How to use nProbe DPI and Sycope to improve security in every company

Piotr Kałuża
Solution Architect

What is Sycope

Sycope is a specialized IT solution designed for comprehensive network traffic analysis and threat detection. It leverages protocols like NetFlow, SFlow, IPFIX, and NSEL to collect and analyse data, providing real-time insights into network performance and security

under control
now and tomorrow

Key features

- Vendorless monitoring - compatible with all Flow standards and any fields extension
- Data deduplication - correct reporting of traffic volume
- High performance - up to 250k flows/sec
- Easy interface - predefine content and easy filtering
- Flexible in configuration – all elements can be customize or create by users

under control
now and tomorrow

Key benefits

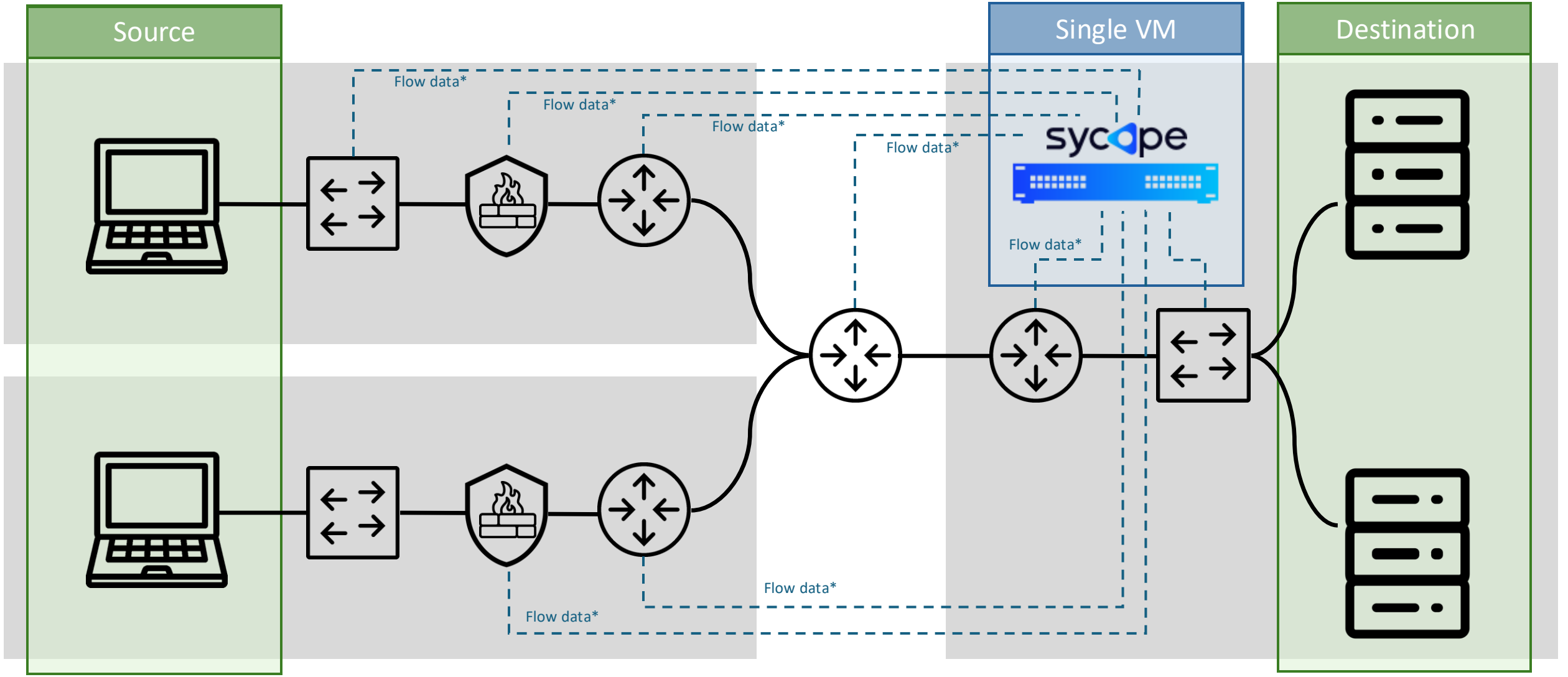
- Reducing TCO of network observability - all data in one place
- Quick and flexible implementation – available as virtual appliance, first results after one hour
- Long term data storage for network of any size
- Troubleshooting - drill-down from easy-to-read charts and graphs to raw data of a single connection

under control
now and tomorrow

How it works


API
ANALYTICS
SECURITY RULESET
ANOMALY DETECTION
-ANALYTICS
-SECURITY RULESET
-ANOMALY DETECTION
COLLECTION
NETFLOW V5/9
IPFIX
NSEL
sFLOW
nProbe
-RAW DATA
-AGREGATION
-DEDUPLICATION

Sycope architecture



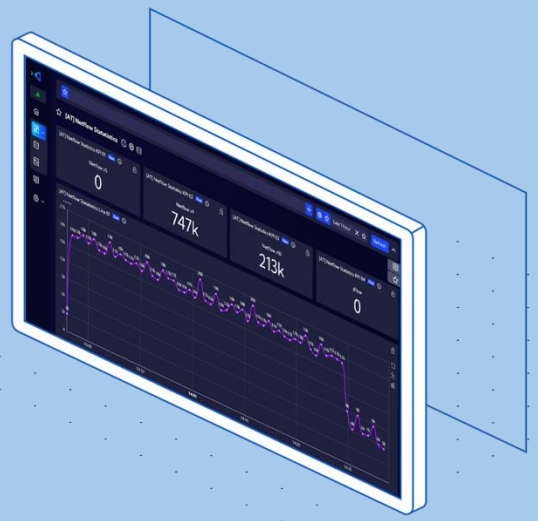
Sycope Modules

Visibility

Traffic Visibility

Statistics and RawData

Performance



Network Performance (NPM)

and L7 data

Security

Threat Hunting, analysis and

mitigation

Asset Discover

IT Asset Inventory

NetFlow in network monitoring

Network & Application Performance Monitoring

Visibility helps to optimize the performance of network resources and manage quality of services (QoS) - detection delays, network congestion, bottlenecks and outages.
Observability provides a more complete picture of the situation, making it easier to understand problems at the entire infrastructure level, not just a single system.

