

# Understanding Declarations of Compromise<sup>®</sup> and Declarations of Policy Violations<sup>®</sup>

### High-fidelity Incident Events from Clear NDR®

#### **Executive Summary**

Clear NDR generates two critical types of events that represent high-fidelity, asset-oriented security incidents designed to streamline threat detection and incident response: Declarations of Compromise (DoC) and Declarations of Policy Violations (DoPV).

Both incident types share fundamental characteristics — they are asset-specific, highconfidence detections with near-zero false positives and provide comprehensive evidence collection for effective investigation.

**Declarations of Compromise (DoC)** focus on security threats, detecting serious and imminent dangers such as malware, lateral movement, and advanced persistent threats (APTs). DoCs dramatically reduce alert fatigue by identifying only the most critical threats that represent true organizational compromise, transforming millions of network events into focused, actionable incidents. Each DoC maps to specific phases of the cyber security kill chain and provides complete attack timelines from initial compromise through full blast radius analysis.

**Declarations of Policy Violations (DoPV)** address internal compliance and security policy enforcement, identifying unauthorized activities that may not be malicious but still pose organizational risk. These include insecure protocols, outdated TLS versions, vulnerable systems, and potential data leakage scenarios. DoPVs enable continuous, real-time compliance monitoring and governance oversight.

Both event types integrate seamlessly with existing security infrastructure through SIEM integrations and automated response capabilities via webhooks.

Organizations can create custom DoC and DoPV rules through an "escalation" process, extending built-in detection capabilities to address specific organizational needs.

The system supports automated response workflows including incident ticket creation, endpoint isolation, IP blocking, and SOAR playbook initiation.

### Overview

This paper describes two different types of high-fidelity asset-oriented incident events generated by Clear NDR: Declarations of Compromise (DoC) and Declarations of Policy Violations (DoPV). While they share many similarities – such as those listed below, they are intended for two different primary use cases.

The common characteristics of both DoC and DoPV are:

- Asset oriented a given DoC or DoPV can only be associated with only one asset. And the complete collection of evidence and insights are associated with the asset
- **High confidence, high-fidelity** each of the curated threat detection methods that can initiate a DoC or DoPV incident are designed to trigger only under conditions of an active incident
- Low noise while Clear NDR continues to record repeated detection events against a given asset, only the first one generates a DoC or DoPV and optionally initiates an automated response.
- Effective with the UI or SIEM the events sent to the SIEM contain information about the DoC/DoPV such as the status along with the first time and most recent time the threat was seen attacking the asset. Therefore, the value of DoC and DoPV can be leveraged in SIEM integrations as well as security teams who use the Clear NDR UI as their primary interface.
- **Built-in and/or customized** while Stamus Networks provides extensive built-in detections which are updated daily, users may create their own DoCs and DoPVs to suit the needs of their organizations.

The primary benefit of both DoC and DoPV is that it gives security personnel a clear starting point for what is important and worthy of investigation.

# Declaration of Compromise (DoC)

A Declaration of Compromise is the high-fidelity **security incident event** in Clear NDR. Examples may include the observation of malware, lateral movement, or advanced persistent threats (APTs) associated with a specific asset (e.g. host) in the network.

#### Powerful Security Alert Noise Reduction

The power of the DoC is that it gives security personnel a clear starting point for what is important and worthy of investigation. The diagram below illustrates this concept more clearly for a typical deployment of Clear NDR monitoring a 10 Gbps network connection.

# Threat Detection Event Reduction with Declarations of Compromise<sup>®</sup> in Clear NDR<sup>®</sup>



You can see that, while Clear NDR collects extensive network metadata and discrete threat detections, it simplifies the incident responder's job by identifying the most serious and imminent and true positive threat events – those that represent a true compromise to the organization, issuing a confident '**declaration**' of compromise.

