LogRhythm™

The Security Intelligence Company

Jean-Pierre CARLIN
Directeur, Southern EMEA
Jeanpierre.carlin@logrhythm.com
01 40 88 11 80 – 06 13 50 79 12

LogRhythm en 2014

- Le plus grand éditeur indépendant de SIEM
- Siège dans le Colorado
- Croissance annuelle > 50%
- 350 employés
- Solution “best of breed”
- Innovations continues

Gartner

Named a Leader in Gartner Magic Quadrant for SIEM 2014

SC MAGAZINE ★★★★★

SC MAGAZINE BEST BUY

SC MAGAZINE INNOVATOR

SC MAGAZINE RECOMMENDED

VENDOR LANDSCAPE AWARD
CHAMPION
INFO~TECH research group

BEST PRODUCT
FORENSICS SOLUTION 2014
★CDM★
www.cyberdefensemagazine.com

GLOBAL SIEM/LM MARKET PENETRATION LEADERSHIP AWARD
2014
by
FROST & SULLIVAN

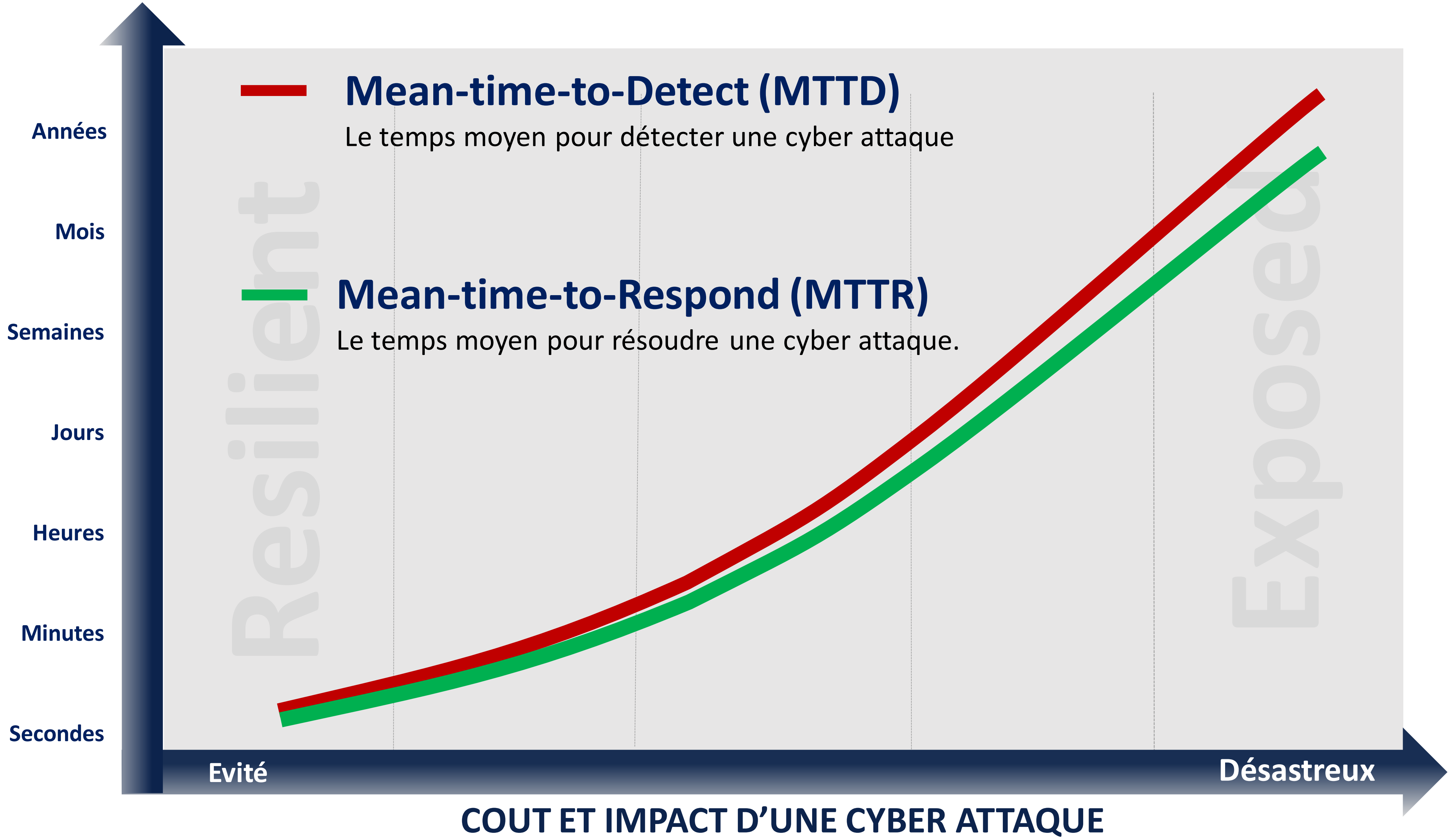
Le coût des cyber attaques en 2014

- Coût moyen par employé: **entre 437 et 1600 dollars**
- Temps moyen pour les stopper: **31 jours**
- Fréquence annuelle: **1,67 attaques**

