

# NSHaRP Security Architecture Upgrade

**Wayne Routly**

Head of Information & Infrastructure Security

TF-CSIRT, Poznan.pl

22 May 2015

- NSHARP
- SERVICE UPGRADE
- CHALLENGES
  - Backbone network
  - Netflow v9 migration
  - Flow forwarding and collection
  - NfSen
  - Ticketing system
- SOLUTION & PROCESS
- PILOT PHASE
- WHERE ARE WE
- GEANT CERT
- FUTURE



- GEANT maintains process as part of GEANT IP
- Complete security solution
- Provides mechanism to quickly and effectively inform parties
- Adds Value - Serves as an extension to NRENs CERTs
- An Automated Incident Notification & Handling System
- Extends NRENs detection and mitigation capability to GEANT borders
- Innovative and Unique - Caters for different types of requirements
- Supported with GEANT OC TTS



- Things that have changed / been added
  - Ticketing system
    - OTRS
  - Firewall on Demand
    - Pilot
  - Vulnerability Assessments
    - Weekly Reviews
    - Differential Scans?
  - **Backbone Anomaly Detection Tool**
    - **Netflow Management**



- In-house development not feasible
- Most commercial solutions don't cater for backbone networks
- Netflow v9, IPFIX... & IPv6 support is a MUST
- Centralization of flows → Collector + forwarder + analysis
- NfSen uses different ports to collect data... NOT REALLY!

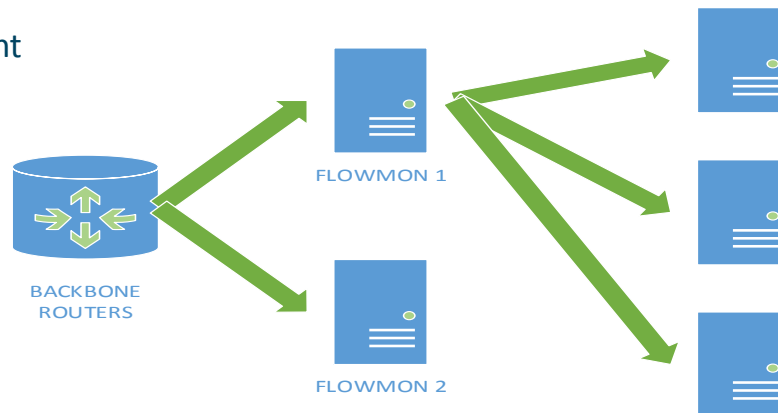
%sources = (

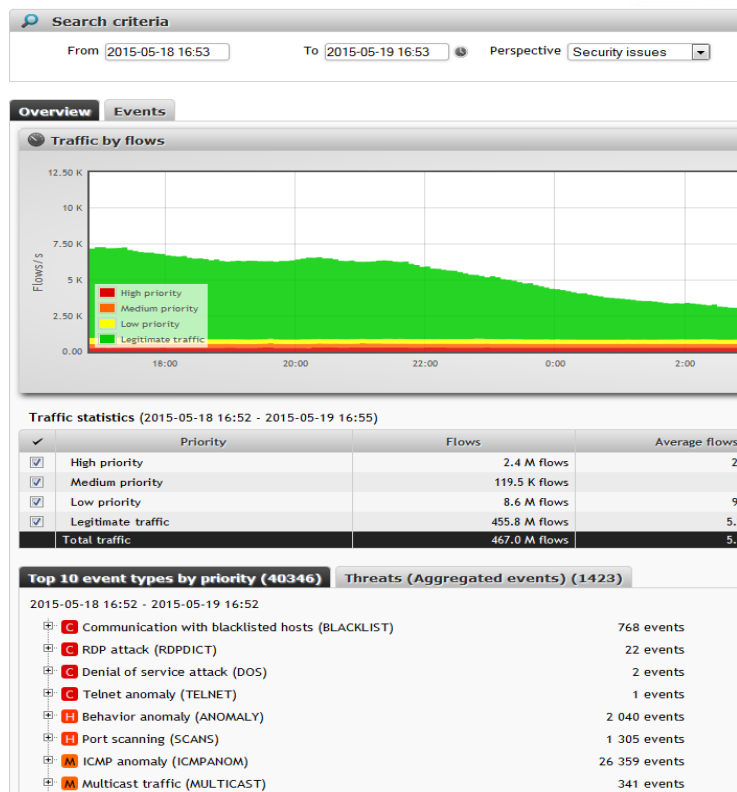
'device' => { 'port' => 'num', 'IP' => 'x.x.x.x', 'col' => 'value' },