Troubleshooting

Quick problem solving (network overloads, data transmission errors, system failures) which reduces downtime.

Observability allows you to track how different network components work together and how they behave in response to specific events.

Planning the expansion of network infrastructure

Provides information to help make decisions regarding future expansion, upgrades or adjustments to network infrastructure.

Correctly planned network saves time and money.

Effective cost management

It helps ISPs measure actual network usage by individual entities for billing purposes.

Assists in resource analysis and cost management through effective resource management.

under control
now and tomorrow

NetFlow in security monitoring

Detecting Network Security Threats

Examples of threats: DDoS, Infiltration and Intrusion Attacks (scans), C2, Violations of Security Policies, Application Attacks
Malicious traffic detected based on reputation
Threat Hunting searches.

A valuable source of data for other systems

SIEM, AntiDDoS

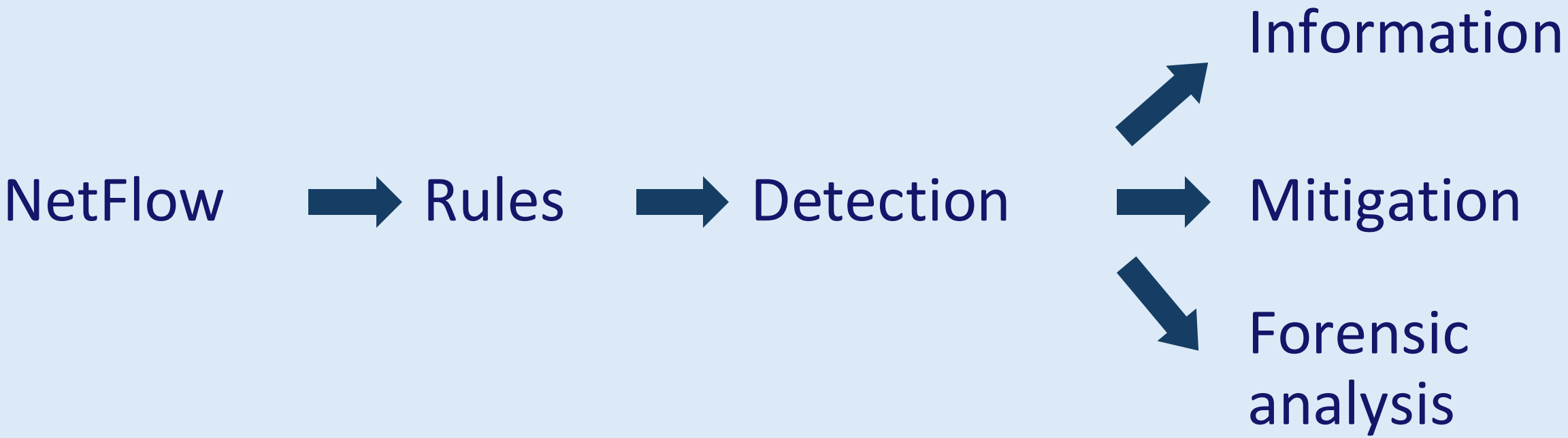
Assists in meeting regulatory requirements

Examples of regulations and standards: HIPAA, GDPR, PCI DSS, DORA, NIS2, ISO/IEC 27001