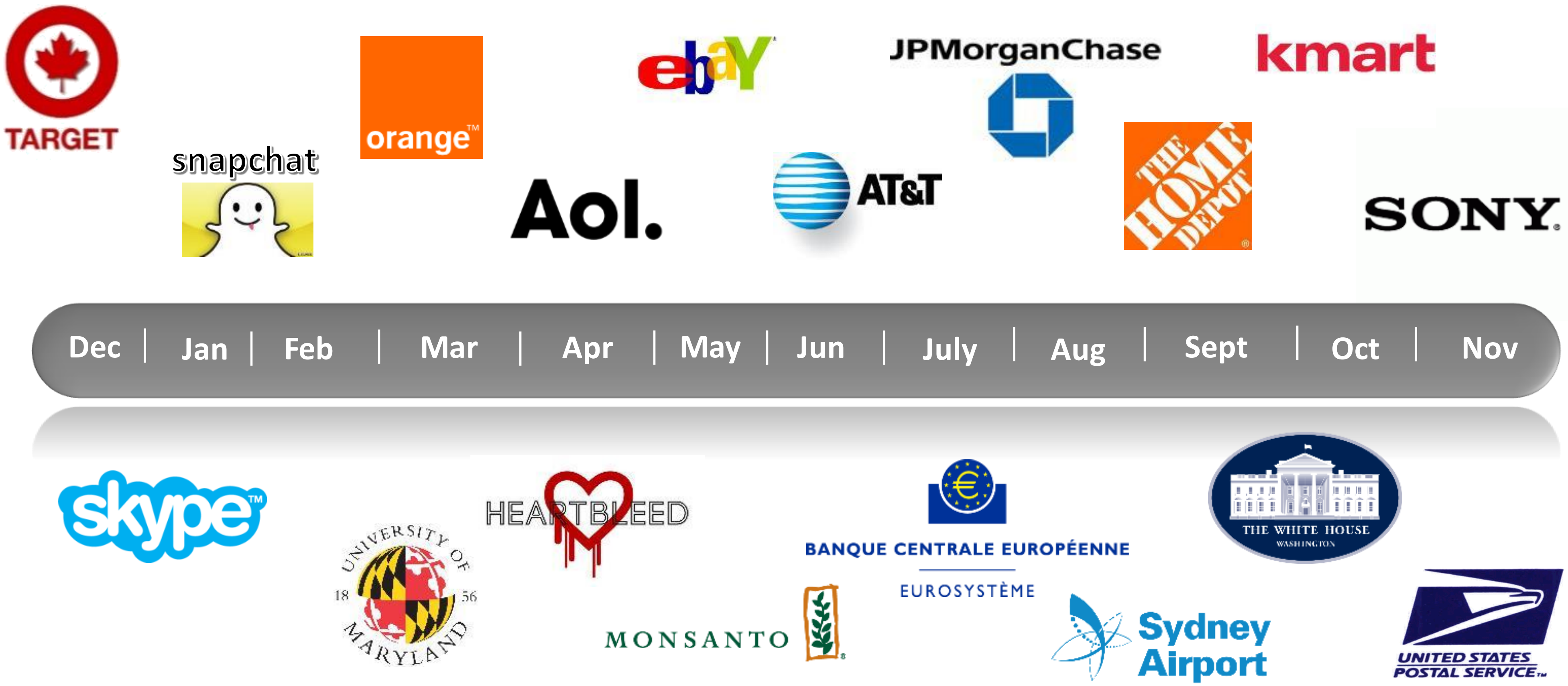
Ponemon INSTITUTE

2014 Global Report on the Cost of Cyber Crime

Le coût en fonction du temps



Cyber attaques notables ces 12 derniers mois



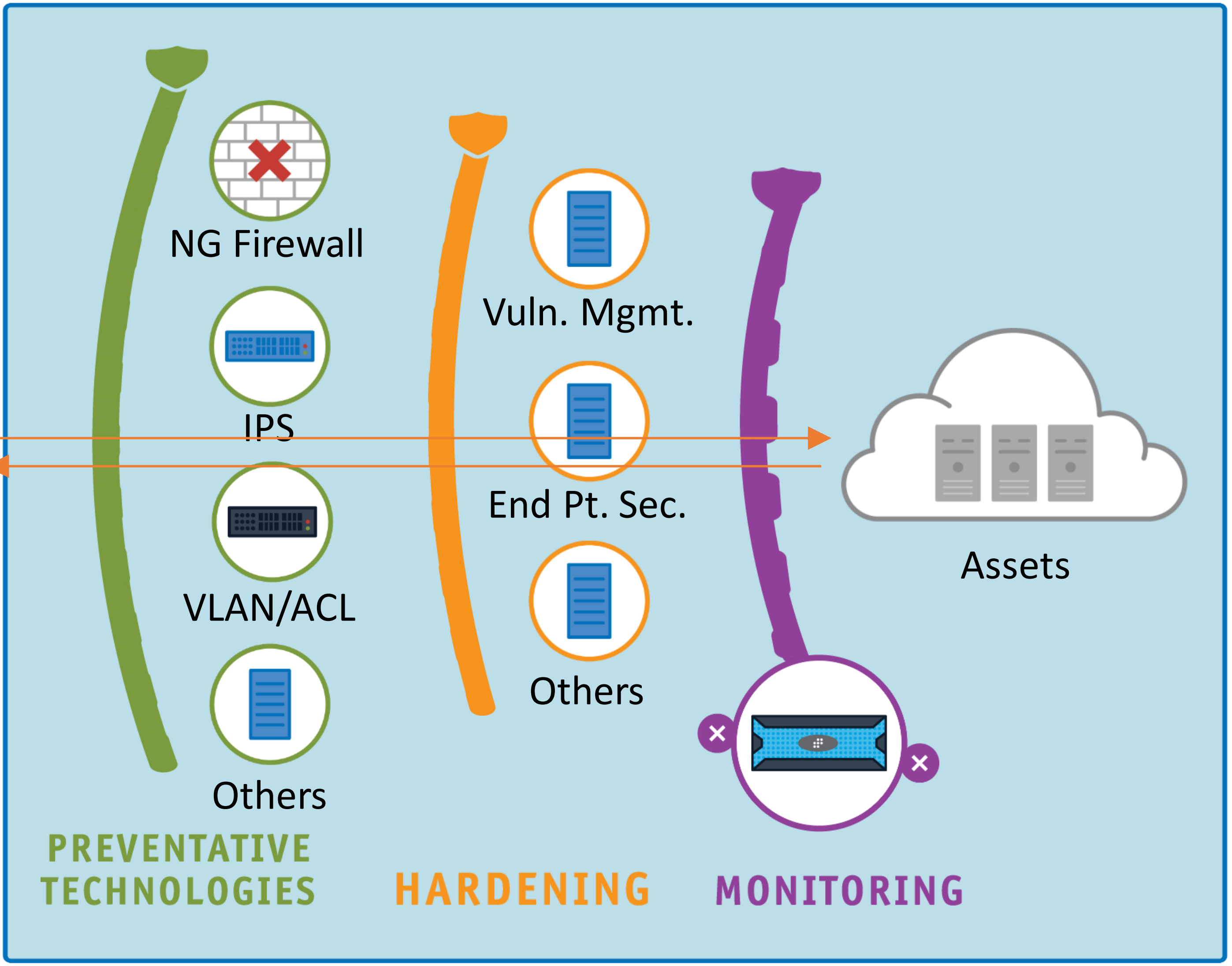
Dec | Jan | Feb | Mar | Apr | May | Jun | July | Aug | Sept | Oct | Nov

LogRhythm
The Security Intelligence Company

Lacunes des protections traditionnelles

- **Identifiants faibles ou volés**
  76% des attaques
- **Botnets/APT**
  59% des attaques
- **Ingénierie sociale/Phishing**
  52% des attaques
- **Menaces internes**
  35% des attaques

