dots.

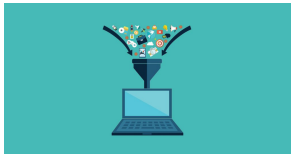
SIEM – prakse, padomi un ieteikumi

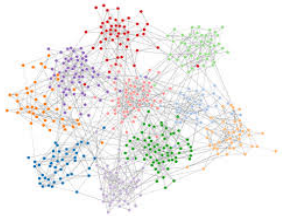
Kaspars Līcis
IT drošības risinājumu grupas vadītājs

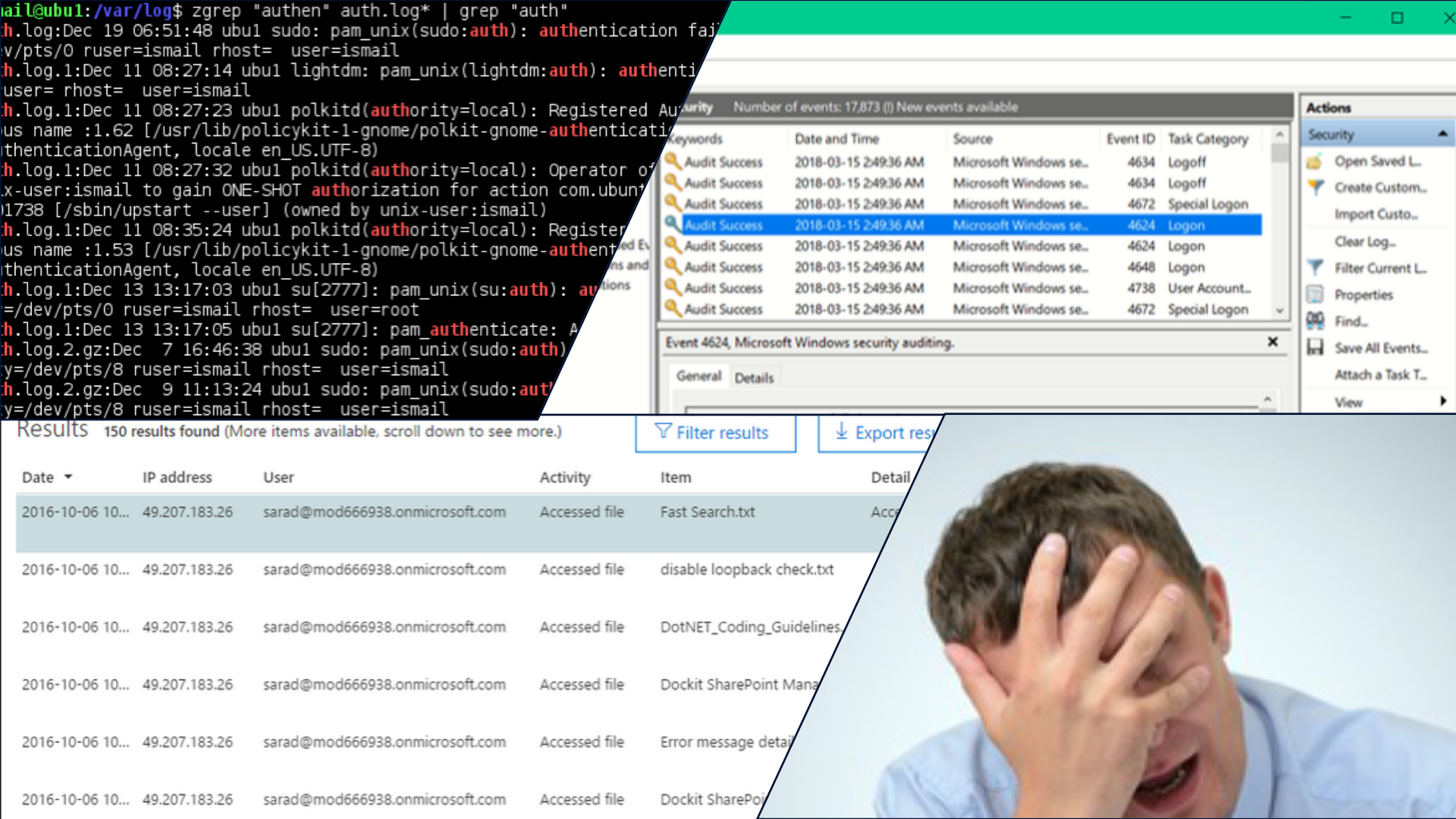
09.10.2018

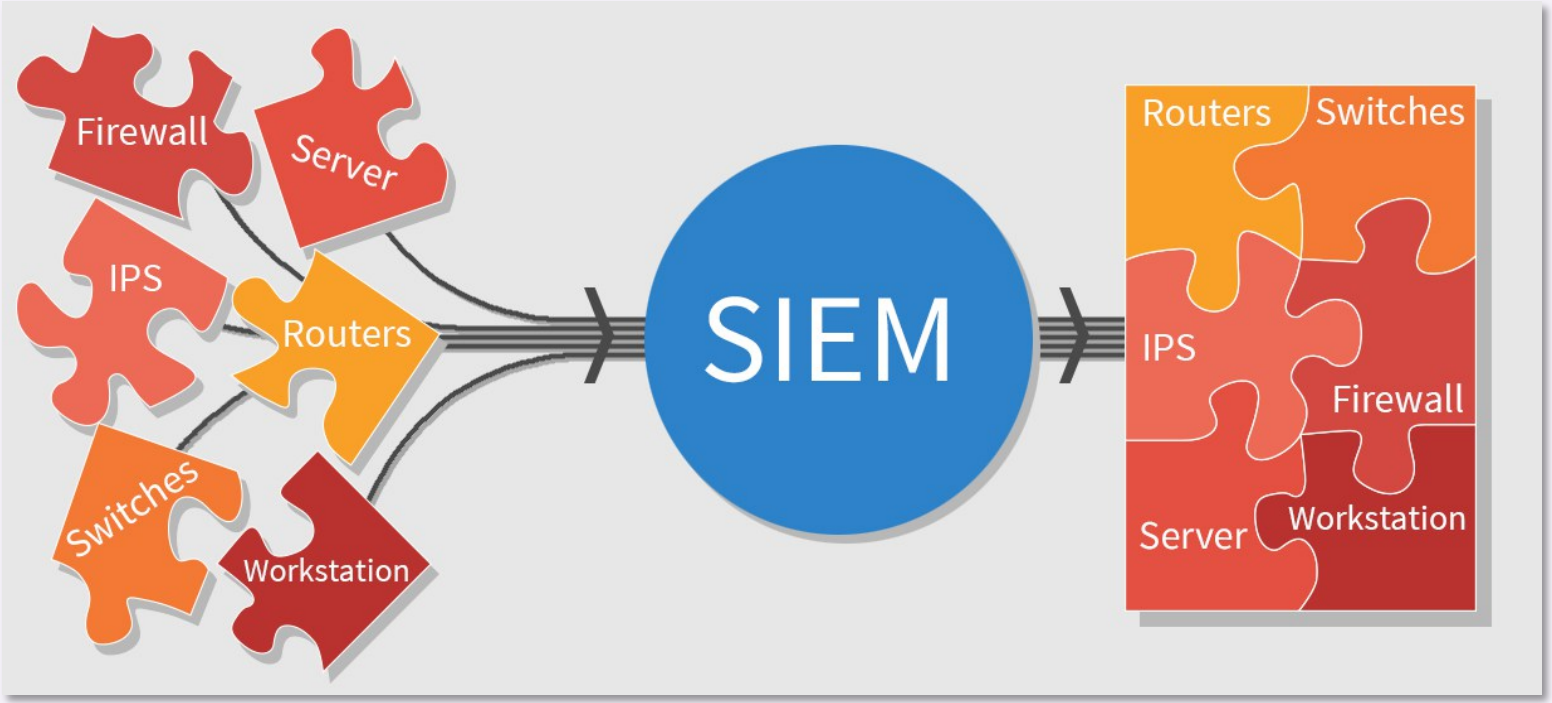

knowledge
performance
skill
vision
Best
Practice
potential
ethic

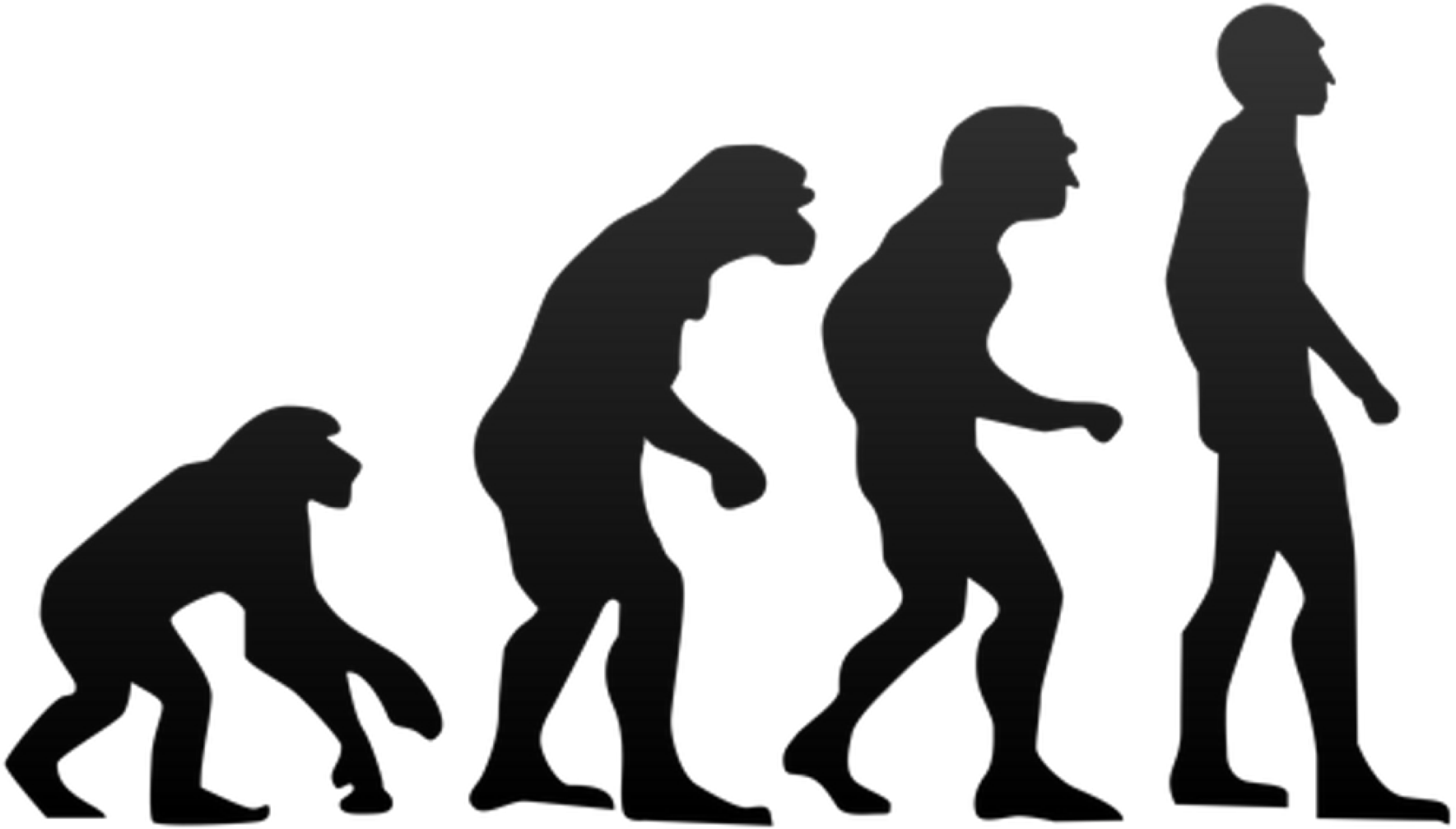
Security information and event management






ail@ubu1:/var/log$ zgrep "authen" auth.log* | grep "auth"
h.log:Dec 19 06:51:48 ubu1 sudo: pam_unix(sudo:auth): authentication fai
v/pts/0 ruser=ismail rhost= user=ismail
h.log.1:Dec 11 08:27:14 ubu1 lightdm: pam_unix(lightdm:auth): authenti
user= rhost= user=ismail
h.log.1:Dec 11 08:27:23 ubu1 polkitd(authority=local): Registered Au
us name :1.62 [/usr/lib/policykit-1-gnome/polkit-gnome-authenticati
thenticationAgent, locale en_US.UTF-8)
h.log.1:Dec 11 08:27:32 ubu1 polkitd(authority=local): Operator of
x-user:ismail to gain ONE-SHOT authorization for action com.ubunt
)1738 [/sbin/upstart --user] (owned by unix-user:ismail)
