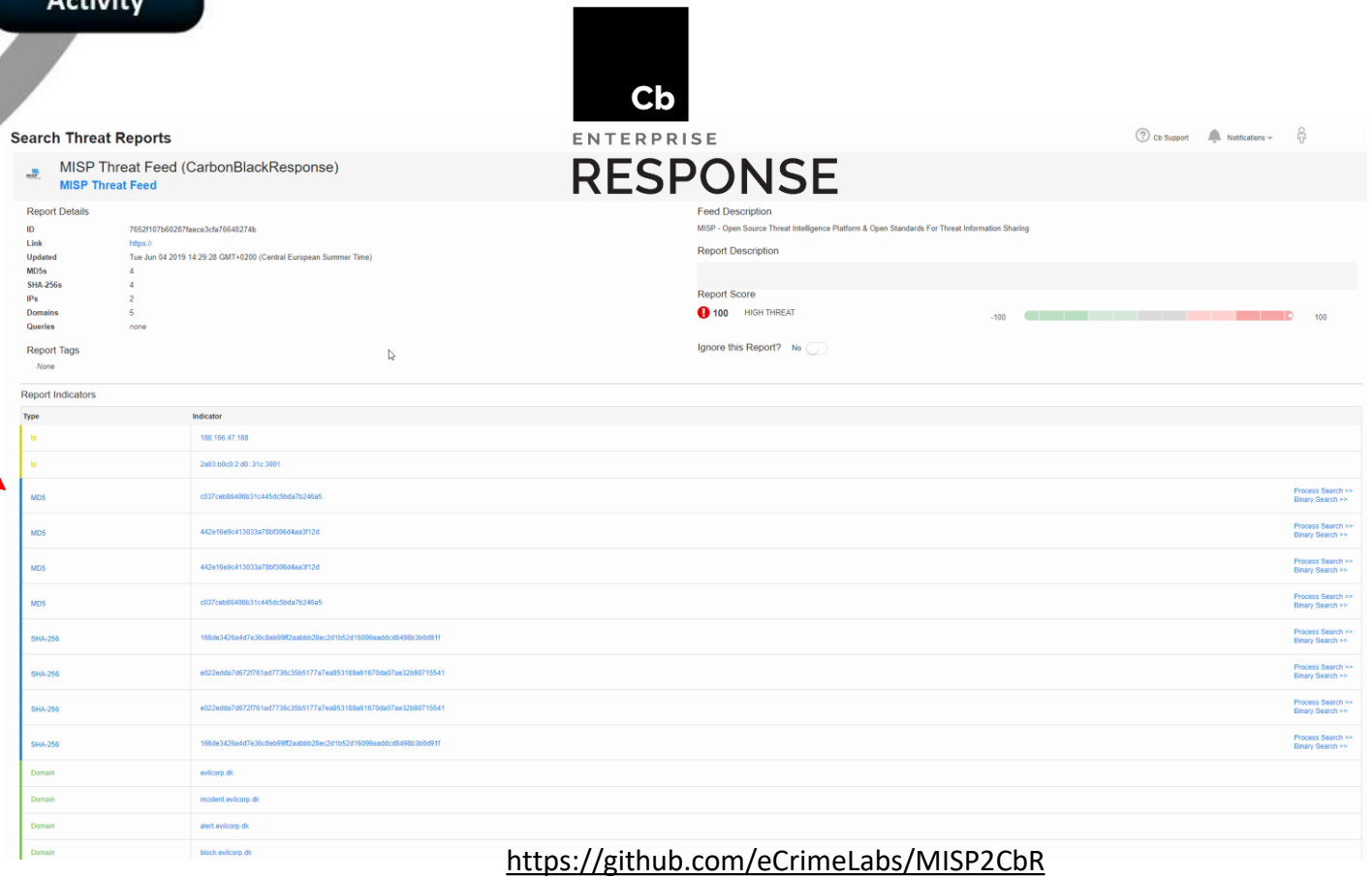


jndata:incident-classification=block

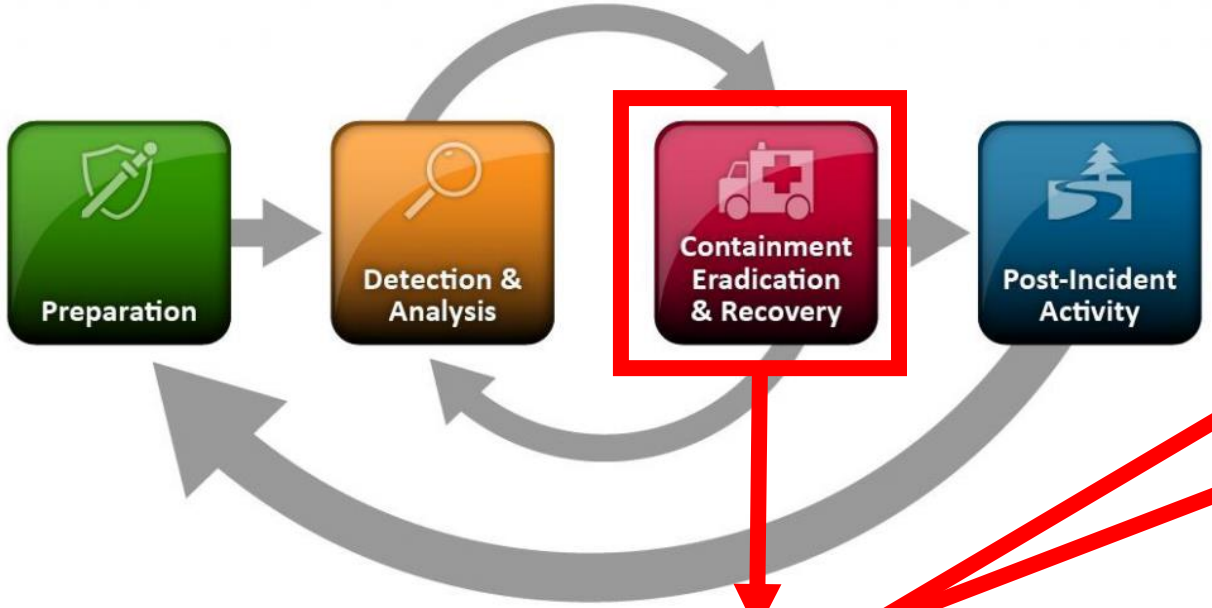
JN DATA