84% des investigations trouvent les preuves dans les logs



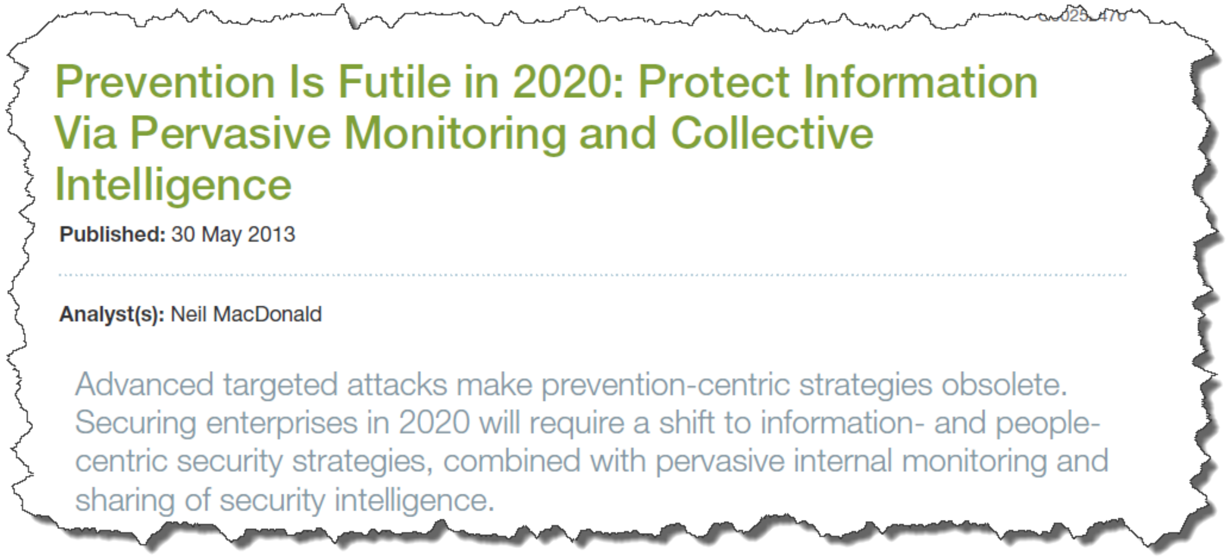
Sources: Ponemon et Verizon

Exemple de cyber attaque

1. Email de Phishing
2. Cheval de Troie de vol d’information Citadel (Botnet)
3. Vol d’identifiants
4. Logiciel malveillant « RAM scraper »
5. Alertes de sécurité ignorées
6. Exfiltration des données de 40 millions cartes de paiement et des informations sur 70 millions de leurs clients.

TARGET®

Prévisions pour le SIEM



G00251476

Prevention Is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence

Published: 30 May 2013

Analyst(s): Neil MacDonald

Advanced targeted attacks make prevention-centric strategies obsolete. Securing enterprises in 2020 will require a shift to information- and people-centric security strategies, combined with pervasive internal monitoring and sharing of security intelligence.

“La sécurité de l’informatique ne peut plus empêcher les attaques ciblées”

“Trop de dépenses ont ciblé la prévention des attaques et pas assez sont allées à la surveillance et aux moyens de réponse”

“En 2020, 60% des budgets sécurité de l’informatique seront alloués à la detection et aux réponses rapides contre 10% en 2013.”

Niveaux de maturité d’ analytiques de sécurité

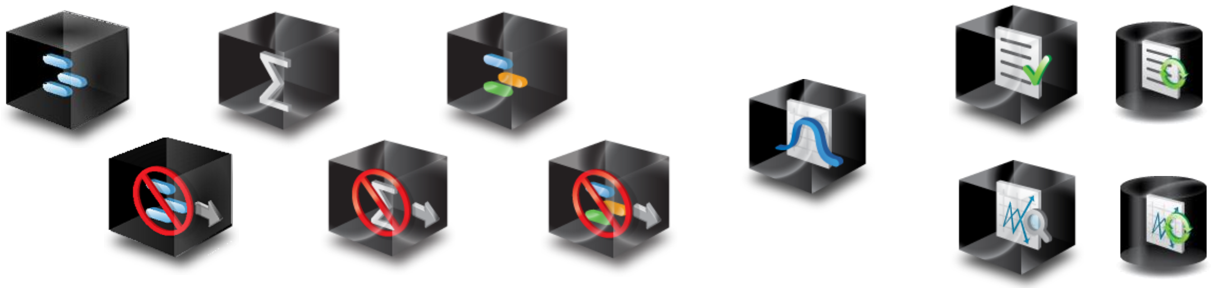
	Gestion de log	SIEM	LogRhythm
Collection et archivage des logs réseaux, systèmes, et applicatifs	●	●	●
Investigation et rapport par script	●	Inutile	Inutile
Normalisation et interprétation des logs	◐	●	●
Investigation et rapport par requête structurée		●	●
Priorisation des évènements par risque et envoi d’alerte		●	●
Corrélation en temps réel		◐	●
Détection d’anomalie et de changement de comportement		◐	●
Suivi des incidents		◐	●
Réponse aux incidents automatisée		◐	●
Surveillance de l’intégrité des fichiers et des registres		◐	●
Surveillance des flux réseau niveau 2 à 7		◐	●

LogRhythm™
The Security Intelligence Company

Avantages techniques LogRhythm

- **Solution pré-packagée rapide à déployer**
  Parseurs de logs + Conformité + Détection des menaces + Rapports

- **Interface facile d’utilisation**



- **Détection des menaces plus avancée**
  (Comportementale multidimensionnelle , Listes blanches, FIM, Analyse réseau, sources de menaces)