### The Anatomy of a DoC

The high-fidelity threat detection algorithms in Clear NDR are called "detection methods" or simply "methods." Most can be associated with threat families and named threats. See the diagram below:

### Hierarchy of Named Threats in Clear NDR®



These detection methods can initiate a DoC or DoPV incident and are designed to trigger only under conditions of an active incident. These individual high-fidelity detection events are logged in the Clear NDR Probe, and they are called "Stamus Events" in the user interface and "Stamus Events" in the API.



A DoC event is created when the first Stamus Event is logged against an asset, such as a HOST or USER. DoC events are created in the Clear NDR Central Server.

Subsequent occurrences of Stamus Events for the same Named Threat on the same asset are logged, but they do not trigger a new DoC.



Each specific named threat is associated with a phase of the cyber security kill chain. And the kill chain phase of the asset is determined by the kill chain phase of the threat which is attacking it.



A given asset may be "compromised" by more than one threat, and as such may be subject to more than one DoC. When an asset is under attack by one or more threats, Clear NDR logs each of them. The asset will be placed in the highest kill chain phase based on the threats associated. Here's an example threat visualization from the Clear NDR UI that illustrates this point.



NOTE: Each one of the event records is accompanied by its associated evidence – including network protocol transaction, anomaly, and flow logs along with the packet capture file (PCAP).

### Threat Coverage

Clear NDR recognizes many different types of threats. The current coverage map of threat families that can trigger a DoC is shown in the Clear NDR screenshot below.

MPROMIBEB > COVERAGE									
tamus Threat Resea	rch								
meat Families Threat Sear	ch								
APT		BACKDOOR		BOTNET		COVERT CHANNEL		CRYPTOCURRENCY	
Covered threats Detection methods	(55 (864)	Covered threats Detection methods	62 800	Covered threats Detection methods	94 918	Covered threats Detection methods	0 0	Covered threats Detection methods	6
CUSTOM THREATS		CVE		DATA THEFT		DOWNLOADER		EXPLOIT KIT	
New victims Covered threats Detection methods	<b>8</b> 00 6	Covered threats Detection methods	0	New victims Covered threats Detection methods	(11)	Covered threats Detection methods	38 (11)	Covered threats Detection methods	8
SENERIC CNC		LATERAL MOVEMENT	r.	LOADER		MOBILE BACKDOOR		OFFENSIVE TOOLS	
Covered threats Detection methods	0	New offenders New victims Covered threats Detection methods	<b>0</b> 0 0	Covered threats Detection methods	3) 639	Covered threats Detection methods	0	New victims Covered threats Detection methods	9 27 783
PENTEST TOOLS		PHISHING		RANSOMWARE		RAT		REVERSE SHELL	
Covered threats Detection methods	6	New victims Covered threats Detection methods	(1) (2) (2)	Covered threats Detection methods	60 (21)	Covered threats Detection methods	157 78k	Covered threats Detection methods	8
ROOTKIT		SOCIAL ENGINEERIN	G	SUPPLY CHAIN ATT	АСК	TROJAN			
Covered threats Detection methods	8	Covered threats Detection methods	0 (5)	Covered threats Detection methods	8	Covered threats Detection methods	230 9110		

Within a given threat family such as "Ransomware", there may be as many as 70 or more individual named threats. Here's a screenshot from the "Ransomware" coverage page in the Clear NDR UI.