h.log.1:Dec 11 08:35:24 ubu1 polkitd(authority=local): Register
us name :1.53 [/usr/lib/policykit-1-gnome/polkit-gnome-authen
thenticationAgent, locale en_US.UTF-8)
h.log.1:Dec 13 13:17:03 ubu1 su[2777]: pam_unix(su:auth): au
=/dev/pts/0 ruser=ismail rhost= user=root
h.log.1:Dec 13 13:17:05 ubu1 su[2777]: pam_authenticate: A
h.log.2.gz:Dec 7 16:46:38 ubu1 sudo: pam_unix(sudo:auth)
y=/dev/pts/8 ruser=ismail rhost= user=ismail
h.log.2.gz:Dec 9 11:13:24 ubu1 sudo: pam_unix(sudo:aut
y=/dev/pts/8 ruser=ismail rhost= user=ismail
Number of events: 17,873 (!) New events available
Keywords
Date and Time
Source
Event ID
Task Category
Audit Success 2018-03-15 2:49:36 AM Microsoft Windows se... 4634 Logoff
Audit Success 2018-03-15 2:49:36 AM Microsoft Windows se... 4634 Logoff
Audit Success 2018-03-15 2:49:36 AM Microsoft Windows se... 4672 Special Logon
Audit Success 2018-03-15 2:49:36 AM Microsoft Windows se... 4624 Logon
Audit Success 2018-03-15 2:49:36 AM Microsoft Windows se... 4624 Logon
Audit Success 2018-03-15 2:49:36 AM Microsoft Windows se... 4648 Logon