- **Option de FIM et d’Analyse réseau du même éditeur**

Nouveautés

- Nouvelle Interface Web (Facilité d’utilisation)
- Nouveaux modules préconfigurés de sécurité (Solution pré-packagée)
- LogRhythm Network Monitor (Détection des menaces plus avancée)
- Intégration avec des listes de détection des menaces (Détection plus avancée)
- Délégation d’administration + Support plusieurs AIE (Grands comptes)

Modules préconfigurés de sécurité

- Base Security Analytics
- SANS Top 20 Critical Controls for Cyber Defence
- Privileged User Monitoring
- Network Behavioural Anomaly
- APT Attack
- Web Application Defence
- Honeypot Analytics
- Retail Cyber Crime

WHITEPAPER
Retail Cyber Crime
LogRhythm

Several high-profile data breaches have hit retail organizations over the past few years, exposing millions of customers' credit card details and personal information. Some of these breaches involved malware, while others involved malicious insider activity or the use of stolen credentials. In the event of any breach, however, all of these attack vectors leave
indicators and forensic evidence of the compromise in their wake. When these indicators and ev
time via machine-based analytics, initial compromises can be detected so that data breaches ca

Identifying malicious behavior indicative of an initial compromise or attempted data breach req
infrastructure involved in card processing be properly instrumented and monitored for anomal
everything from Point-of-sale (POS) system endpoints to the payment processor, as well as all b
infrastructure. This is a critical component of detecting specific behavior indicative of an attack

For example, when a piece of malware is installed on a POS system, it might reach out to a Com
abnormal communication from the POS. Or the malware might initiate suspicious process activ
to the POS's file system. Another indicator might be a user attempting to abnormally access a b
sensitive customer data. In all of these scenarios, various log trails will contain artifacts of anor
properly monitored and analyzed, will alert organizations that a breach is being attempted.

LogRhythm's Security Intelligence Platform not only collects log data already generated by ope
devices across the credit card processing infrastructure, but can also directly monitor endpoint
an independent, detailed forensic audit trail. All available data can then be analyzed for anomal
the AI Engine, LogRhythm's patented machine analytics technology.

This Threat Insight paper describes how to properly instrument a retail organization's IT enviro
forensic view into anomalous and malicious activity. Techniques include configuring data to be
real time to detect and identify threats and compromises and avoid costly data breaches.

POS Endpoints

Implement Instrumentation

For the AI Engine to monitor POS endpoints for malicious activity, the proper data must be coll
Specifically, we are interested in understanding details about processes that run on a POS endp
user behavior.

If the POS system is running an operating system that supports LogRhythm's System Monitor A
that one be installed to utilize its advanced endpoint monitoring features. These advanced feat
Monitor, Network Connection Monitor, User Activity Monitor, Data Loss Defender, and File Integ
independent and deeper view of system activity. Independent monitoring is critical since malwa
native auditing system. Real-time forensic data generated by the System Monitor will be fed to
machine-based analytics.

Implement SecurityAnalytics

POS endpoints are purpose-specific devices, making them excellent candidates for behavioral b
for certain behavioral dimensions, peer trending. These activities make it easier to identify ano
indicative of malware or other unauthorized activity on the POS endpoint.

To accurately identify when malicious behavior is happening, certain attributes should be moni
POS should be running the same set of processes. Their file systems should look identical to on
change during scheduled updates. Ideally, a single POS should be deployed in a known clean sta

WWW.LOGRHYTHM.COM

WHITEPAPER
SANS Top 20 Critical Controls for Cyber Defense
LogRhythm

SANS "Top 20"
Critical Controls f
Effective Cyber Defe

WWW.LOGRHYTHM.COM

THREAT INSIGHT
The APT Lifecycle and its Log Trail
LogRhythm

Advanced Persistent Threats, or APTs, are a growing concern in the security industry. APTs differentiate themselves from other types of hacking activities by targeting a specific organization for a specific target, often extremely high pay-off data.

APTs are "advanced" in that the attackers often write customized zero-day malware and exploits specific to their target organization. They will also frequently launch specifically targeted "phishing" attacks in an attempt to exploit user systems. In effect, APTs will harness the full spectrum of logical, physical and social attack vectors – with extreme sophistication and capability.

APTs are "persistent" in that they are extremely patient and methodical in their approach to reconnaissance, target compromise, and data exfiltration. An APT doesn't care if it takes a week or a year to reach their objective – just so long as they eventually do.

There is no single attack vector used by APTs, no single activity pattern, and thus no easy way for an organization to protect itself from an APT. A defense-in-depth strategy across logical, physical, and social boundaries is fundamental.

When log data is collected from "touch points" as the APT works through the layers of defense, context is provided along with cross-phase correlation and corroboration to determine what is taking place, how and when.