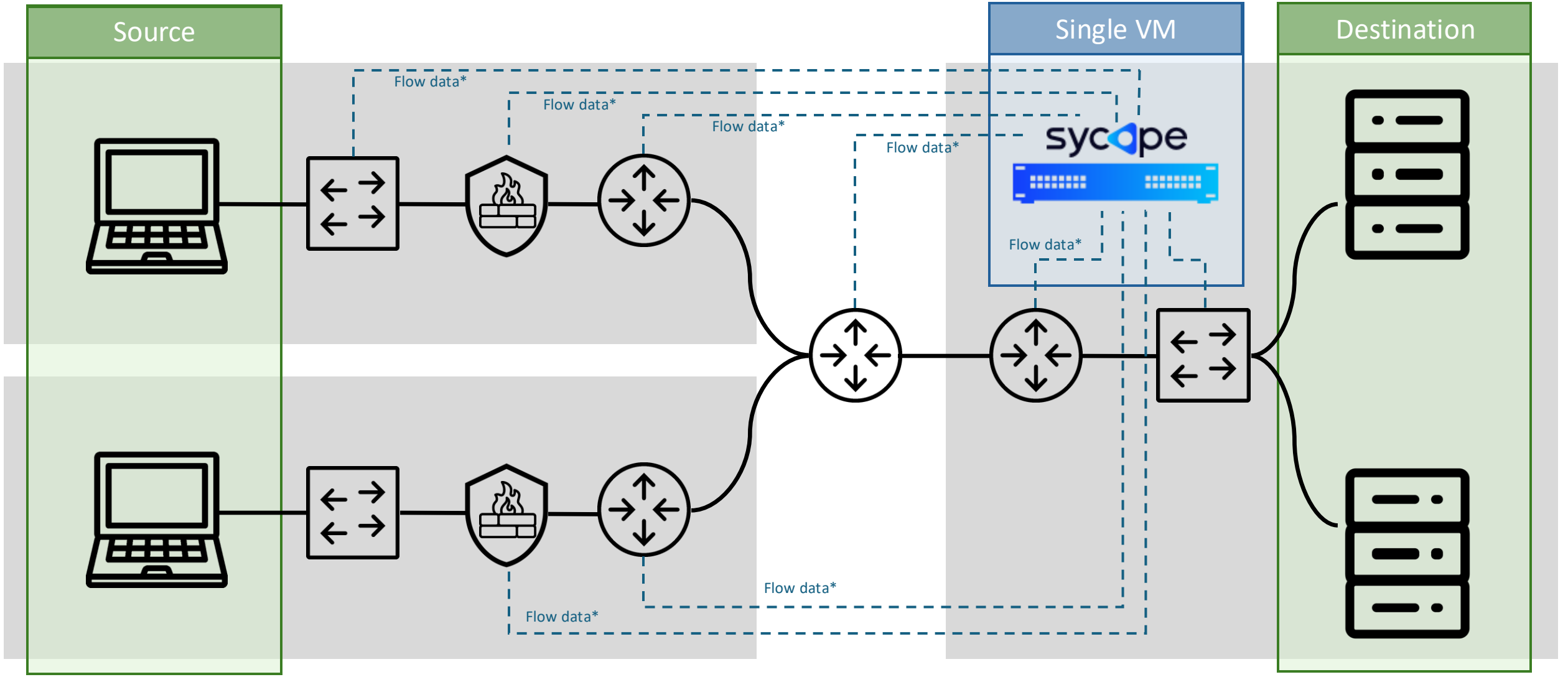
Forensic Analysis

Network Behaviour - identification of Sources and Targets involved in suspicious community
NetFlow data may be used as evidence in criminal investigations or cybercrime court proceedings.

Detection workflow

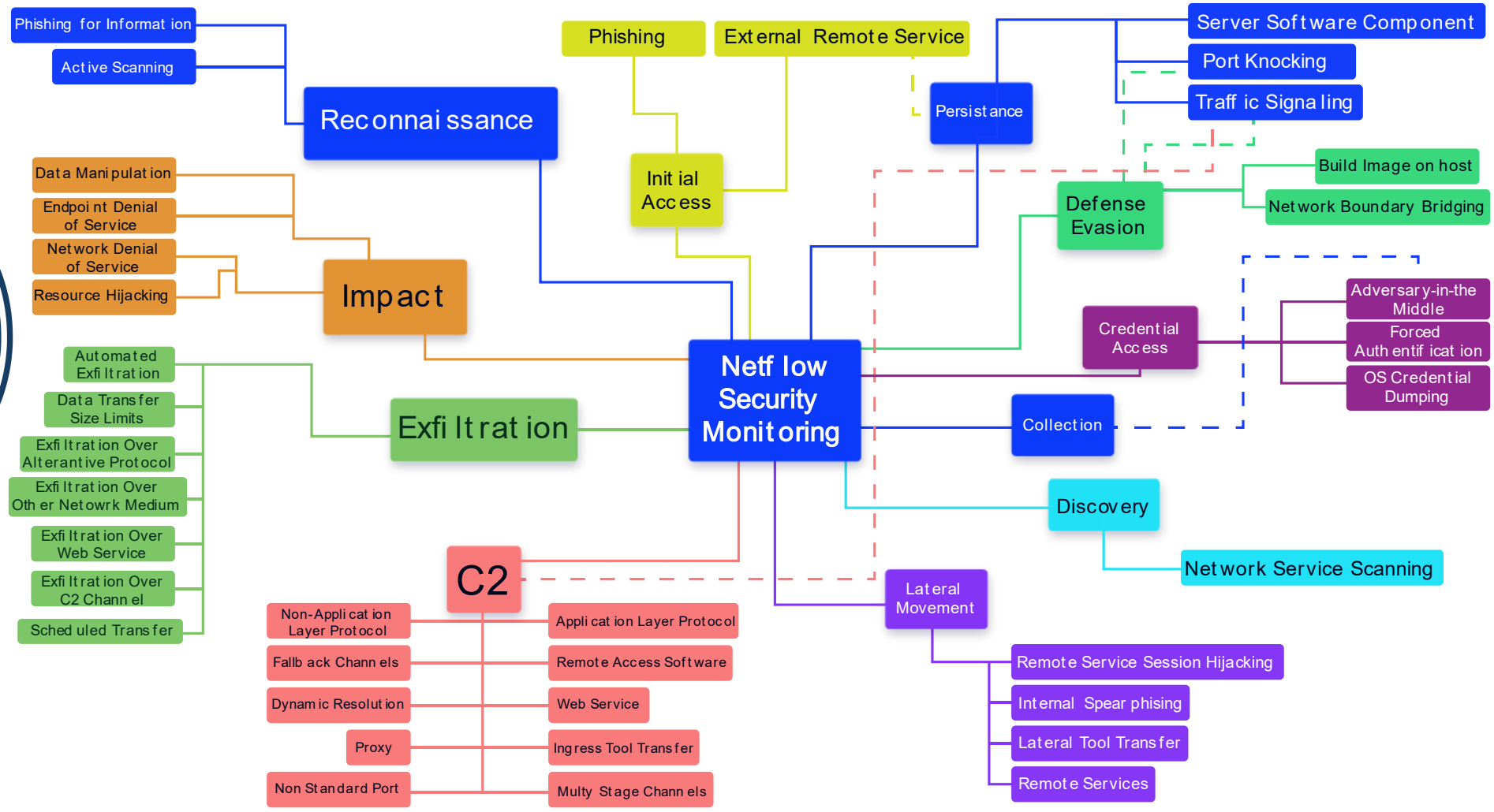


NetFlow


Source
Single VM
Destination
Flow data*
Flow data*
Flow data*
Flow data*
Flow data*
Flow data*
Flow data*