Audit Success 2018-03-15 2:49:36 AM Microsoft Windows se... 4738 User Account...
Audit Success 2018-03-15 2:49:36 AM Microsoft Windows se... 4672 Special Logon
Event 4624, Microsoft Windows security auditing.
General
Details
Actions
Security
Open Saved L...
Create Custom...
Import Custo...
Clear Log...
Filter Current L...
Properties
Find...
Save All Events...
Attach a Task T...
View
Results
150 results found (More items available, scroll down to see more.)
Filter results
Export res
Date
IP address
User
Activity
Item
Detail
2016-10-06 10... 49.207.183.26 sarad@mod666938.onmicrosoft.com Accessed file Fast Search.txt
2016-10-06 10... 49.207.183.26 sarad@mod666938.onmicrosoft.com Accessed file disable loopback check.txt
2016-10-06 10... 49.207.183.26 sarad@mod666938.onmicrosoft.com Accessed file DotNET_Coding_Guidelines
2016-10-06 10... 49.207.183.26 sarad@mod666938.onmicrosoft.com Accessed file Dockit SharePoint Mana
2016-10-06 10... 49.207.183.26 sarad@mod666938.onmicrosoft.com Accessed file Error message detai
2016-10-06 10... 49.207.183.26 sarad@mod666938.onmicrosoft.com Accessed file Dockit SharePoi