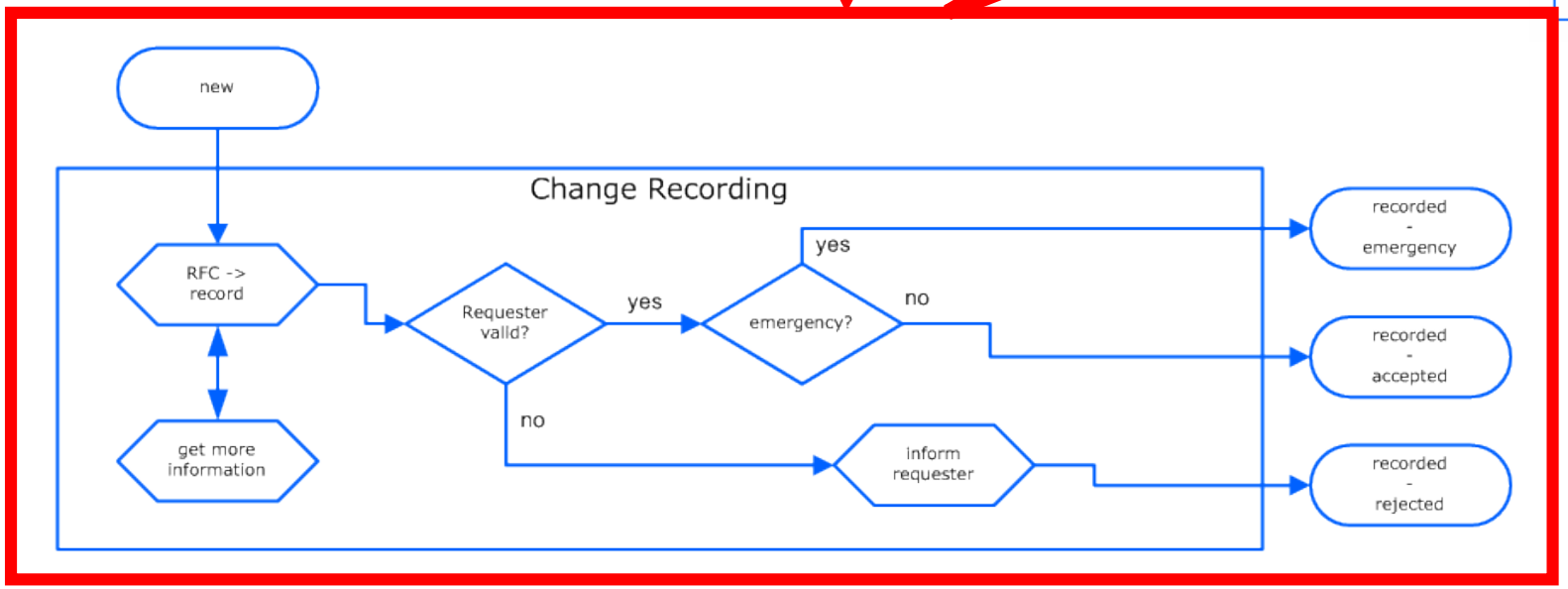
https://www.securitydistractions.com/2019/05/17/enriching-elasticsearch-with-threat-data-part-2-memcached-and-python/