tamus Threat Research				
APT	BACKDOOR	BOTNET	COVERT CHANNEL	CRYPTOCURRENCY
Covered threats 155 Detection methods 18.43	Covered threats 02 Detection methods 000	Covered threats (34) Detection methods (918)	Covered threats (2) Detection methods (3)	Covered threats Detection methods
CUSTOM THREATS	CVE	DATA THEFT	DOWNLOADER	EXPLOIT KIT
New victims 2 Covered threats 1 Detection methods 3	Covered threats Detection methods	New victims (20) Covered threats (247) Detection methods (18.4 k)	Covered threats (8) Detection methods (13)	Covered threats Detection methods
GENERIC CNC	LATERAL MOVEMENT	LOADER	MOBILE BACKDOOR	OFFENSIVE TOOLS
Covered threats (2) Detection methods (855)	New offenders New victims Covered threats Detection methods	Detection methods	Covered threats O Detection methods O	New victims Covered threats Detection methods
PENTEST TOOLS	PHISHING	RANSOMWARE	RAT	REVERSE SHELL
lovered threats (3) Netection methods (3)	New victims Covered threats Detection methods	Covered threats (80) Detection methods (221)	Covered threats (157) Detection methods (78%)	Covered threats Detection methods
ROOTKIT	SOCIAL ENGINEERING	SUPPLY CHAIN ATTACK	TROJAN	
overed threats	Covered threats Oetection methods	Covered threats 2 Detection methods (6)	Covered threats (212) Detection methods (214)	

The DoC event is logged when Clear NDR detects that an asset is under attack by one of the curated threat detection algorithms or rules that are known to trigger with very high accuracy (nearly zero false positives) and pose an extreme danger to the asset under attack. We call these, "detection methods."

Stamus Networks includes an updated set of these curated DoC algorithms in the daily Clear NDR threat detection updates.

### Custom DoCs

In addition to those built-in and included in the daily threat detection updates, users may create their own through a process known as "escalation," whereby the results of an investigation or hunt can be turned into a DoC rule. These custom DoCs may be used for real-time detection in future network traffic or applied retroactively to historic data.

### Custom DoCs

In addition to those built-in and included in the daily threat detection updates, users may create their own through a process known as "escalation," whereby the results of an investigation or hunt can be turned into a DoC rule. These custom DoCs may be used for real-time detection in future network traffic or applied retroactively to historic data.

#### Viewing the DoCs in the Hunt and Investigation Console

Sometimes it becomes important to view all the DoCs and all the assets under attack from one summary screen. To view all DoCs from the Clear NDR Hunting dashboard, toggle the event times "Detection" and "Sightings" to the off position, add a filter to remove the events in the "policy violation" phase of the kill chain. See instructions below. Further filtering can be performed to investigate one or more of the assets under attack.



Using the same mechanism, users may also use filters to proactively create a custom DoC for events not yet seen in the network. For example, a user might create a custom DoC by creating a filter to identify an attempt to exploit a particular CVE that is known to be a vulnerability in the environment.

### How to Identify DoCs Using a SIEM Query

Below is an example of how to query your SIEM for a DoC. The query uses "Event Type = Stamus" and the negation to exclude those "Stamus events" that are not yet associated with a kill chain phase (DoPVs).

Query:

#### "event\_type":"stamus" + !(NOT) "kill\_chain":"pre\_condition" + unique incident\_id

This will return the DoC JSON log entry that includes Stamus Event information. See example below.

```
"stamus": {
 "extra info": null,
 "source": "62.204.41.23",
 "family name": "Lateral Movement",
 "incidents_id": [71],
 "threat id": 399,
 "asset net info": "wifi-users-hq.organization-acme",
 "pk": 3581,
 "asset info": {
  "last seen": "2025-07-24T02:40:34.977144Z",
  "event_id": 88,
  "first seen": "2025-07-24T02:40:34.968258Z",
  "incident_id": 71,
  "kill chain": "delivery",
  "state": "ongoing"
 },
 "method id": 1002026992,
 "family_type": "family",
 "event id": 88,
 "offender_type": "ip",
 "asset type": "ip",
 "family id": 7,
 "threat name": "Powershell",
 "asset": "192.168.100.60",
 "kill_chain": "delivery"
}
```

Note: This query returns only the first Stamus Event that triggered a DoC on an Asset

# Declaration of Policy Violation (DoPV)

Like a DoC, a Declaration of Policy Violation (DoPV) is a high-confidence and high-priority incident detection event in Clear NDR. DoPV events are related to the security and compliance policy of an organization and activities identified as "unauthorized".

### Continuous Compliance and Security Audits

The power of the DoPV is that it gives security, governance, and risk personnel a continuous and real-time understanding of significant policy violations taking place in their organizations.