Firewall
Server
IPS
Routers
Switches
Workstation
SIEM
Routers
Switches
IPS
Firewall
Server
Workstation

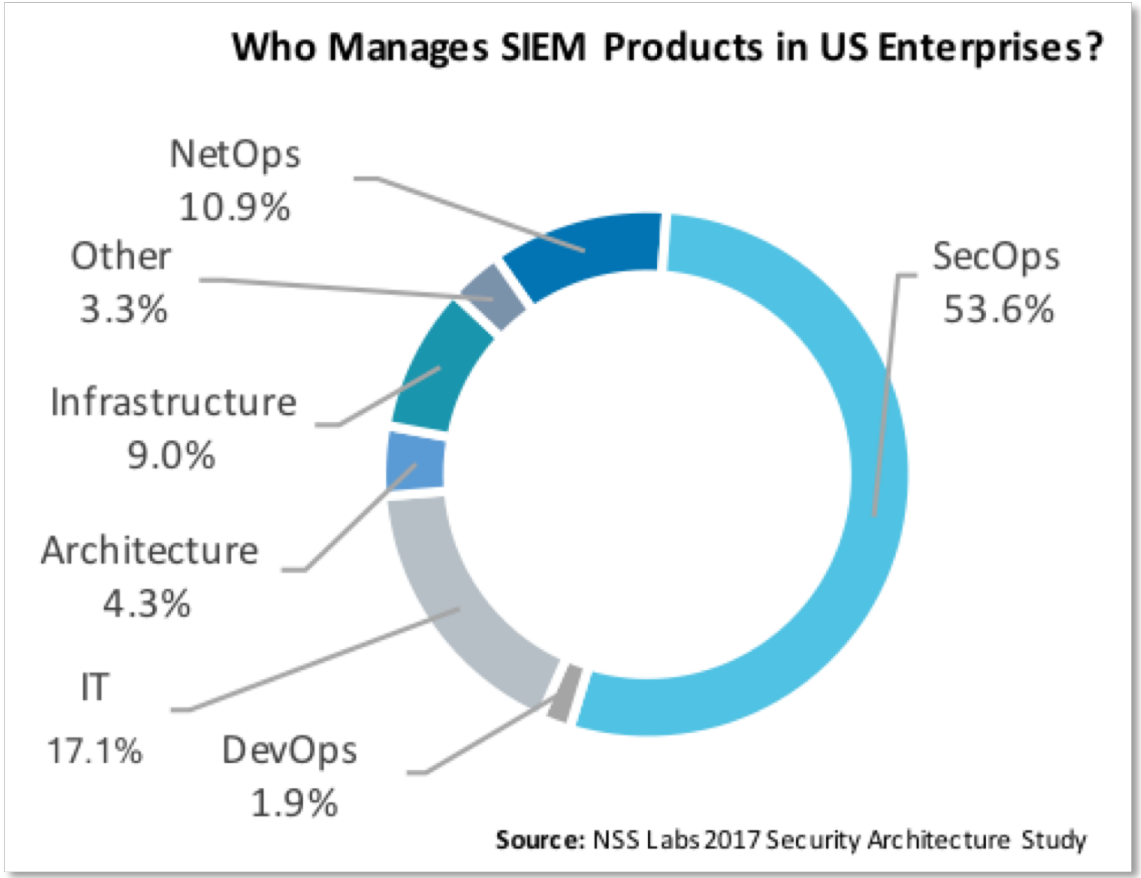


SANS top 20

Critical Control		Effect on Attack Mitigation
1.	Inventory of Authorized and Unauthorized Devices	Very High
2.	Inventory of Authorized and Unauthorized Software	Very High
3.	Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Very High
4.	Continuous Vulnerability Assessment and Remediation	Very High
5.	Malware Defenses	High
6.	Application Software Security	High
7.	Wireless Device Control	High
8.	Data Recovery Capability	Moderately High to High
9.	Security Skills Assessment and Appropriate Training to Fill Gaps	Moderately High to High
10.	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Moderately High
11.	Limitation and Control of Network Ports, Protocols, and Services	Moderately High
12.	Controlled Use of Administrative Privileges	Moderate to Moderately High
13.	Boundary Defense	Moderate
14.	Maintenance, Monitoring, and Analysis of Security Audit Logs	Moderate
15.	Controlled Access Based on the Need to Know	Moderate
16.	Account Monitoring and Control	Moderate
17.	Data Loss Prevention	Moderately Low to Moderate
18.	Incident Response Capability	Moderately Low to Moderate
19.	Secure Network Engineering	Low
20.	Penetration Tests and Red Team Exercises	Low

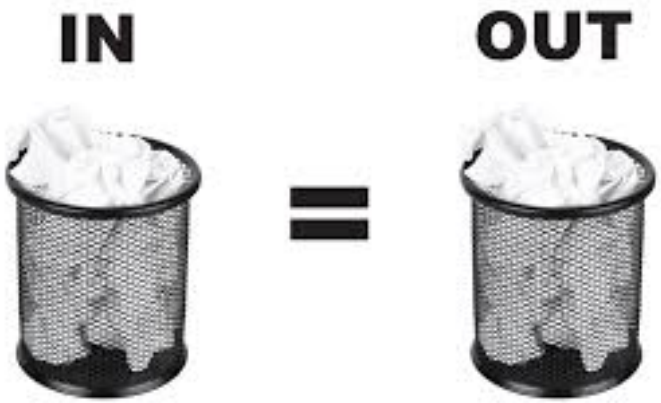

Pretty Miss


YJK 006
JL 888
LH 60
VW
LATVIJAS
GADA
AUTO
2018


Who Manages SIEM Products in US Enterprises?
NetOps
10.9%
Other
3.3%
Infrastructure
9.0%
Architecture
4.3%
IT
17.1%
DevOps
1.9%
SecOps
53.6%
Source: NSS Labs 2017 Security Architecture Study

