Datasheet

uptycs

XDR Overview

Detections and Remediations

404 Wyman Street
Suite 357
Waltham, MA 02451
www.uptycs.com

Uptycs XDR covers four detection types:

Behavioral – Scan for MITRE ATT&CK techniques
Contextual – YARA scan of process memory and files
IOCs – Match against threat intelligence to identify known-bad indicators such as domains, IPs, file hashes, and JA3 fingerprints
Advanced – Scan for advanced attacks including process hollowing and DLL injection

Uptycs XDR also includes key forensic investigation capabilities:

Detailed historic telemetry available for further analysis, even if endpoint is offline.
Ability to **carve files and memory** from endpoints in real time.
Ability to **scan files and memory** with YARA rules in real time

	Behavioral Detections
What Is It?	Mapping to the MITRE ATT&CK Framework and analyzing behavior to detect various techniques and sub-techniques used in execution, persistence, privilege escalation, lateral movement, and more.
	Pre-built library of 1,000+ event and alert rules that cover **180+ MITRE ATT&CK** techniques across Windows, Linux, and macOS Ability to add **custom behavioral rules** **Correlation engine** to link multiple alerts and events into a single detection, to reduce alert fatigue & accelerate triaging Detection of **lateral movement** by looking at remote login activity related to suspicious / malicious events Monitoring of file events via **built-in FIM** capabilities Ability to tune rules to environment by adding **exceptions** Built-in **workflow management** tools (Assign, Add Notes, Close)
Advantages	1. By focusing on suspicious activities Uptycs can **uncover actual attacker** (human) activity, in addition to the malware involved e.g if an attacker wants to use net.exe to add a user we can detect it 2. Through a behavior-based approach, Security Analyst can easily arrive at a **baseline of alerts** normally seen in his organization's environment and **identify abnormalities** requiring deeper introspection 3. Behavioral detection of threats round-the-clock forms the basis for **Threat Hunting and Continuous Compliance**

	Examples
Windows OS	ATTACK_INHIBIT_SYSTEM_RECOVERY_T1490_WINDOWS_LOLBAS_ VSSADMIN - Vssadmin.exe execution detected for deleting shadow copies - **T1490 - Inhibit System Recovery** - Windows ATTACK_DEOBFUSCATE_DECODE_FILES_OR_INFORMATION_T1140_ WINDOWS_LOLBAS_ DOWNLOAD_DECODE_CERTUTIL - Certutil.exe execution detected to download and decode data - **T1140 - Deobfuscate/ Decode Files or Information** - Windows ATTACK_EXECUTION_T1560_WINDOWS_EXECUTABLE_FIM_LATERAL_ SYSTEM - Likely remote system process dropped portable executable file - **T1570 - Lateral Movement** - Windows
MacOS	ATTACK_CREDENTIAL_DUMP_T1555_MACOS_KEYCHAIN_MODIFY - Keychain file dumped to disk - T1555 Credential Dumping for macOS ATTACK_PERSISTENCE_T1037_MACOS_BOOT_OR_LOGON_FILE - Process added Boot or Logon Initialization Scripts - T1037 Persistence for macOS ATTACK_PERSISTENCE_T1159_MACOS_FILE_PLIST_LAUNCHDAEMONS - Process created plist file in LaunchDaemons - T1159 Persistence for macOS
Linux	ATTACK_CREDENTIAL_ACCESS_T1110.001_LINUX_PASSWORD_ GUESSING - Password guessing detected - T1110.001 Credential Access Linux ATTACK_IMPAIR_DEFENSE_T1562.004_LINUX_DISABLE_MODIFY_ FIREWALL - Process or script trying to alter firewall rules - T1562.004 Impair Defense Modify Firewall_LINUX ATTACK_PRIVILEGE_ESCALATION_T1548.003_LINUX_MODIFY_ SUDO_CONFIGURATION - Process trying to modify sudo configuration - T1548.003 Privilege escalation_LINUX

	Contextual Detections
What Is It?	Use YARA scanning for malware / toolkit detection based on rules curated by the Uptycs Threat Research and enriched with intel on top APT groups
Malware Covered	200+
APT Threat Actors	30+

Differentiating Features	• Uptycs performs highly optimized process memory scans on Windows and Linux endpoints/hosts to identify malware
	  • Scans are conducted on every new process that stays alive for 5 seconds (configurable) or more
	  • Scans are done on specific regions of memory to reduce asset overhead
	• For any OS that doesn't support process memory scan (e.g MacOS), process file scan is conducted on the binary based on the YARA rule
	• Ability for user to define custom YARA scan rules

	Examples
Mimikatz	Mimikatz is a post-exploitation tool that dumps passwords from memory and enables lateral movement within a network. (rule Uptycs_Mimikatz)
Whispergate	Whispergate is a wiper targeting Ukraine which overwrites the MBR (Master Boot Record) and files. (rule Uptycs_Whispergate)
Coinminer	Coin miner is an application that uses the infected device's physical resources to mine digital currency. (rule Uptycs_Coinminer)
Sysjoker	Sysjoker is a multi platform backdoor which targets windows, mac and linux operating systems. (rule Uptycs_Sysjoker)