Unlike Declarations of Compromise (DoC) which alert organizations to high-priority threats, DoPVs focus on unauthorized activities or policy violations that may not necessarily be malicious but still pose a risk to the organization.

Examples may include insecure protocols, outdated TLS versions, expired TLS certificates, vulnerable systems, software, TOR browser usage, or unencrypted (clear text) passwords. These fall largely into two families of detections:

- Adware This detection family identifies unwanted software designed to display advertisements to users, most often within a web browser. These are dangerous because they can become weaponized
- **Potential Data Leakage** This detection family identifies security vulnerabilities and risky behaviors that could lead to unauthorized data exposure or exfiltration. The detections focus on conditions that create pathways for sensitive information to leave the organization through insecure channels or compromised systems.

STAMVS A. ACM Q soin M SECURITY POSTURE Operational Center Potential data leakage @ Investigate events TE COMPROMISES ecialists toil away to create better, sma & heromes more prevalent and thus as is, there is one fisk they can't progra acted Assets Timeline Coverage TE POLICY VIOLATIONS Cleartext o Commonly Abused File Sharing ol - FTF Explore 0 115 0 84 0 4 0 C ANALYTICS Beaconing - LLMNR TLS Excit Sightings 2 0 43 0 1 HUNTING Methods Dashboards Events Detection Methods Hosts Network Tree Metadata Palicies ADMINISTRATIO Filter Assets 2 new / O fixed / Total: 2 Anniances Meters General Info DoPV / DeC Threats Seen dates Details Month Othe Туре Threat Last Seen Buler RYOD 10.7.5.101 19 15 hours ago 15 hours and Linglassified home Users (P) 1078.5 15 hours ago 15 hours ago Undersided home

You can see more detailed examples from the Potential Data Leakage family coverage here:

### How to Identify DoPVs in the Clear NDR User Interface

You may start an investigation into a policy violation from the Operations Center. Click on Declaration of Policy Violations (Policy Violations)



### Custom DoPVs

In addition to those built-in and included in the daily threat detection updates, users may create their own through a process known as "escalation," whereby the results of an investigation or hunt can be turned into a DoPV rule. These custom DoPVs are built using the filters and may be used for real-time policy violation detection on future network traffic or applied retroactively to historic data.

### Viewing the DoPVs in the Hunt and Investigation Console

To view all DoPVs from the Clear NDR Hunting dashboard, toggle the event type "Detection" and "Sightings" to the off position, add a filter to add the events in the "policy violation" phase of the kill chain. See instructions below.