https://github.com/eCrimeLabs/MISP2CbR

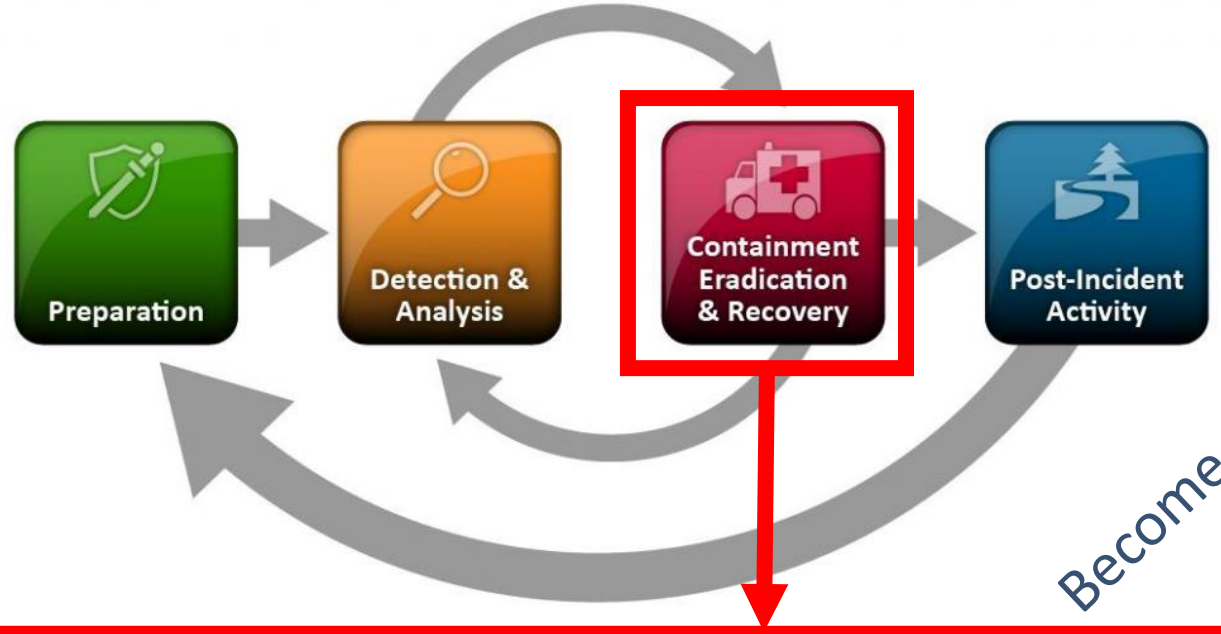


Change Priority #	Change Priority Name	Description
1	**emergency**	An accelerated authorization and planning procedure has to be performed in the case of an Emergency Change. The ECAB is responsible for the authorization and scheduling of this kind of changes.
2	**high**	If a potential damage exists, the change required for resolution of the related incidents or underlying problems/errors is often assigned a high priority. The existence of high-priority changes may result in reallocation of available resources for change planning and implementation.
3	**middle**	A medium-priority change is usually a non-time-critical change, providing the opportunity to be thoroughly planned. Often, Service Level Management is a main source of medium-priority changes, propagating service innovations or improvements
4	**low**	A low-priority change usually embodies a desirable, but not a necessary change.