While no two APTs are the same, most follow a common lifecycle in which reconnaissance is performed against a target organization, an initial compromise of a host is accomplished and credentials are stolen, tools are installed to maintain access, lateral movement to the target data occurs, and ultimately the target data is exfiltrated. Although this activity is generally done "low and slow," often utilizing custom malware and/or legitimate credentials to avoid detection, activity at each phase leaves a footprint in the log trail.

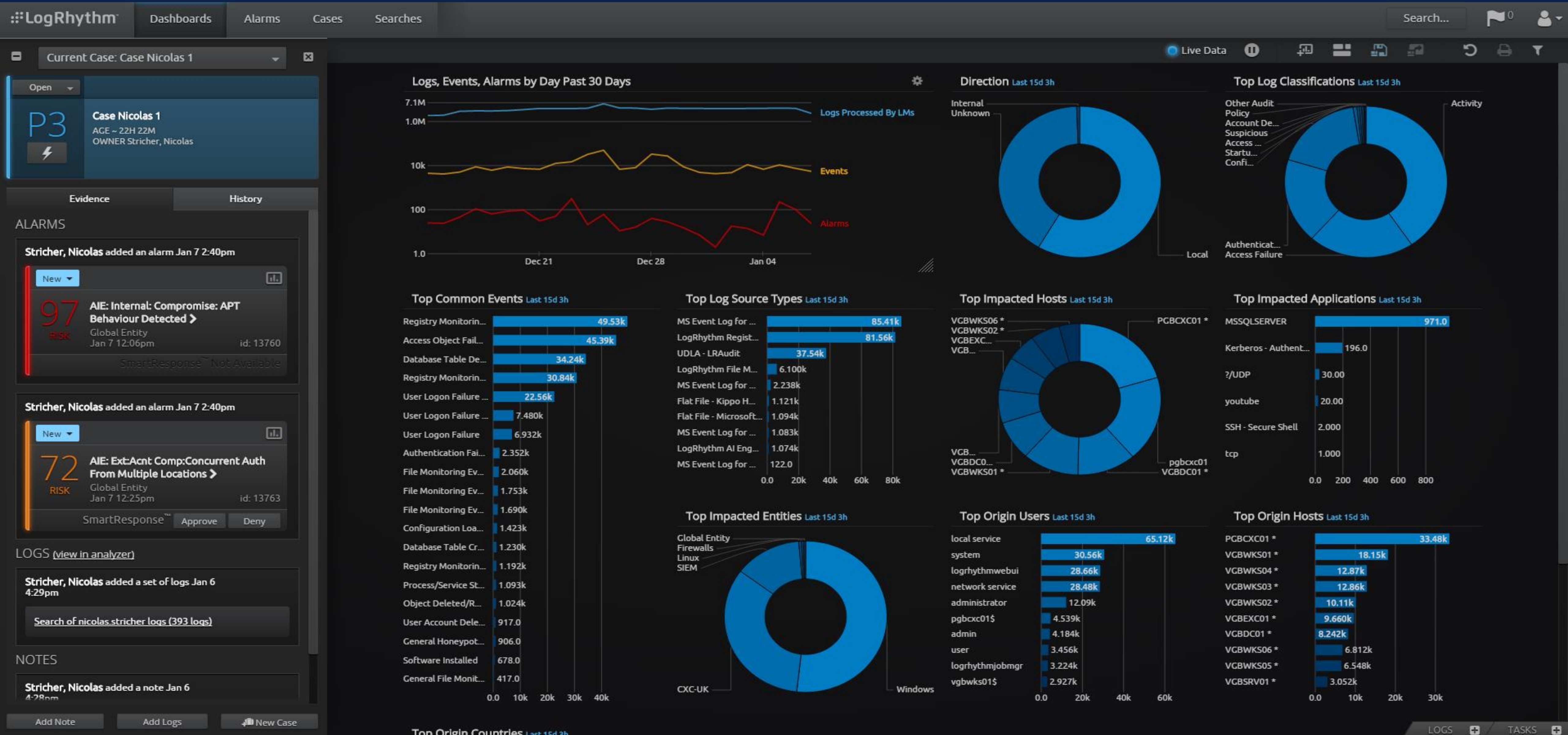
This Threat Insight Paper examines each phase of the APT lifecycle and provides insight and examples of the log trail that is often left behind at each phase.