STAMVS METRORIXE	C Reload 🔥 Photenia-comportation 🛇 list 24 hr	curs ⑦ Help 🛛 R mdurrett	
	NAMINO 1 CASIBOARDS		
Operational Center	Filters # Tags Filters	Actions	
COMPROMISES	V CED Detection OIL Inform	mational × Clear Filters	
Impacted Assets	De-select "Detection"	vant T Load Filter Set	
Timeline	and "Sightings"	gged Ø Policy Actions	
Coverage			
DE POLICY VIOLATIONS	Tags Probes		
Explore	100	$\frown$	
« ANALYTICS	75		
Inventory	50	94	
Beaconing		current count	
Sightings	25		
(e) HUNTING		previous count III current count	
Dashboards	ματ 2,005 ματ 2,005 ματ 2,005 ματ 2,005 ματ 3,005 ματ		
Events		CNO Hide empty tiles	
Detection Methods	Basic Information		
Policies	Detertion Mathods = Catenories = Severities = Prohes =		
Appliances	SN M5-SCMR service - RicetastServiceW 22 Unknown 66 Contextual 64 sn-probe-aws-1 64 SN M5-SCMR service - RicetastService W 23 Severe 15		
History	PowerShell Base64 Encoded Content Comma_ 0 A Network Trojan was detected 11 Suspicious 14		
Monitoring	SN Legacy protocol - LUMAIN M Market Commandia and Control Activity Jetec. 4 PowerShell Based Encoded Content Comma. 6 Potential Corporte Privacy Violation 2		
Other			
Rulesets	Stamus Threat Information		
RYOD	Assets         Ξ         Offenders         Ξ         Threats         Ξ         Families         Ξ         Kill Chain Phases         Ξ		
Sources External Sales	10.44.65.43 14 10.44.65.43 15 Lateral - Policy Bypass Exec 15 Custom Threats 10 Installation 10		
External links	10.446.511 6 83.9720.81 21 Powersher 13 Lateral Movement		
CO OTHER APPS	10.44.05.36 0 114.120.69.633 0 114.20.69.633 0 100.000 0 12 12 10 0 100.0000 0 12 100.0000 0 100.0000 0 100.00000 0 100.00000 0 100.00000 0 100.00000 0 100.00000 0 100.00000 0 100.00000 0 100.000000 0 100.0000000 0 100.00000000		
EveBox	10.44.65.10 5 185.174.174.220 2 Cobalt 5 5 7 7 7 19 7 19		
EVEDOX			
	Click to add a filter for Kill Chain		
	Phase = Policy Violation		
	C Reload	d 👌 Phoenix-corporation 🕓 I	ast 24 hours ⑦ Help ႙ mdurrett
	ME SECURITY POSTURE HUNTING > DASHEDARDS		
	Operational Center ellevent	Providence -	rite
		Event types Tags	Actions
	J, Commoniada	Citize Section ON	Pelevant T Load Filter Set
	Impactor Assets VI Chan Bayas Bala Malating 2 0 V	ON Stamus ON	Save Filter Set
		- Stanus	Ø Policy Actions ∨
	Coverage		

### How to Identify a DoPV Event Using a SIEM Query

Below is an example of how to query your SIEM for a DoPV. Note, the query uses "Event Type = Stamus" and the DoPV qualifier: "Stamus events" that are not associated with a kill chain phase.

#### Query:

#### "event\_type":"stamus" + "kill\_chain":"pre\_condition" + unique incident\_id

This will return the DoC JSON log entry that includes Stamus Event information. See example on next page

```
"stamus": {
 "extra info": null,
 "source": "212.193.30.21",
 "family name": "Adware",
 "incidents id": [118],
 "threat id": 1058,
 "asset_net_info": "wifi-users-hq.organization-acme",
 "pk": 1218,
 "asset info": {
  "last seen": "2025-07-24T03:36:27.077767Z",
  "event id": 183,
  "first seen": "2025-07-24T03:36:27.077767Z",
  "incident id": 118,
  "kill chain": "pre condition",
  "state": "new"
 },
 "method id": 1002010595,
 "family type": "family",
 "event id": 183,
 "offender type": "ip",
 "asset_type": "ip",
 "family_id": 23,
 "threat name": "Potentially Unwanted Program",
 "asset": "192.168.100.238",
 "kill_chain": "pre_condition"
}
```

Note: This query returns only the first Stamus Event that triggered a DoPV

### Asset-Oriented Incident Insights

When a DoC or DoPV event is logged, Clear NDR collects all relevant data - including PCAPs, protocol transaction logs, flow records, and details about the threat detection logic itself – and associates it with the threat and the asset.

And the Host Insights and Timeline feature consolidates all relevant DoC and DoPV detection methods associated with an incident affecting the asset under attack. These include a complete attack timeline outlining the progression of the incident beginning with "patient zero" and expanding to the entire blast radius. The screenshot below illustrates the attack timeline for a DoC Incident involving multiple assets (Hosts).



## Automating Response with DoCs and DoPVs

DoCs and DoPVs can be used to trigger a response using an integration with an outside system such as an EDR, firewall, incident response system, or SOAR. The primary mechanism for this integration is Webhooks, a lightweight API that powers the one-way data sharing triggered by DoC and DoPV events.

See screenshot below.