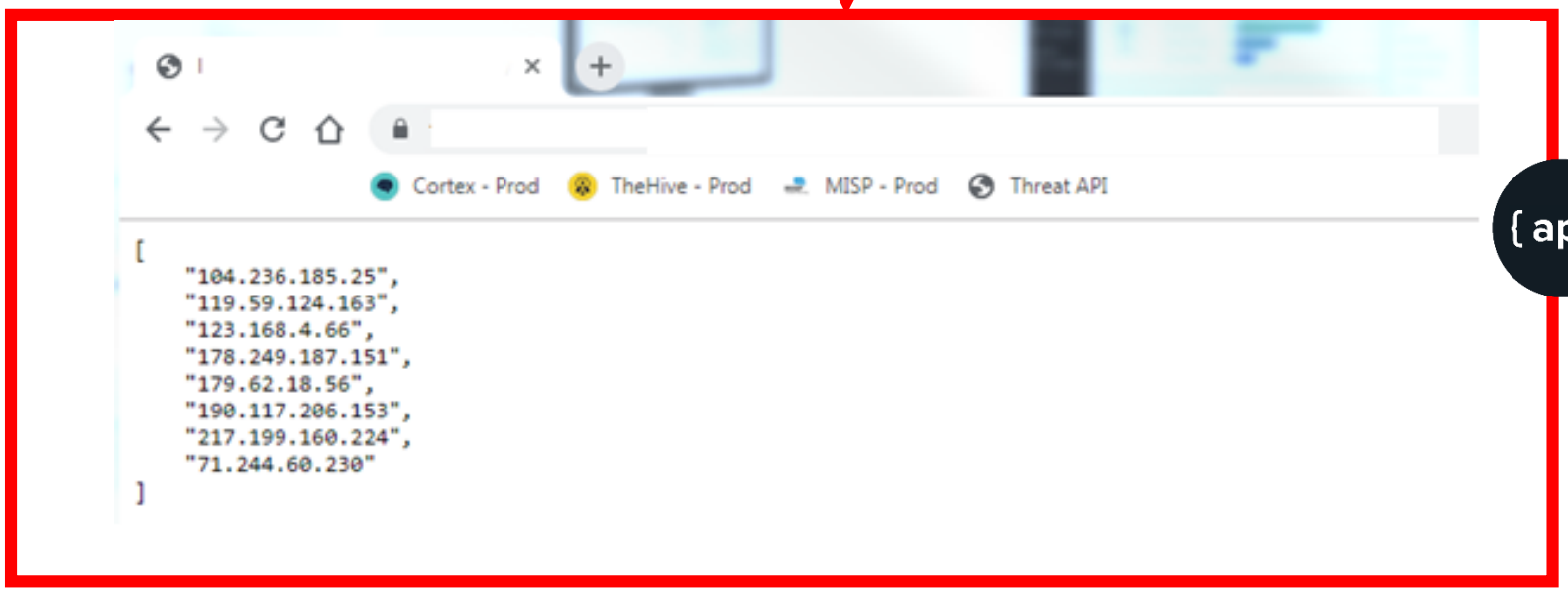


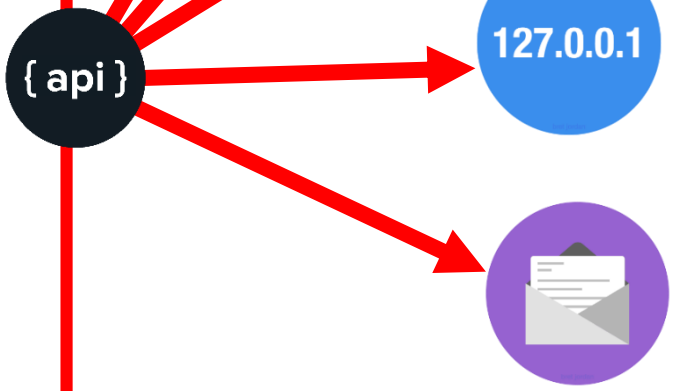
https://www.mitsm.de/change-management-en