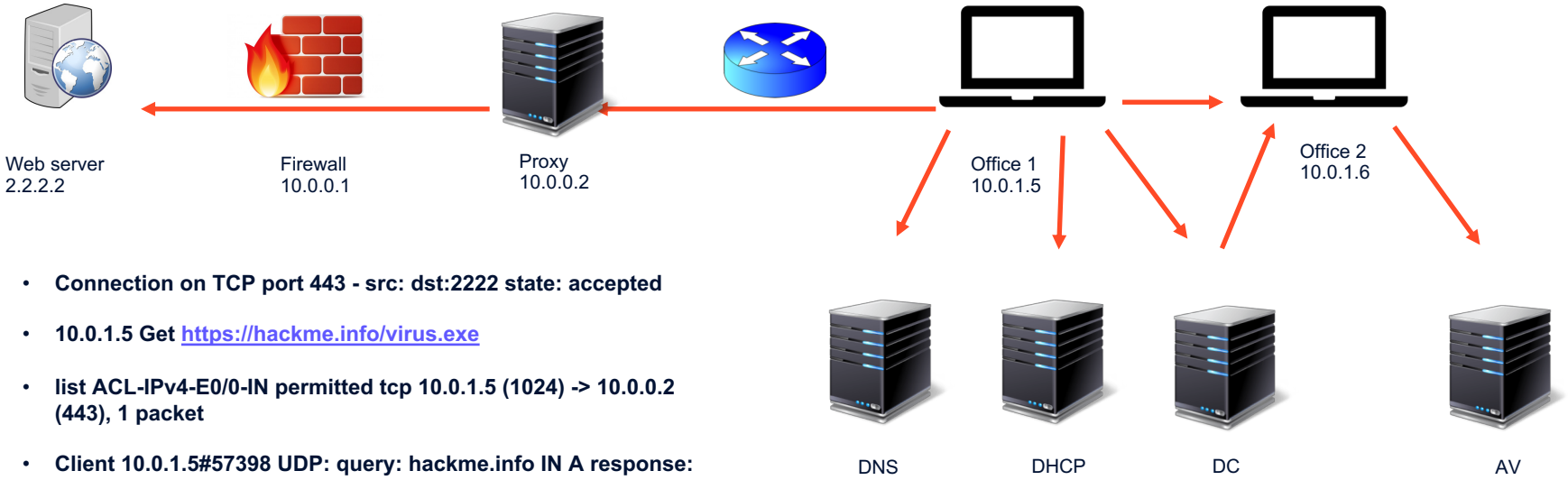

80
20


There are no shortcuts to any place worth going.
Helen Keller
quotefancy


IN
OUT


THE COMPASS WILL TELL YOU WHICH WAY IS NORTH
BUT IT CANNOT TELL YOU WHICH WAY IS RIGHT
THIS FOR EXAMPLE IS VERY BAD


OUTSOURCE
INHOUSE



- **Connection on TCP port 443 - src: dst:2222 state: accepted**
- **10.0.1.5 Get https://hackme.info/virus.exe**
- **list ACL-IPv4-E0/0-IN permitted tcp 10.0.1.5 (1024) -> 10.0.0.2 (443), 1 packet**
- **Client 10.0.1.5#57398 UDP: query: hackme.info IN A response: NOERROR +AED hackme.info 28800 IN A 2.2.2.2**
- **Lease for 10.0.1.5 Assigned to Office1 - MAC:AE:00:AA:10:FF:DD**