Rules

Security Threat Detection capabilities based on ATT&CK MITRE



under control
now and tomorrow

Detection rulesd base on NetFlow data

1. IP Reputation

Sycope CTI use over 100 sources

Updates every 8 hours

Best detection for well known Internet threads

2. Patterns

Predefined rules to detect volumetry incidents

Detects well known attacks like scans and password cracking

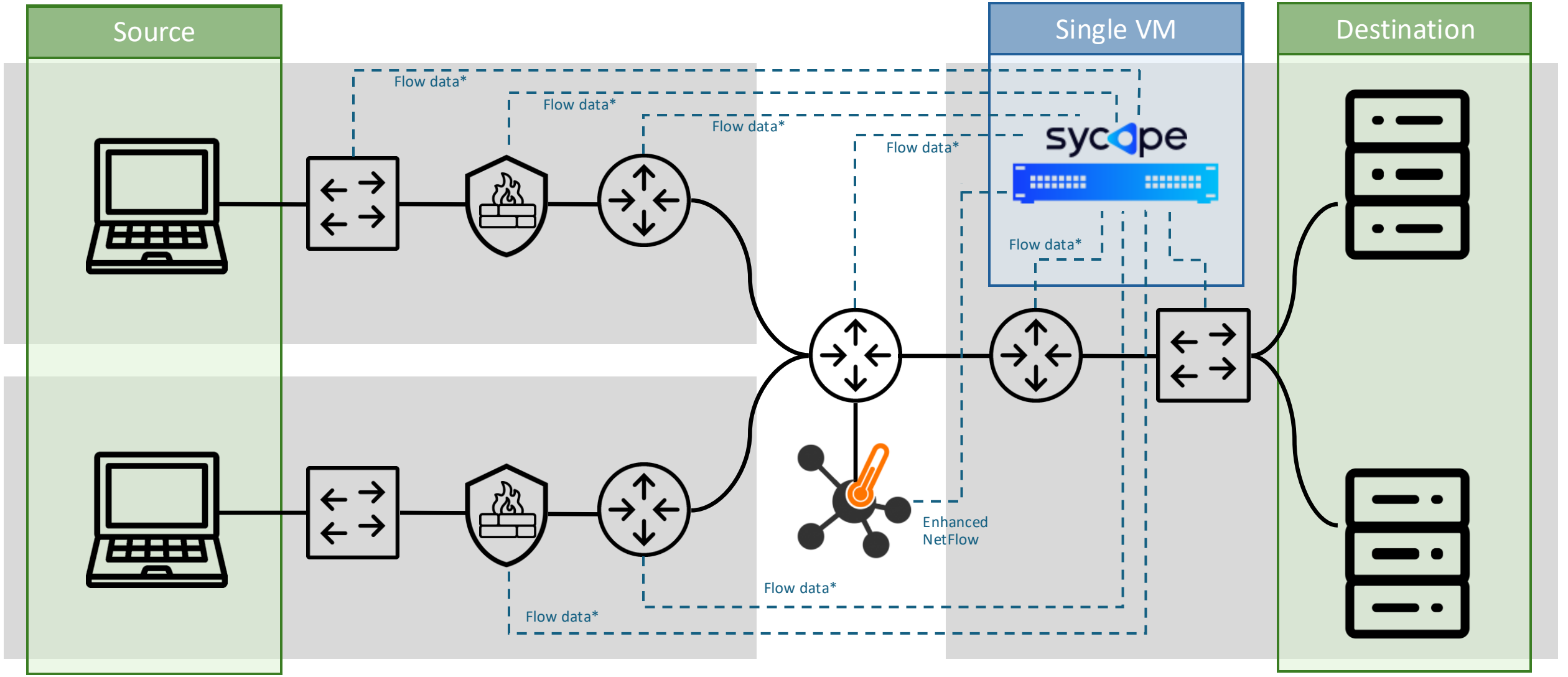
3. Behaviour analysis

Creates baselines

Compare with the past

Predicts future

Enhanced NetFlow



What enhanced data we use

DNS Plugin

[NFv9 57677][IPFIX 35632.205][Len 256 varlen] %DNS_QUERY DNS query
[NFv9 57678][IPFIX 35632.206][Len 2] %DNS_QUERY_ID DNS query transaction Id
[NFv9 57679][IPFIX 35632.207][Len 1] %DNS_QUERY_TYPE DNS query type (e.g. 1=A, 2=NS..)
[NFv9 57680][IPFIX 35632.208][Len 1] %DNS_RET_CODE DNS return code (e.g. 0=no error)
[NFv9 57681][IPFIX 35632.209][Len 1] %DNS_NUM_ANSWERS DNS # of returned answers
[NFv9 57824][IPFIX 35632.352][Len 4] %DNS_TTL_ANSWER TTL of the first A record (if any)
[NFv9 57870][IPFIX 35632.398][Len 256 varlen] %DNS_RESPONSE DNS response(s)

To find suspicious domain queries

What enhanced data we use

HTTP Plugin

[NFv9 57652][IPFIX 35632.180][Len 128 varlen] %HTTP_URL HTTP URL (IXIA URI)
[NFv9 57832][IPFIX 35632.360][Len 4 varlen] %HTTP_METHOD HTTP METHOD
[NFv9 57653][IPFIX 35632.181][Len 2] %HTTP_RET_CODE HTTP return code (e.g. 200, 304...)
[NFv9 57654][IPFIX 35632.182][Len 128 varlen] %HTTP_REFERER HTTP Referer
[NFv9 57655][IPFIX 35632.183][Len 256 varlen] %HTTP_UA HTTP User Agent
[NFv9 57656][IPFIX 35632.184][Len 256 varlen] %HTTP_MIME HTTP Mime Type
[NFv9 57659][IPFIX 35632.187][Len 64 varlen] %HTTP_HOST HTTP(S) Host Name (IXIA Host Name)
[NFv9 57833][IPFIX 35632.361][Len 64 varlen] %HTTP_SITE HTTP server without host name
[NFv9 57932][IPFIX 35632.460][Len 256 varlen] %HTTP_X_FORWARDED_FOR HTTP X-Forwarded-For
[NFv9 57933][IPFIX 35632.461][Len 256 varlen] %HTTP_VIA HTTP Via

To find suspicious hostname

What enhanced data we use

TLS info

[NFv9 57660][IPFIX 35632.188][Len 48 varlen] %TLS_SERVER_NAME TLS server name
[NFv9 57965][IPFIX 35632.493][Len 2] %TLS_CIPHER TLS Connection Cipher
[NFv9 57966][IPFIX 35632.494][Len 1] %TLS_UNSAFE_CIPHER TLS Safe(0)/unsafe(1) cipher
[NFv9 57967][IPFIX 35632.495][Len 2] %TLS_VERSION TLS Version