- Adapt the chosen solution to work for our + NRENs' business needs
- New ticketing system migration running in parallel



- Business case, tool selection & testing procedure
- Partnership always sought
- Final decision → **Flowmon** from INVEA-TECH
  - Collector, forwarder and NAD (ADS plugin) in one solution
  - Predefined security event categories, configurable parameters and criticality
  - Good detection, low false positives ratios
  - Partnership pricing and former academia environment
- OTRS TTS
  - Different queues for automated / manual tickets
- Architecture:










Name	Code	Description
Behavior anomaly	ANOMALY	Anomaly Detection System
Communication with blacklisted hosts	BLACKLIST	Detection of communication with blacklisted IP addresses
DNS traffic anomaly	DNSANOMALY	Detection of anomalies traffic
DNS query volume anomaly	DNSQUERY	Detection of too many DNS queries
Denial of service attack	DOS	Detection of Denial of Service Attacks
High volume of transferred data	HIGHTRANSF	Detection of high data transfers in network
Honeypot traffic	HONEYPOT	Detection of trying to access network traps
Web form attack	HTTDPDICT	Detection of dictionary attacks on web authentication
ICMP anomaly	ICMPANOM	Detection of anomalies in ICMP traffic
L3 network anomaly	L3ANOMALY	Detection of anomalies on the third layer of OSI model
Multicast traffic	MULTICAST	Detection of IPv4 and IPv6 multicast traffic
SMTP anomaly	OUTSPAM	Detection of outgoing e-mail SPAM using SMTP or secured SMTP protocol
RDP attack	RDPDICT	Advanced detection method revealing dictionary attacks on Remote Desktop Protocol
Amplificated/reflected denial of service attack	REFLECTDOS	Detection of amplificated DOS
Port scanning	SCANS	Detection of TCP scans (SYN scan, FIN scan, Xmas scan, Null scan)
SIP floods	SIPFLOOD	Detection of SIP floods
SIP proxy	SIPPROXY	Detection of SIP proxies
SIP scans	SIPSCAN	Detection of scanning SIP devices
Service not available	SRVNA	Detection of service interruption
SSH attack	SSHDICT	Advanced detection method revealing dictionary attacks on secured shell service
Data inconsistency	SYSCHECK	Input data consistency controlling procedure
Telnet anomaly	TELNET	Detection of devices trying to establish telnet connections to various targets

- 2-3 months, March - May, going live June
- Participants:
  - REDIRIS
  - GRNET
  - LITNET
  - CESNET
  - FCCN
- Time for testing, improvements, new ideas...
- About 50 tickets/day in total + Daily report
- Monitoring and KPIs
- End of pilot → Extension to NRENs interested in the service... FOR FREE!