- **Authentic Package: MICROSOFT_AUTHENTICATION_pACKAGE_V1_0 Logon Account: Kaspars Source Workstation: Office1**
- **Client:Office2 - Succesifully removed - C:\Windows\Temp\virus.dll - Reason: Win32/RatProxy**

SOURCE	nb30ptl [172.21.2.36]

Hostname: nb30ptl
MAC Address: C8:5B:76:67:87:0E
Port: 63795
Latest update: *N/A*
Username & Domain: *N/A*
Asset Value: 2

Location: *N/A*
Context: d81de3eb-1085-11e5-b941-000c29d195d0
Asset Groups: *N/A*
Networks: LV-Riga-Main-Office
Logged Users: *N/A*
OTX IP Reputation: No

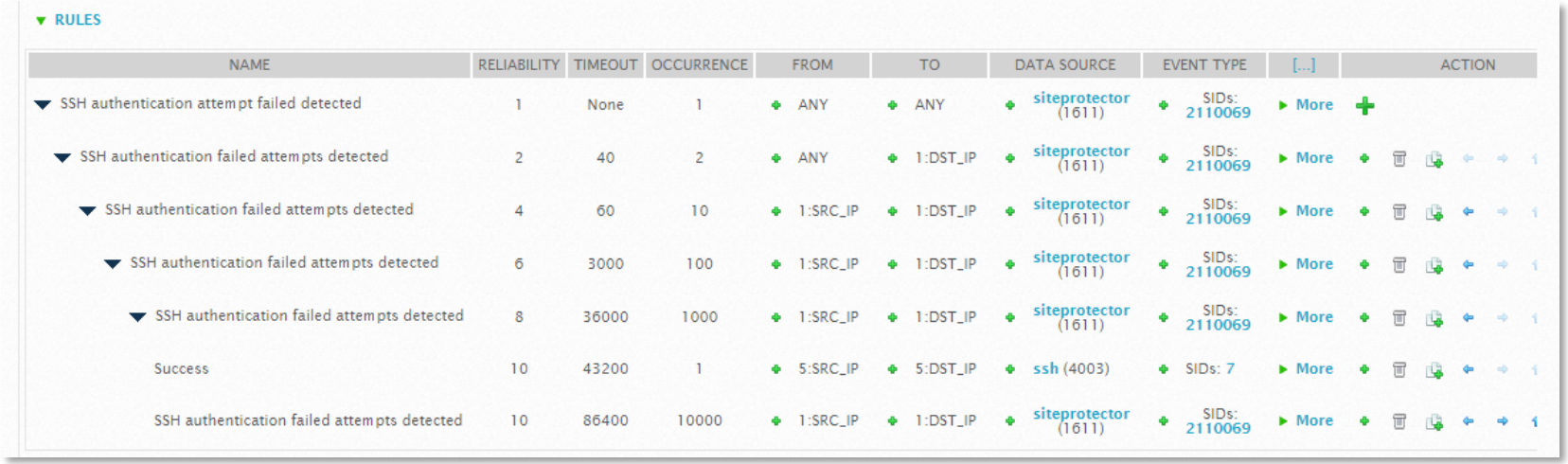
DESTINATION	DC-LV-01 [172.21.0.2]