JN DATA



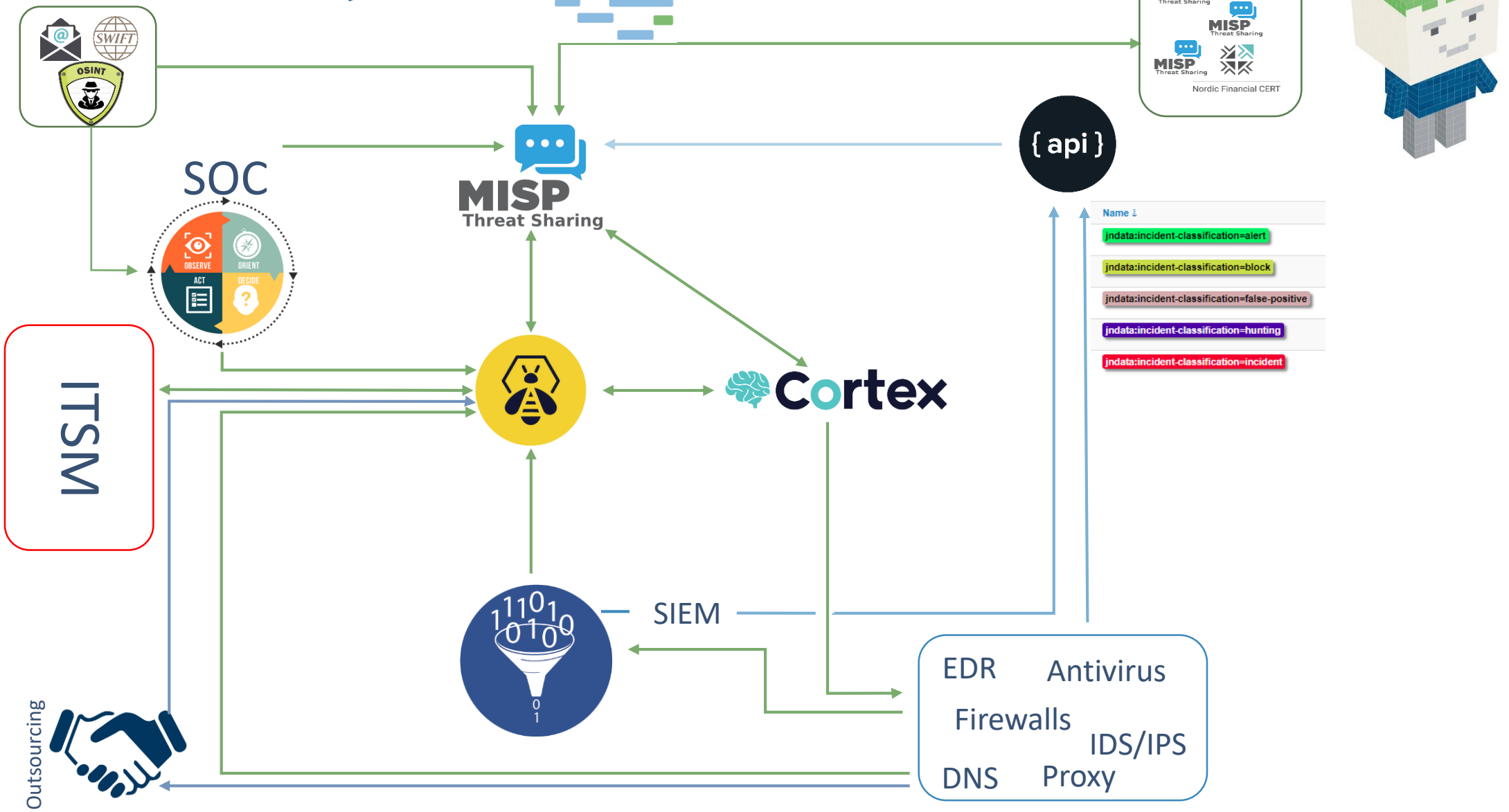
Become a feed vendor to your own organization.



