FORENOVA

NOVAMDR

Alert Triage Playbook

Version: 1.0

Author: lucas salvatore

1. Verdict Priority Framework

Verdict	Definition	Typical evidence	Recommended action	Escalation
False positive	The detection fired, but the activity did not match the behavior it was designed to detect.	Incorrect rule match, bad parsing, duplicate event, or unrelated normal activity.	Close the alert and document the cause. Recommend detection tuning if needed.	Escalate recurring or high-impact false positives to detection engineering.
Benign or authorized	The activity was genuinely detected, but it was legitimate, expected, or approved.	Approved administrator action, scheduled vulnerability scan, authorized penetration test, or known business process.	Close or suppress according to policy. Record the user, tool, approval, and timeframe.	Escalate if the activity exceeds its approved scope or authorization cannot be verified.
Suspicious	The activity has concerning indicators, but there is not enough evidence to confirm malicious behavior.	Unusual login, encoded PowerShell, unfamiliar process, anomalous data access, or incomplete telemetry.	Gather more evidence, monitor related activity, and apply approved containment if risk justifies it.	Escalate to T2 when investigation is complex, risk is high, or evidence remains concerning.
Confirmed malicious	Evidence shows that the activity is unauthorized and harmful or part of an attack.	Known malware, confirmed credential compromise, ransomware behavior, malicious persistence, or verified unauthorized access.	Start the incident-response procedure. Contain affected accounts, devices, or indicators according to authorization and preserve evidence.	Escalate immediately to T2 or incident response and notify the customer according to the SLA.
Undetermined	Available evidence is insufficient to reach a reliable conclusion.	Missing logs, unavailable endpoint, incomplete timeline, or conflicting evidence.	Record what was checked, identify missing information, and continue the	Escalate if the potential impact is high or the

Verdict	Definition	Typical evidence	Recommended action	Escalation
			investigation or request customer input.	investigation cannot proceed at T1.

2. Common Alert Categories & Quick Triage

2.1. Upon detection, the following procedures could be taken

- Auto/Semi-Auto/Manual enrichment (gather contextual info, lookup IOC etc, make sure CSMs has all the neccessary info that the customer can react on that and then document them in the platform)
- Analyst triage (Verdict, Description, Recommendations) (Escalate if you don't have enough understanding of the alert to write these.)
- Customer notification (via CSMs)
- Containment recommendation or action (Quarantine virus, artifacts, scripts)
- Root-cause analysis (escalate to T3 when needed)
- Remediation tracking (escalate to T3 when needed)
- Executive summary (escalate to T3 when needed)

2.2. NovaMDR specific notes respecting the ground truths of NovaMDR

- Maliciou Defination: it describes an action, a http request or a ProcessOpen for example. when there is bad intention in it. any one can add a user, but what did they do with that user account, adding a user is not malicious. making it hidden is suspicious still not malicious.
- Botnet, trojan, Malicious DNS queries: Verify IOCs across multiple sources. Figure out what it really is as our threat intelligence feed is far behind.
- Port specific scan: ignore, detection rules deprecated.
- Brute force attack: rules deprecated, ignore.
- Crypto Mining: Be careful with traffic direction, investigate the source IP and the target IP, rule out the FPs eg: shodan miner pool probe

2.3. Malware / Malicious File

- **Check:** Hash reputation (VirusTotal, internal intel), file path, process tree
- **Verdict drivers:** Confirmed detonation? Sandbox result? Signed binary?

- **Common FP:** Known IT tools, custom scripts, legitimate installers

2.4. Command & Control (C2) Beaconing

- **Check:** Destination IP/URL reputation, beacon interval regularity, DNS patterns
- **Verdict drivers:** Known C2 infrastructure? Rare external destination? Encoded/encrypted comms?
- **Common FP:** CDNs, cloud services (AWS/Azure), telemetry/analytics endpoints

2.5. Credential Abuse / Brute Force

- **Check:** Source IP geolocation, failed vs successful count, user account type
- **Verdict drivers:** Successful logon after failures? Service account? Impossible travel?
- **Common FP:** Password rotation, MFA prompts, monitoring scans

2.6. Lateral Movement

- **Check:** Source/dest asset relationship, tool used (PsExec, WMI, RDP), time of day
- **Verdict drivers:** Unusual admin path? New service creation? Known attack toolkit?
- **Common FP:** IT admin activity, backup tools, management consoles

2.7. Scanning Activity

- to identify a scanner, if platform already put the scanner name in the alert title, then recoginize that, no matter what other info says otherwise, leave the worries to the ones who maintain the detection rules. if not in the title, judge from http headers: UserAgent

Tool	Attacker uses?	Install	Why
Nmap	✅ Yes	Trivial	Universal port/service scanning standard
Rustscan	✅ Yes	Easy	Fastest single-host port discovery
Masscan	✅ Yes	Easy	Internet-scale sweeps
Naabu	✅ Yes	Trivial	ProjectDiscovery fast SYN scanner, pipes into httpx
Zmap	⚠️ Rare	Moderate	Academic internet scanning; masscan preferred
Angry IP	❌ No	Easy	GUI hobbyist tool, not scriptable
Unicornscan	❌ No	Moderate	Obsolete, replaced by Rustscan/Masscan
Nuclei	✅ Yes	Trivial	CVE/misconfig templates, automated hunting
httpx	✅ Yes	Trivial	Web probing, pipeline glue
ffuf	✅ Yes	Trivial	Directory/content bruteforce standard