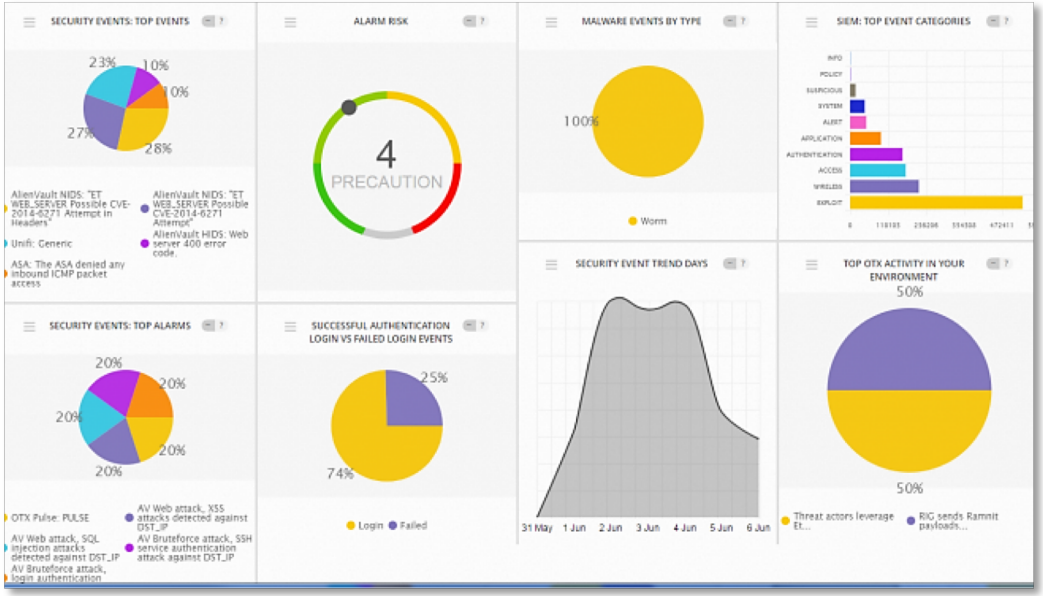
Hostname: DC-LV-01
MAC Address: 00:15:5D:00:04:07
Port: *N/A*
Latest update: *N/A*
Username & Domain: *N/A*
Asset Value: 3

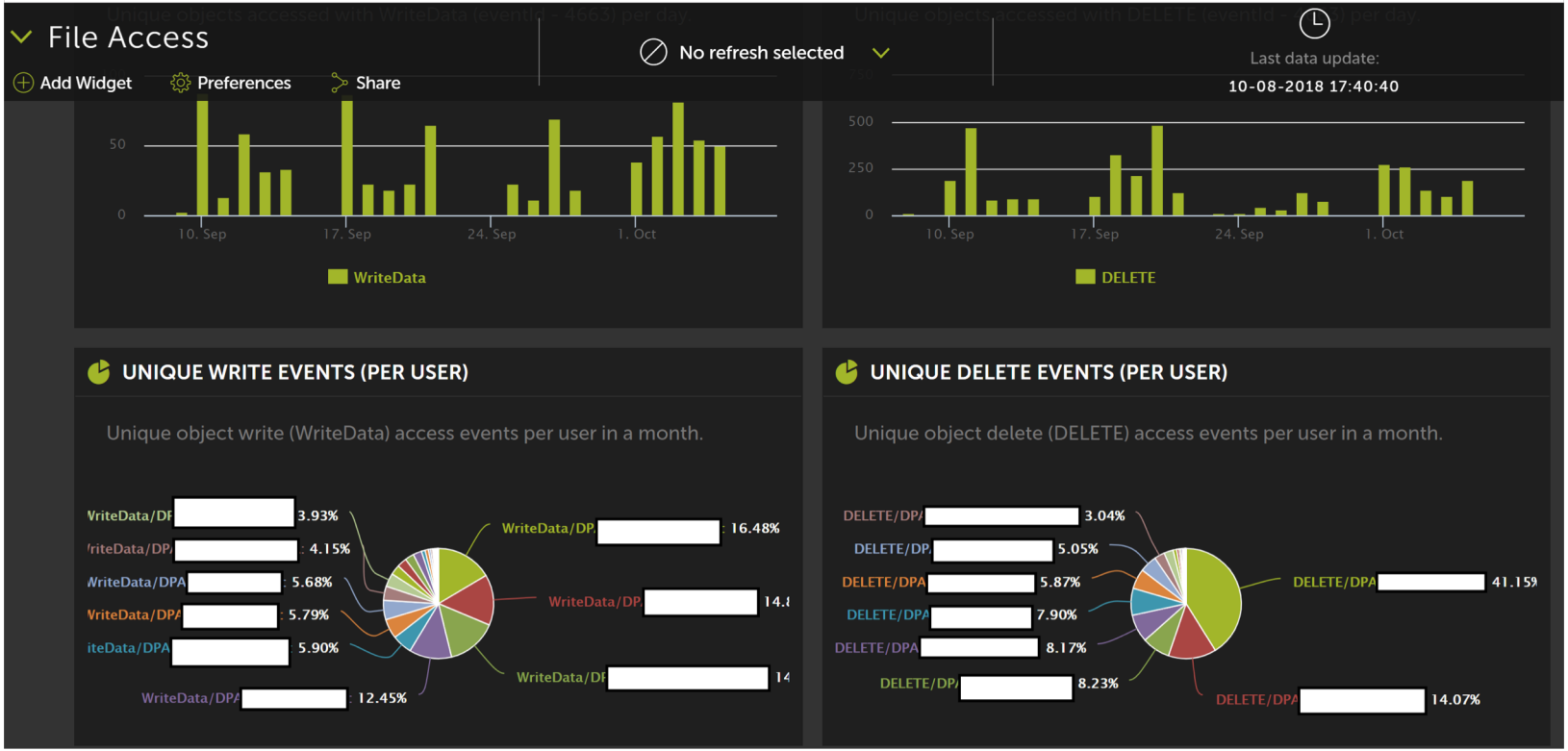
Location: *N/A*
Context: d81de3eb-1085-11e5-b941-000c29d195d0
Asset Groups: AlienVault HIDS Availability monitoring
Networks: LV-Riga-Main-Office
Logged Users: *N/A*
OTX IP Reputation: No