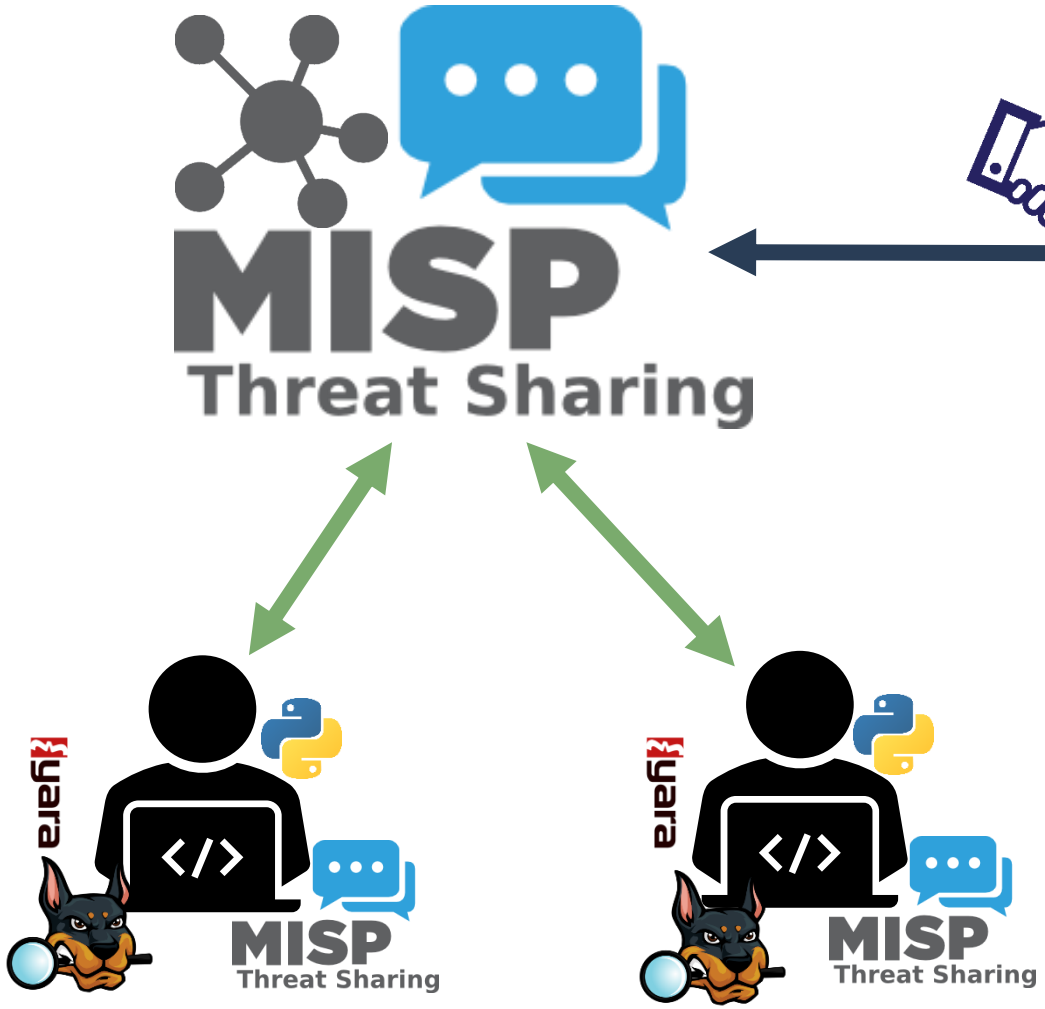


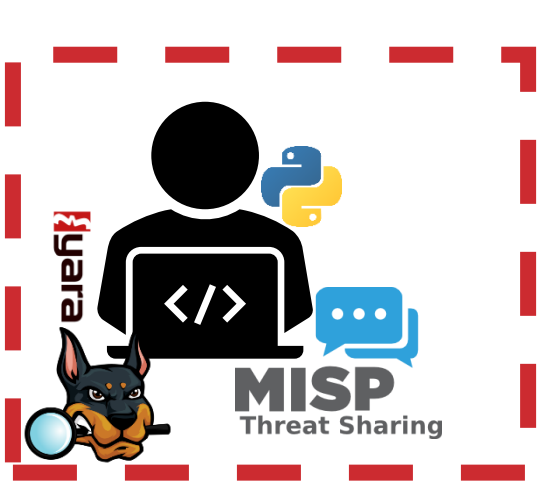
JN DATA

JN DATA Stack



Incident responders Go-Bag





At times you want to test

eCrimeLabs TIP - EvilCorp sample page

You have accessed this website using the following domain: **'misp.evilcorp.dk'**

This page can be used as a test page when implementation of the Threat API feeds in your security solutions.
The following IOC's has been mapped to this page, and can be used in MISP where Threat platform tags can be added.

The MISP event with the below information can be downloaded here and imported into your MISP instance: DOWNLOAD MISP EVENT

Domain:

- evilcorp.dk

Hostname:

- incident.evilcorp.dk
- alert.evilcorp.dk
- block.evilcorp.dk
- hunt.evilcorp.dk

URL's

- http://incident.evilcorp.dk/redpill/index.html
- http://alert.evilcorp.dk/redpill/index.html
- http://block.evilcorp.dk/redpill/index.html
- http://hunt.evilcorp.dk/redpill/index.html
- https://incident.evilcorp.dk/redpill/index.html
- https://alert.evilcorp.dk/redpill/index.html
- https://block.evilcorp.dk/redpill/index.html
- https://hunt.evilcorp.dk/redpill/index.html

eMail related

- no-reply@evilcorp.dk
- evilcorp.dk test subject

IP's

- 188.166.47.188
- 2a03:b0c0:2:d0::31c:3001

Files
Checksums of ecrimelabs_file.bin (text file)

- MD5: 442e16e9c413033a78bf306d4aa3f12d
- SHA1: 39730d06f0c5b89aa978564ff533387ac30175fd
- SHA256: e022edda7d672f761ad7736c35b5177a7ea853189a61670da07ae32b90715541

Checksums of ecrimelabs_test.exe (safe exe file)

- MD5: c037ceb86406b31c445dc5bda7b246a5
- SHA1: 8325c52cd197c9c3994fc52299c0b7a061962d7c
- SHA256: 166de3426a4d7e36c8eb99ff2aabbb28ec2d1b52d16099aaddcd8498b3b0d91f