# WHERE ARE WE?

CRITICAL 	HIGH 	MEDIUM 	LOW 	INFORMATION 
	RDPDICT	HTTDPDICT		
		BLACKLIST		
		SCANS		
		SSHDICT		
		TELNET		

<ID>: num;  
<Category>: ANOMALY;  
<Type>: Behavior anomaly;  
<Perspective>: NREN;  
<Severity>: Critical;  
<Time>: 2015-05-13 09:55:00;  
<Protocol>: ;  
<Source IP>: x.y.z.t;  
<Target IPs>: a.b.c.d;  
<Ports involved>: ;  
<Flows sample>:  
Source IP;Source port;Destination IP;Destination  
port;Protocol;Timestamp;Duration;Transferred;Packets;Flags;  
Source AS;Destination AS  
x.y.z.t;42096;a.b.c.d;24384;TCP;2015-05-13  
10:54:31.770;3.43900012969971;208000;4000;.A....;786;2108

Dear NREN,

We have detected a CAT. event affecting your network. All the information pertaining to it can be found below:

=====

#Start Time: 2015-05-14 01:56:04 UTC

#Protocol: UDP

#Source IP: x.y.z.t

#Target IPs: a.b.c.d

#Ports: 60312

#Evidence:

Source IP;Source port;Destination IP;Destination  
port;Protocol;Timestamp;Duration;Transferred;Packets;Flags;Source AS;Destination AS  
x.y.z.t;a.b.c.d;60312;UDP;2015-05-14 02:56:04.566;0;84500;500;.....;36351;766

=====

If you wish to reply to this email please leave the subject unaltered so the ticket can be updated accordingly.  
If no response is received, this ticket will be automatically closed after 5 working days.

Regards,

GEANT CERT

[cert@oc.geant.net](mailto:cert@oc.geant.net) (PGP Key ID: 99833085 / Fingerprint: 3CBF F211 8305 635D 5839 BB27 BA6B F34A 9983 3085)

Phone no.: +44 (0)1223 866 140

-  ~~GEANT CERT~~
- <http://www.geant.org/GEANTCERT/Pages/default.aspx>

## 1.3 TEAM

### **Wayne Routly (Head of Information & Infrastructure Security)**

Email: [Wayne.Routly@geant.org](mailto:Wayne.Routly@geant.org)

PGP Key ID: 0x27269182

### **Juan Quintanilla**

Email: [Juan.Quintanilla@geant.org](mailto:Juan.Quintanilla@geant.org)

PGP Key ID: 0x6CF95248

### **Evangelos Spatharas**

Email: [Evangelos.Spatharas@geant.org](mailto:Evangelos.Spatharas@geant.org)

PGP Key ID: 0x49778EC8

## 1.4 CONTACT INFORMATION

The preferred method of contact is by e-mail.

Please send incident reports to [cert@oc.geant.net](mailto:cert@oc.geant.net). Please, use encryption for all mails that contain highly confidential information:

Key ID: 0x99833085 Key type: RSA

Key size: 4096 Expires: never

GEANT CERT PGP = 3CBF F211 8305 635D 5839 BB27 BA6B F34A 9983 3085

### **Phone number:**

+44 1223 733033

### **Physical Address:**

GÉANTCERT

City House

126-130 Hills Road

Cambridge

CB2 1PQ, UK

## 1.5 RFC 2350 COMPLIANT TEAM DESCRIPTION

 [GÉANT CERT RFC2350 Description](#)

- Flowmon
  - New blacklists
  - DoS detection plugin
  - Threat intelligence - New malware detection through own and external info
  - High availability
  - NRENs manage their profiles
  - MSR through API
- TTS - Signing and encryption
- Log Management
- FoD Integration
- ....





Thank you

[wayne.routly@geant.org](mailto:wayne.routly@geant.org)



Networks · Services · People  
[www.geant.org](http://www.geant.org)



© GEANT Limited on behalf of the GN4 Phase 1 project (GN4-1).

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).

- The aims of the SIG-ISM are:
  - Establish a community of NREN security management professionals
  - Develop, maintain and promote trust framework between NRENs based on international standards
  - Promote the use of international security standards and share best practices for security management within NRENs
  - Discuss and promote issues of information security management of particular interest to NRENs

<https://www.terena.org/activities/ism/ws2/agenda.html>





<https://www.terena.org/activities/ism/ws2/agenda.html>