Tool	Attacker uses?	Install	Why
feroxbuster	✅ Yes	Easy	Recursive content discovery
gobuster	✅ Yes	Trivial	Dir/DNS/vhost bruteforce, preinstalled on Kali
katana	✅ Yes	Trivial	Modern web crawler by ProjectDiscovery
sqlmap	✅ Yes	Trivial	SQLi exploitation standard
Nikto	⚠️ Some	Easy	Legacy background check, noisy
Burp Suite	✅ Yes	Moderate	Manual web testing king
OWASP ZAP	⚠️ Some	Moderate	Free Burp alt, mostly CI pipelines
WPScan	✅ Yes	Easy	WordPress sites — huge attack surface
WhatWeb	✅ Yes	Trivial	Tech fingerprinting, preinstalled on Kali
Wappalyzer	✅ Yes	Trivial	Browser ext, passive fingerprinting
Acunetix	❌ No	Hard	Commercial defender tool
Netsparker	❌ No	Hard	Commercial defender tool
Dirbuster	❌ No	Easy	Dead since 2015
Nessus	❌ No	Hard	License + feeds + identity trail
OpenVAS/GVM	❌ No	Hard	30–60 min setup, defender infra
Qualys	❌ No	N/A	Enterprise SaaS
Rapid7 Nexpose	❌ No	Hard	Enterprise defender tool
subfinder	✅ Yes	Trivial	Passive subdomain enum
amass	✅ Yes	Easy	Deep subdomain enum
dnsx	✅ Yes	Trivial	DNS resolution at scale
Shodan CLI	✅ Yes	Easy	Passive — target never sees you
theHarvester	⚠️ Some	Easy	Email/subdomain OSINT, aging
Recon-ng	⚠️ Some	Moderate	OSINT framework, modules decay
BloodHound	✅ Yes	Moderate	AD attack path mapping, red team standard
CrackMapExec / NetExec	✅ Yes	Easy	Internal network Swiss army knife
Responder	✅ Yes	Trivial	LLMNR/NBT-NS poisoning, preinstalled
Impacket suite	✅ Yes	Easy	SMB/Kerberos attacks, essential
enum4linux-ng	✅ Yes	Trivial	SMB/AD enumeration
ldapdomaindump	✅ Yes	Easy	LDAP dumping post-foothold
Kerbrute	✅ Yes	Trivial	Kerberos user enum/password spray

Tool	Attacker uses?	Install	Why
PingCastle	⚠️ Rare	Easy	AD **auditing** — some attackers repurpose it
ScoutSuite	✅ Yes	Moderate	Multi-cloud misconfig audit
Prowler	✅ Yes	Moderate	AWS/Azure/GCP security checks
trivy	✅ Yes	Trivial	Container/IaC vulns, single binary
kube-hunter	⚠️ Some	Easy	K8s hunting
Pacu	✅ Yes	Moderate	AWS exploitation framework

- tools hackers use: 100% report

2.8. Privilege Escalation

- **Check:** Pre/post access level, token manipulation, group membership changes
- **Verdict drivers:** Service account misuse? UAC bypass? Exploited CVE?
- **Common FP:** Approved elevation workflows, scheduled tasks

2.9. Phishing / Malicious Email

- **Check:** Attachment/URL detonation, sender reputation, user click action
- **Verdict drivers:** Credential harvest page? Macro execution? URL shortener chains?
- **Common FP:** Simulated phishing, marketing campaigns, newsletter links

2.10. Anomalous Login / Impossible Travel

- **Check:** VPN/proxy detection, device trust, user behavior baseline
- **Verdict drivers:** TOR exit node? New device + new location? Off-hours?
- **Common FP:** Travel, VPN reconnection, mobile device

2.11. Data Exfiltration

- **Check:** Volume transferred, destination, protocol (DNS tunneling, HTTPS, ICMP)
- **Verdict drivers:** Bulk upload to unknown external? Sensitive file access + egress?
- **Common FP:** Cloud sync, backup services, approved file shares

2.12. Ransomware Indicators

- **Check:** Mass file rename, shadow copy deletion, encryption entropy
- **Verdict drivers:** Known ransomware hash? Double extortion behavior?
- **Common FP:** Archive tools, compression scripts

2.13. Vulnerability Exploitation

- **Check:** CVE match, patch status, network exposure, exploit in-the-wild status
- **Verdict drivers:** Exploit kit source IP? Exploitation post-compromise?
- **Common FP:** Vulnerability scanner traffic, authenticated scans

3. Enrichment Checklist (Before Verdict)

- **Intel match:** Hash/IP/domain in threat intel feeds?
- **Asset criticality:** Crown jewel? Production? Dev?
- **User context:** Admin, service account, executive, contractor?
- **Time correlation:** Aligns with other alerts in same window?
- **Behavioral baseline:** Is this normal for this user/host?
- **Network context:** Internal-only or egress to internet?