WWW.LOGRHYTHM.COM PAGE 1

LogRhythm

The Security Intelligence Company

Nouvelle Interface web



Current Case: Case Nicolas 1

Open

P3

Case Nicolas 1
AGE ~ 22H 22M
OWNER Stricher, Nicolas

Evidence | History

ALARMS

Stricher, Nicolas added an alarm Jan 7 2:40pm

New

97 RISK

AIE: Internal: Compromise: APT Behaviour Detected >
Global Entity
Jan 7 12:06pm
id: 13760

SmartResponse™ Not Available

Stricher, Nicolas added an alarm Jan 7 2:40pm

New

72 RISK

AIE: Ext:Acnt Comp:Concurrent Auth From Multiple Locations >
Global Entity
Jan 7 12:25pm
id: 13763

SmartResponse™ Approve Deny

LOGS (view in analyzer)

Stricher, Nicolas added a set of logs Jan 6 4:29pm

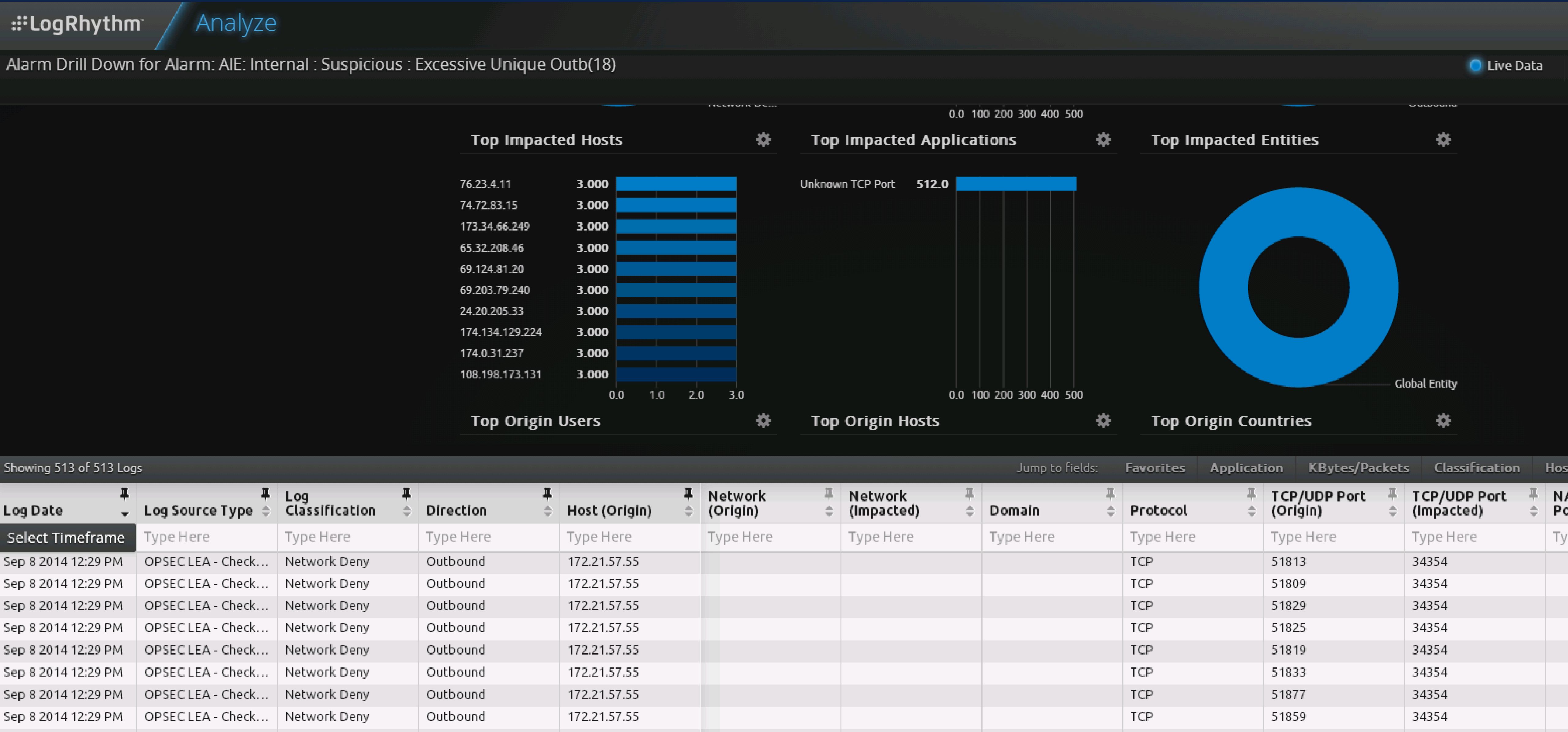
Search of nicolas.stricher logs (393 logs)