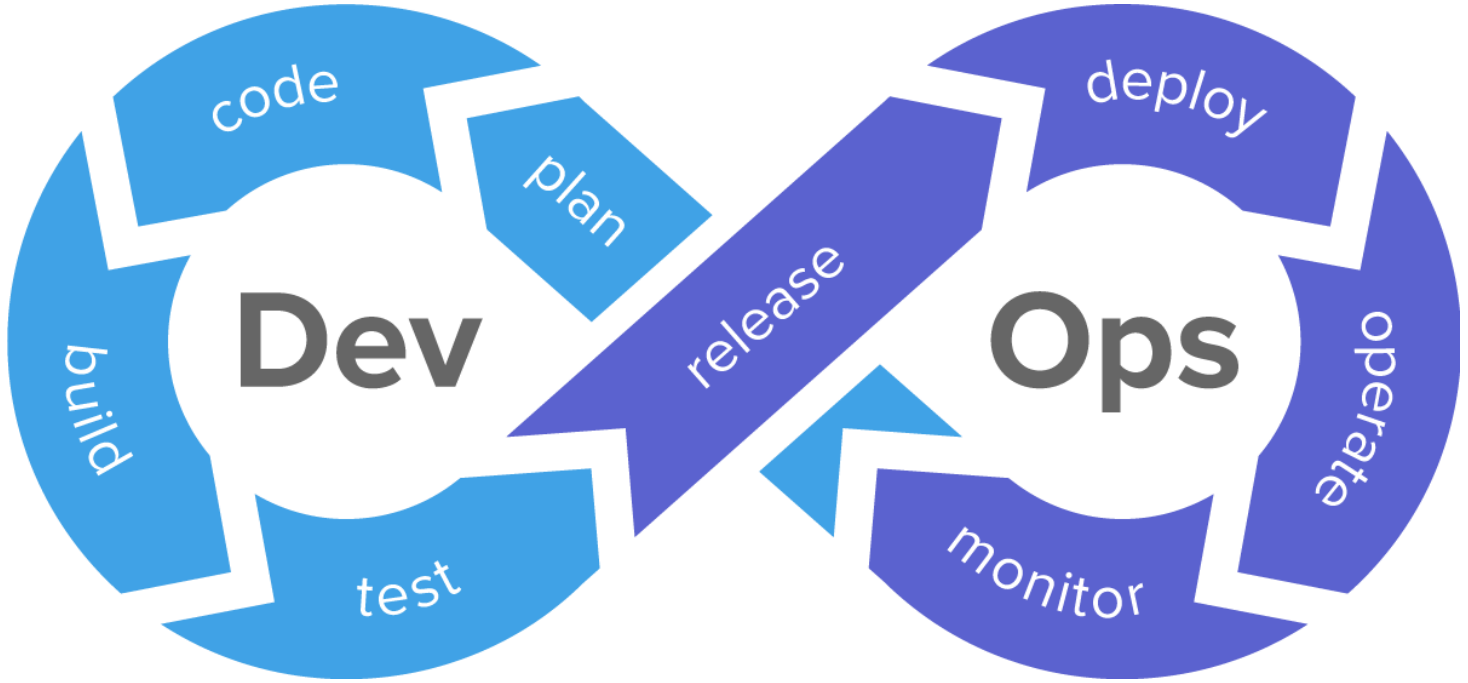
Mutex
Mutex of ecrimelabs_test.exe (safe exe file)

- eCrimeLabsTestMutex

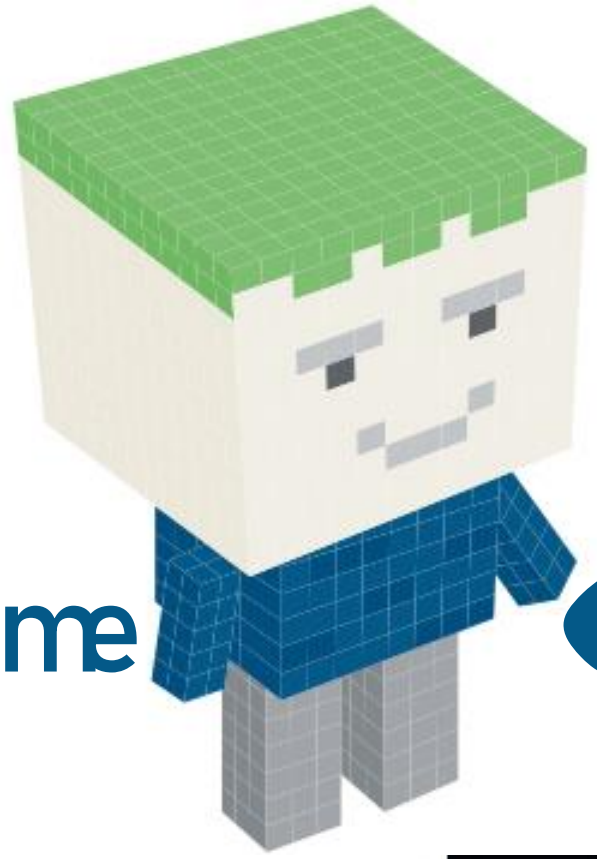
Yara
Yara rule ecrimelabs_test.yara (yara file)

- Can be used to detect ecrimelabs_test.exe

Certificate Fingerprint for the https version of this site (See URL's)



http://misp.evilcorp.dk



Thank you for your time

https://github.com/ecrimelabs

SharingisCaring

@DennisRand
@eCrimeLabs