To find suspicious certificate CommonName

What enhanced data we use

JA3 Hash

```
[NFv9 57961][IPFIX 35632.489][Len 32 varlen] %JA3C_HASH JA3 client hash
[NFv9 58048][IPFIX 35632.576][Len 32 varlen] %JA4C_HASH JA4 client hash
[NFv9 57962][IPFIX 35632.490][Len 32 varlen] %JA3S_HASH JA3 server hash
```

Suspicious JA3 Fingerprint

What enhanced data we use

Deep Packet Inspection

[NFv9 57981][IPFIX 35632.509][Len 8] %L7_PROTO_RISK Layer 7 protocol risk (bitmap)
[NFv9 57982][IPFIX 35632.510][Len 64 varlen] %L7_PROTO_RISK_NAME Layer 7 protocol risk (string)
[NFv9 57999][IPFIX 35632.527][Len 2] %L7_RISK_SCORE Layer 7 flow Risk Score

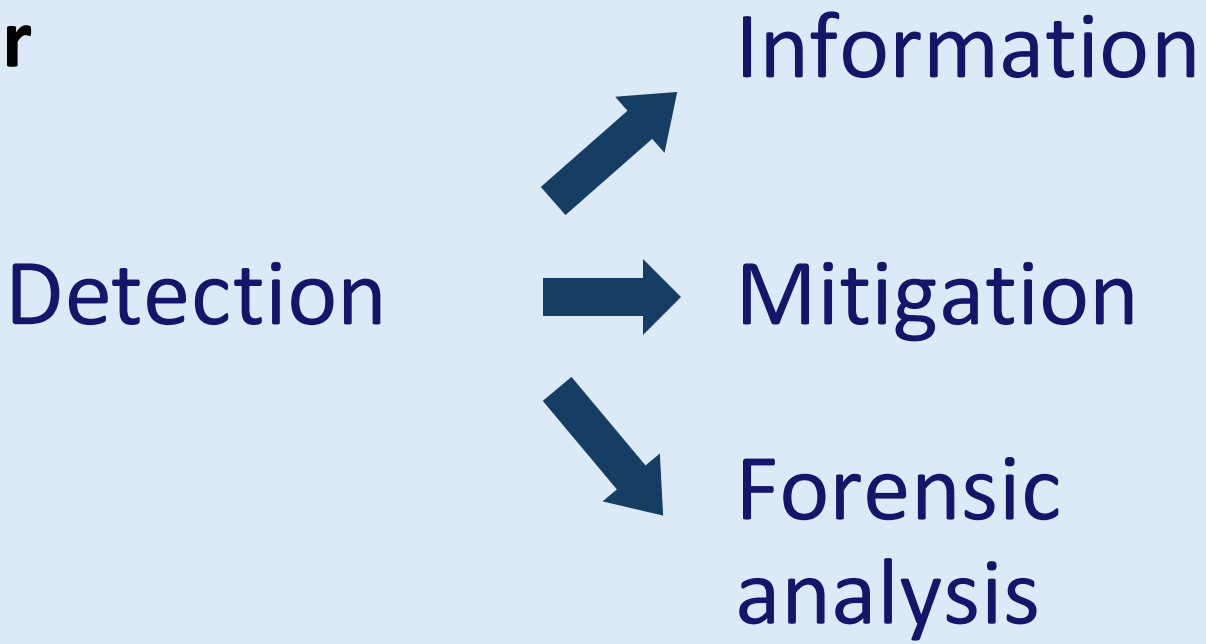
To find the threads like SQL-injection, certificate and encryption issues and many others

NetFlow in security monitoring

1. IP and **domain** Reputation
   - Sycope CTI use over 100 sources
   - Updates every 8 hours
   - Best detection for well known Internet threads
2. Patterns
   - Predefined rules to detect volumetry incidents
   - Detects well known attacks like scans and password cracking
3. Behaviour analysis
   - Creates baselines
   - Compare with the past
   - Predicts future
4. Deep Packet Inspection
   - Application layer threads
   - Encryption mechanism analysis

Detection

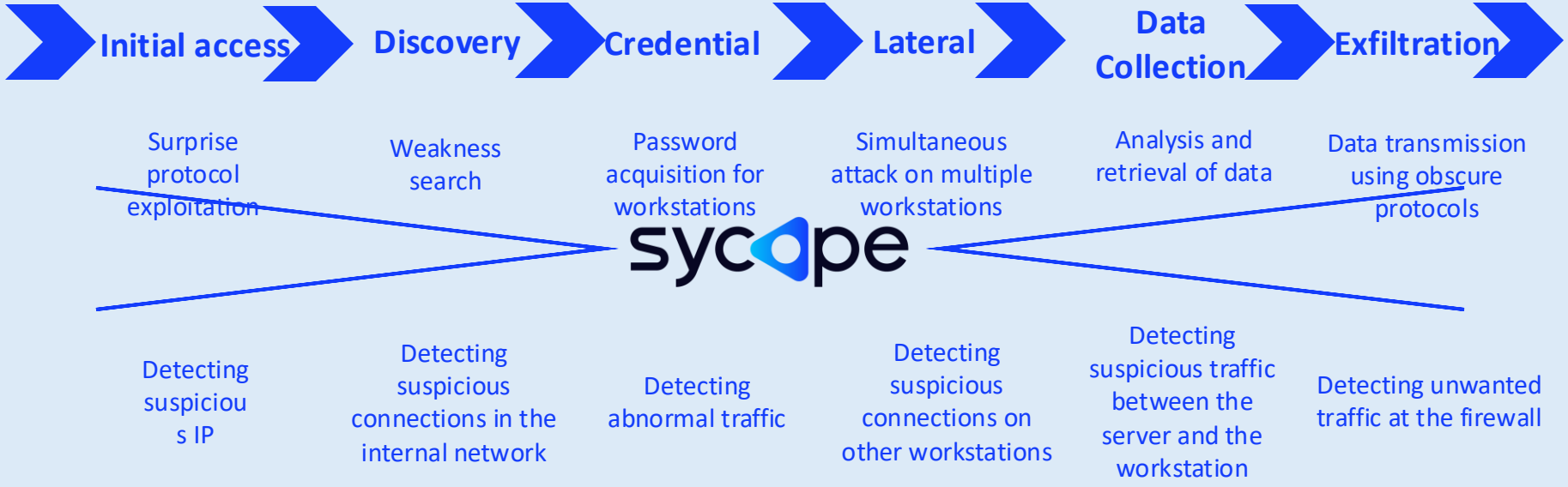
What Sycope gives you to improve the analysis and why it is better than raw information