NOTES

Stricher, Nicolas added a note Jan 6 4:28pm

LogRhythm
Dashboards
Alarms
Cases
Searches
Search...
0
Live Data
Add Note
Add Logs
New Case
Logs, Events, Alarms by Day Past 30 Days
7.1M
1.0M
10k
100
1.0
Dec 21
Dec 28
Jan 04
Logs Processed By LMs
Events
Alarms
Direction Last 15d 3h
Internal
Unknown
Local
Top Log Classifications Last 15d 3h
Other Audit
Policy
Account De...
Suspicious
Access ...
Startu...
Confi...
Authenticat...
Access Failure
Activity
Top Common Events Last 15d 3h
Registry Monitorin... 49.53k
Access Object Fail... 45.39k
Database Table De... 34.24k
Registry Monitorin... 30.84k
User Logon Failure ... 22.56k
User Logon Failure ... 7.480k
User Logon Failure 6.932k
Authentication Fai... 2.352k
File Monitoring Ev... 2.060k
File Monitoring Ev... 1.753k
File Monitoring Ev... 1.690k
Configuration Loa... 1.423k
Database Table Cr... 1.230k
Registry Monitorin... 1.192k
Process/Service St... 1.093k
Object Deleted/R... 1.024k
User Account Dele... 917.0
General Honeypot... 906.0
Software Installed 678.0
General File Monit... 417.0
0.0 10k 20k 30k 40k
Top Log Source Types Last 15d 3h
MS Event Log for ... 85.41k
LogRhythm Regist... 81.56k
UDLA - LRAudit 37.54k
LogRhythm File M... 6.100k
MS Event Log for ... 2.238k
Flat File - Kippo H... 1.121k
Flat File - Microsoft... 1.094k
MS Event Log for ... 1.083k
LogRhythm AI Eng... 1.074k
MS Event Log for ... 122.0
0.0 20k 40k 60k 80k
Top Impacted Hosts Last 15d 3h
VGBWKS06 *
VGBWKS02 *
VGBEXC...
VGB...
VGB...
VGBDC0...
VGBWKS01 *
PGBCXC01 *
pgbcxc01
VGBDC01 *
Top Impacted Applications Last 15d 3h
MSSQLSERVER 971.0
Kerberos - Authent... 196.0
?/UDP 30.00
youtube 20.00
SSH - Secure Shell 2.000
tcp 1.000
0.0 200 400 600 800
Top Impacted Entities Last 15d 3h
Global Entity
Firewalls
Linux
SIEM
CXC-UK
Windows
Top Origin Users Last 15d 3h
local service 65.12k
system 30.56k
logrhythmwebui 28.66k
network service 28.48k
administrator 12.09k
pgbcxc01$ 4.539k
admin 4.184k
user 3.456k
logrhythmjobmgr 3.224k
vgbwks01$ 2.927k
0.0 20k 40k 60k
Top Origin Hosts Last 15d 3h
PGBCXC01 * 33.48k
VGBWKS01 * 18.15k
VGBWKS04 * 12.87k
VGBWKS03 * 12.86k
VGBWKS02 * 10.11k
VGBEXC01 * 9.660k
VGBDC01 * 8.242k
VGBWKS06 * 6.812k
VGBWKS05 * 6.548k
VGBSRV01 * 3.052k
0.0 10k 20k 30k
Top Origin Countries Last 15d 3h
LOGS
TASKS

Nouvelle Interface web



Alarm Drill Down for Alarm: AIE: Internal : Suspicious : Excessive Unique Outb(18)

Showing 513 of 513 Logs

Log Date	Log Source Type	Log Classification	Direction	Host (Origin)	Network (Origin)	Network (Impacted)	Domain	Protocol	TCP/UDP Port (Origin)	TCP/UDP Port (Impacted)	N Po
Select Timeframe	Type Here	Type Here	Type Here	Type Here	Type Here	Type Here	Type Here	Type Here	Type Here	Type Here	Ty
Sep 8 2014 12:29 PM	OPSEC LEA - Check...	Network Deny	Outbound	172.21.57.55				TCP	51813	34354	
Sep 8 2014 12:29 PM	OPSEC LEA - Check...	Network Deny	Outbound	172.21.57.55				TCP	51809	34354	
Sep 8 2014 12:29 PM	OPSEC LEA - Check...	Network Deny	Outbound	172.21.57.55				TCP	51829	34354	
Sep 8 2014 12:29 PM	OPSEC LEA - Check...	Network Deny	Outbound	172.21.57.55				TCP	51825	34354	
Sep 8 2014 12:29 PM	OPSEC LEA - Check...	Network Deny	Outbound	172.21.57.55				TCP	51819	34354	
Sep 8 2014 12:29 PM	OPSEC LEA - Check...	Network Deny	Outbound	172.21.57.55				TCP	51833	34354	
Sep 8 2014 12:29 PM	OPSEC LEA - Check...	Network Deny	Outbound	172.21.57.55				TCP	51877	34354	
Sep 8 2014 12:29 PM	OPSEC LEA - Check...	Network Deny	Outbound	172.21.57.55				TCP	51859	34354	

Thank you

LogRhythm™