	IOC Detections
What Is It?	Look for **indicators of compromise** in real-time and historical data (via Threat Books), using a **pre-curated** list of indicators from Uptycs Threat Research team or **custom lists uploadable** by users.
Indicators	~6M across 7 categories (e.g. malware, coinminer, phishing, DGA, unrecognized website)
Indicator Types	• Domain • IP • File hash • JA3 fingerprint
Differentiating Features	• Intelligence feed curated by Uptycs Threat Research team using open-source intel and primary research (sandbox analysis) • Daily updates to intelligence feed • Ad Hoc threat intelligence feed update support • Threat Books: Ability to look for new attacks with specific IoCs in historical data • Pre-built Threat Books for active campaigns • Ability to add custom indicators • Integration with VirusTotal
Advantages	1. By Curated intelligence from various sources allows for real-time alerts to be generated on most current threat indicators 2. Deeper detection intelligence by extracting additional insights (metadata) on potential malware via sandbox 3. Substantial reduction of false positives daily through automation, allowlist data from reliable sources, passive DNS data, and manual validation by the Uptycs threat intelligence team

	Examples
Async	Through a simple email phishing tactic with an HTML attachment, threat attackers are delivering AsyncRAT designed to remotely monitor and control its infected computers through a secure, encrypted connection. This campaign has been in effect for a period of 4 to 5 months.

	Advanced Detections (Beta)
What Is It?	Detection of advanced attacks (e.g. Ransomware, Keylogging) on the endpoint using correlation of system API calls.
Advanced Techniques	• Clipboard stealing • Credential dumping • DLL injection • Keulogger • MBR Attack • Process Hollowing • Ronsomware • Token Impersonation
Differentiating Features	• Logic built into endpoint agent to rapidly detect advanced attacks • Ability to intervene and block attacks in certain scenarios

	Examples
DLL Injection	Detection of a process is trying to load its code in another process via forced loading of a shared library, e.g. LD_PRELOAD on Linux
Process Hollowing	Detection when a process creates another in a suspended state, unmaps (hollows) its memory, and replaced with different (malicious) code

Remediation

Uptycs XDR comes with an array of features that empowers the user to apply remediation measures in real-time, through various modes:

- **Automatic:** Based on event rules and selected criteria
- **Manual:** Based on investigative outcome
- **Firewall Policy:** Based on IP Address, Port, Protocol and Application type

The platform offers remediation controls across multiple levels of user engagement:

a. **Highly Exclusive** (e.g Quarantine Host)

b. **Semi-Exclusive** (e.g Kill Container, Block outbound/inbound ports)

c. **Highly Granular** (e.g Kill Process, Delete File).

Automatic Remediation can be configured for specific events (via Event Rule Wizard) with the option to include multiple remediation paths in a particular sequence. Also, Asset Tags can be leveraged to apply specific remediation paths to certain groups/categories of endpoints and hosts. Manual Remediation can be invoked as corrective action taken on an

Remediation Capability	Linux	MacOS	Windows	Container
Process				
Pause / Resume	✓	✓	✓	✓
Kill Process	✓	✓	✓	✓
Pause / Stop / Kill Container	✓			✓
Networking				
Quarantine / Un-quarantine	✓	✓	✓	
Add / Delete Firewall Rules*	✓		✓	
File				
Delete	✓	✓	✓	✓
Permissions Update (UI Support - Coming Soon)	✓	✓		

Registry				
Revert Changes			✓	
Run Script				
Run Script**	✓	✓	✓	
Users				
Enable / Disable	✓	✓	✓	
Services				
Enable / Disable	✓		✓	
Restart / Start / Stop			✓	
Host				
Reboot / Shutdown	✓	✓	✓	
Restart osquery	✓	✓	✓	
Force Config Refresh for osquery	✓	✓	✓	

*Firewall Rules can be applied to block communications on the basis of local/remote IP Address and/or Port

** Scripts can be used for a diverse set of remediation steps related to information capture and diagnostics (e.g. downloading a hotfix & applying, finding all instances of a file and deleting, etc)

Blocking

Uptycs XDR comes with a host of blocking actions that can proactively protect IT assets from potential threats and attacks. The analyst can define a Blocking Policy based on specific attributes (path, certificate, binary hash, Yara rule) and matching criteria. Also, exceptions can be enforced for potential false positives, thereby removing the block.

In addition, Uptycs kubequery incorporates Gatekeeper as an admission controller. This can be used to block container/pod/object deployments that do not match desired criteria, e.g. block if image contains critical vulnerabilities, block if network ingress is set to wildcard match, block if privileged container etc. New policies can be added to the policy library, which provides a very flexible framework for blocking unwanted containers from being deployed.

Blocking Capability	Linux	MacOS	Windows
Process (Block / Allow / Log)			
Path Regex Match	✓	✓	✓
File Hash Match	✓	✓	✓
Certificate Signature Hash Match		✓	✓
Yara Rule Match	✓	✓	✓
DNS (Block)			
Domain Match		✓	

About Uptycs

Uptycs, the first unified CNAPP and XDR platform, reduces risk by prioritizing your responses to threats, vulnerabilities, misconfigurations, sensitive data exposure, and compliance mandates across your modern attack surface—all from a single UI. This includes the ability to tie together threat activity as it traverses on-prem and cloud boundaries, thus delivering a more cohesive, enterprise-wide security posture.

Start with your Detection Cloud, Google-like search, and the attack surface coverage you need today. Be ready for what's next.

Shift your cybersecurity up with Uptycs.

uptycs