Information

System information

- **Clear info about the threat**
- **MITRE ATT&CK® Framework clasification**



under control
now and tomorrow

Information

Email notification

under control
now and tomorrow

Information

SIEM integration

- **Syslog notification**

- **Instead of sending NetFlow data to SIEM analyse NetFlow in Sycope Security module and send info only about the incidents**

- **Reduce cost of SIEM license**
  - **For IP reputation rules corelation is 1:1**
  - **For Patterns reduce hundreds ot thousends of flows to one message**
  - **For Behaviour analysis reduce milons of flows to one message**
  - **And do not inform about all legitimate traffic**

Mitigation

- **Integration with macmon NAC**

- **Scripting engine**


```
{
    "http_method": "GET",
    "results": {
        "conf_scripts": {
            "remote": [],
            "history": [
                {
                    "id": 0,
                    "timestamp": 1676620011,
                    "name": "script",
                    "type": "Local",
                    "status": "Success"
                }
            ]
        },
        "backup_service_available": false
    },
    "vdom": "root",
    "path": "system",
    "name": "config-script",
    "action": "",
    "status": "success",
    "serial": "FWF40FTK20000000",
    "version": "v7.2.3",
    "build": 1262
}
```

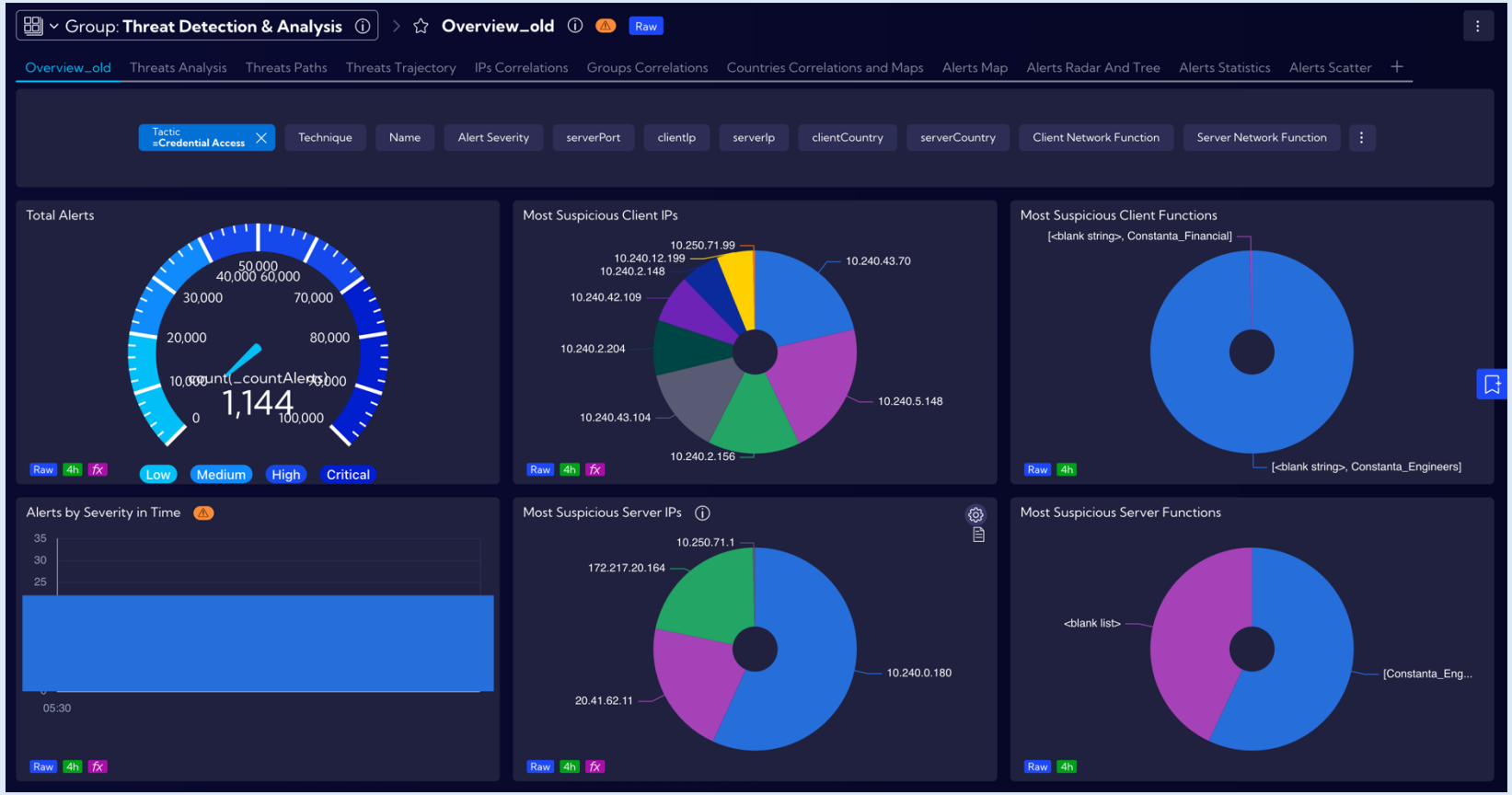
Forensic analysis

From general information…

under control
now and tomorrow

Forensic analysis

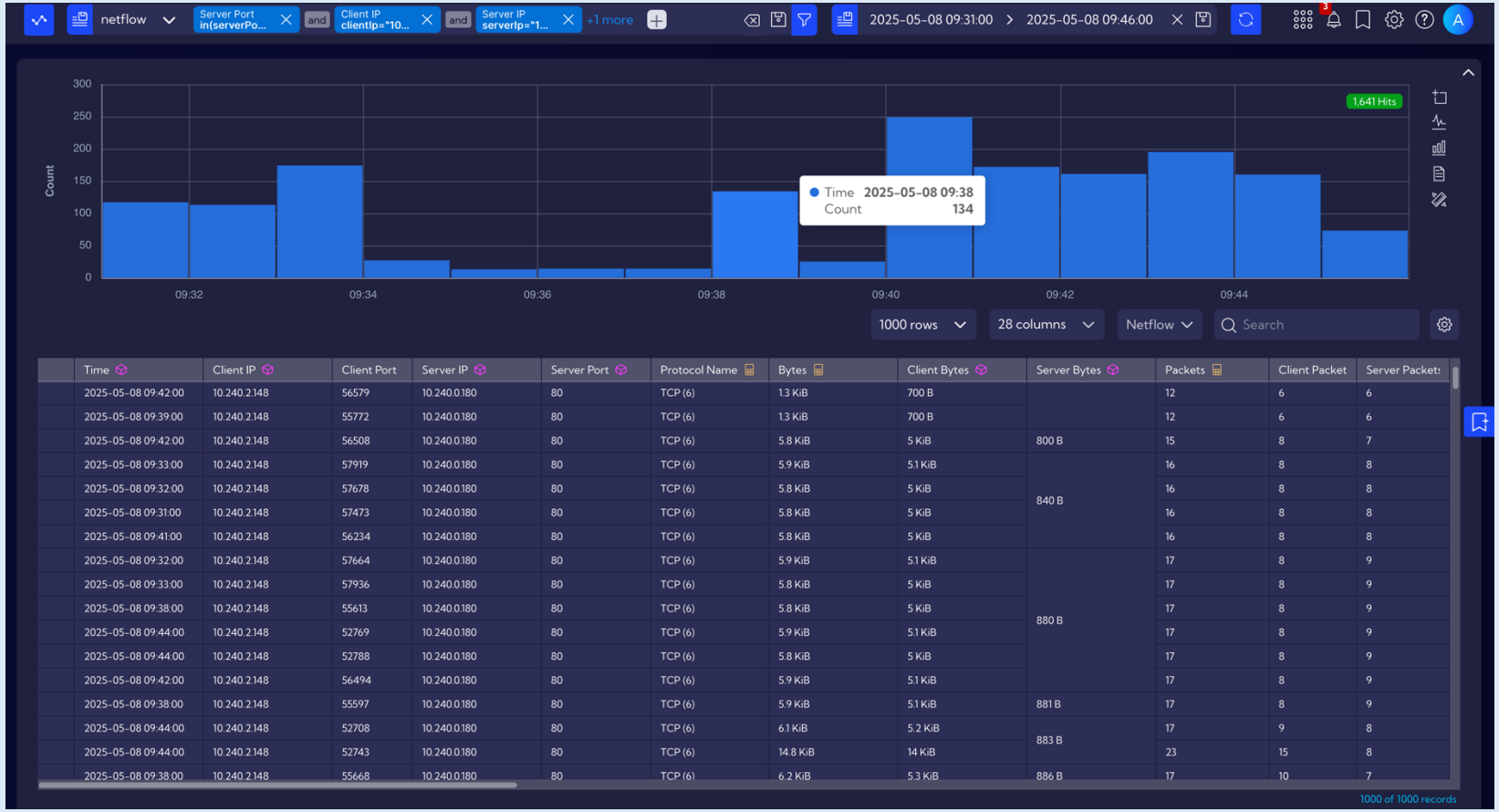
…through detailed information…



under control
now and tomorrow

Forensic analysis

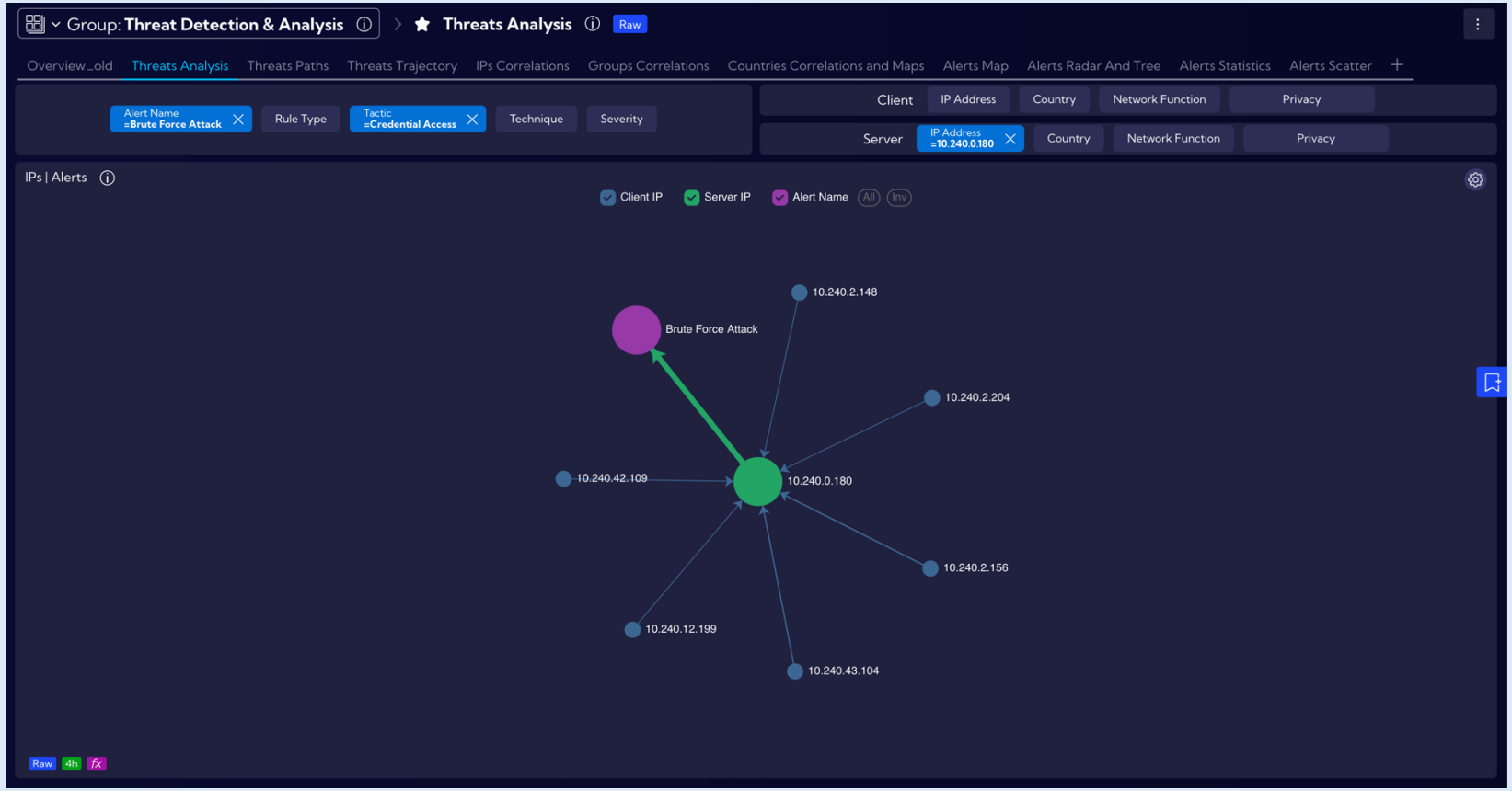
…for traffic connected with incident analysis….