STAMVS - Clear NDR	Management 🕈 Home 🍖 Sources 🏭 Rulesets 👁 Appliances 🖨 Monitoring ≿ RYOD
System status Elasticsearch Disk Memory	Webhooks Emails Name
Platform status Probes	Name     Test Syntax     Test Send     Delete       Provider     ~     ~
Integration Edit provider	Hook Threat on Asset
Tasks Status of tasks Periodic tasks Report periodic tasks	DoC DoPV URL
No Task in progress	URL Headers Content-Type: application/json
Help Integration	
	HTTP method

In addition to Webhooks, a DoC or DoPV can generate an email. See screenshot below.

NETWORKS		
System status	Webhooks Emails	
Elasticsearch Disk Memory	Name	
	Name Test Syntax Test Set	nd Delete
Platform status	Hook	
Probes	Threat on Asset 🗸	
ntegration		
dit provider		
Tasks	From	
Status of tasks	From	
Periodic tasks	То	
Report periodic tasks	То	
	Comma separated list	
lo Task in progress	Subject	
	DoC - {{ asset.value }}	
Help	Body	
ntegration	New Declaration of Compromise:	
	* Asset under attack: {{ asset.value }}	
	<ul> <li>Inreat: {( inreathane ))</li> <li>Threat Semity of family name ))</li> </ul>	
	* Killchain phases ( Killchain pame )}	
	Contraction of the second	
	Investigate using Stamus Central Server: {{ family_url }}	

Examples of common webhook integration use cases for DoC include the following:

- Open an incident response (IR) ticket ticket via an IR system
- Isolate an offending endpoint via an EDR (endpoint detection and response) system
- Block an offending IP Address via a firewall rule
- Initiate a response playbook via a SOAR (security orchestration and response) system
- Send a message to your instant messaging platform of choice (Slack, Teams, WhatsApp, Google Chat...)

# Reviewing the Power of DoCs and DoPVs

Clear NDR's Declarations of Compromise and Policy Violations represent a paradigm shift from traditional security monitoring approaches, providing security teams with precise, high-confidence starting points for investigation rather than overwhelming them with low-fidelity alerts. By focusing on asset-oriented incidents with comprehensive evidence collection, these detection events bridge the gap between raw network data and actionable security intelligence.

The dual approach addresses both threat detection (DoC) and policy compliance (DoPV), creating a comprehensive security posture management solution. The system's integration capabilities spanning SIEM platforms, automated response systems, and custom DoC and DoPV escalation creation-ensure that organizations can adapt these high-fidelity detections to their specific operational workflows and security architectures.

Ultimately, DoCs and DoPVs transform security operations from reactive alert processing to proactive incident management, enabling security personnel to focus their expertise on genuine threats and policy violations while maintaining the detailed forensic capabilities necessary for thorough investigation and response. This approach significantly enhances both the efficiency and effectiveness of modern cybersecurity operations.

## Contact Stamus Networks Today

To request a custom live demonstration of Clear NDR, visit the Stamus Networks website at https://www.stamus-networks.com/demo To generate a custom pricing quote for your application, visit the Stamus Networks website at https://www.stamus-networks.com/pricing-guote-generator

#### ABOUT STAMUS NETWORKS

Stamus Networks is the global leader in Suricata-based network security and the creator of the innovative Clear NDR® system. Designed to close visibility gaps and reduce alert fatigue, Clear NDR transforms raw network traffic into actionable security insights with unmatched transparency, customization, and effectiveness. Trusted by leading financial institutions, government agencies, and participants in NATO's largest cybersecurity exercises, Stamus Networks delivers proven, high-performance network detection and response solutions. Stamus empowers security teams - delivering clarity amidst complexity – with greater control, fewer false positives, faster response times, and a more responsive, open approach than legacy vendors.



229 rue Saint-Honoré 75001Paris 450 E 96th St. Suite 500 Indianapolis, IN 46240 United States

- ∝ contact@stamus-networks.com
- S www.stamus-networks.com