under control
now and tomorrow

Forensic analysis

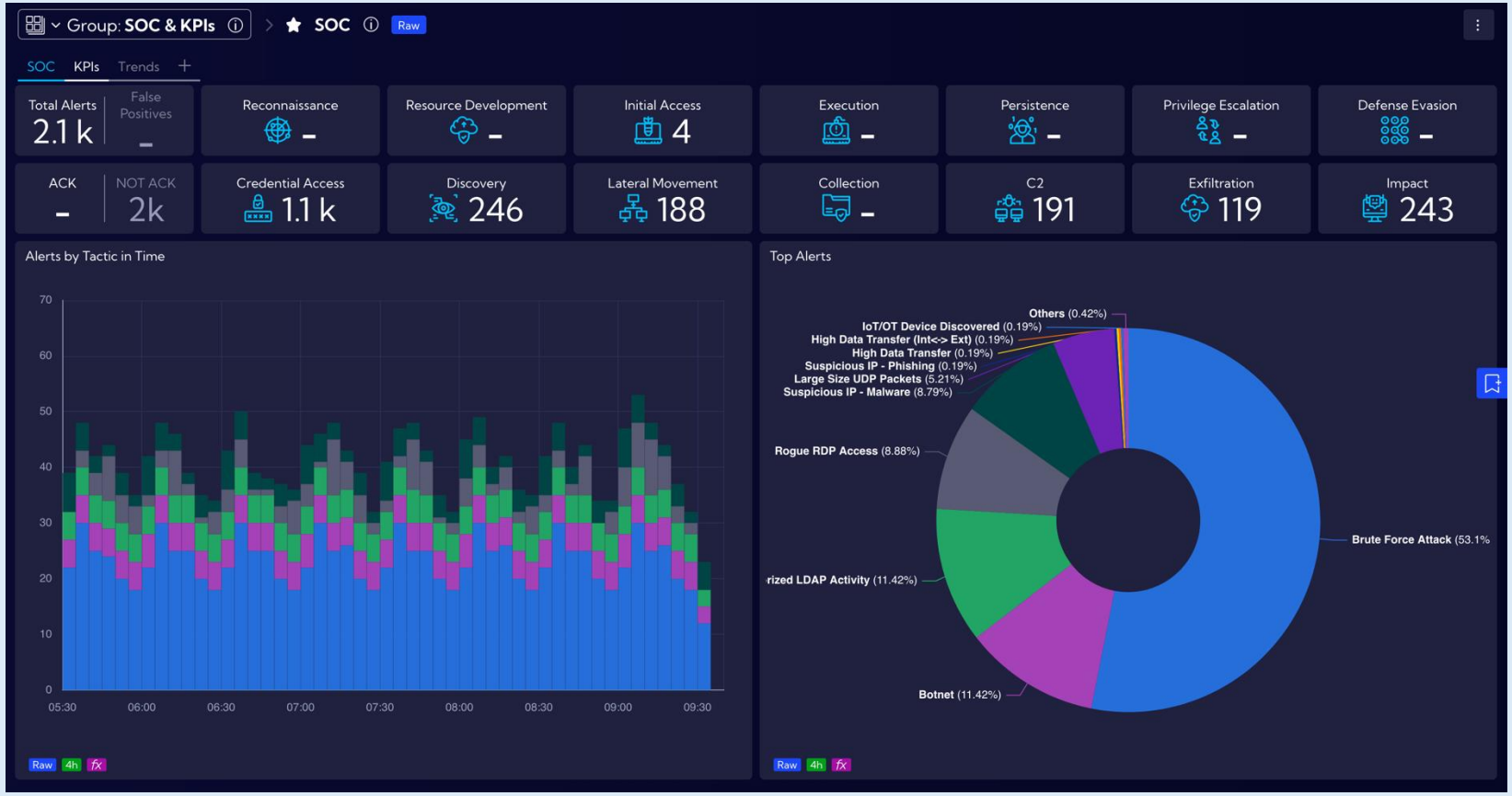
…and back to incident corelation…



under control
now and tomorrow

Forensic analysis

…to see full path of atack!



under control
now and tomorrow

Demo

Summary

Sycope is a network traffic monitoring and security tool that leverages real-time flow analysis with business context to enhance performance and secure IT infrastructure

under control
now and tomorrow

Piotr Kałuża

Solution Architect

Piotr.kaluza@sycope.com

+48 502 710 923

www.sycope.com