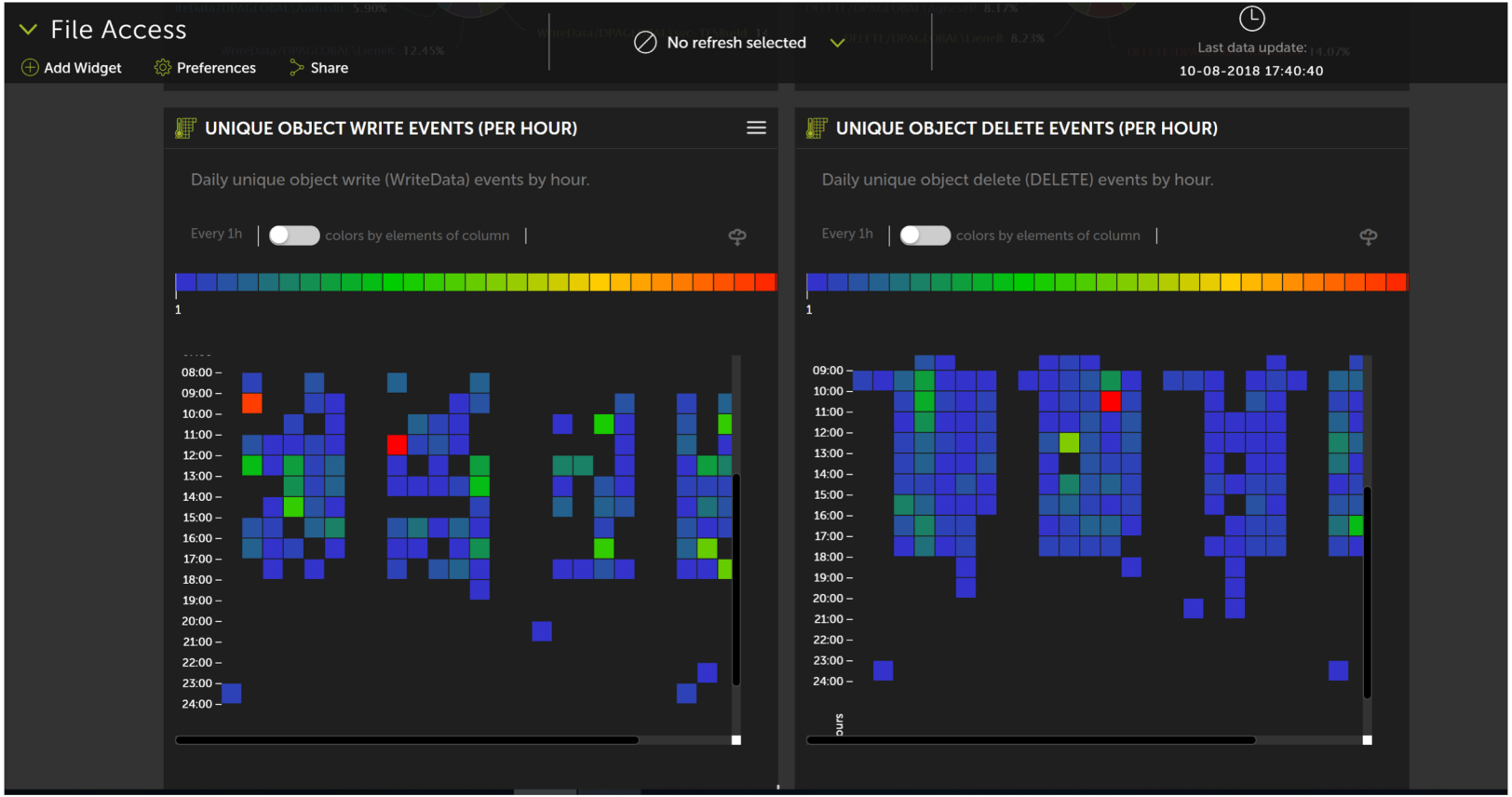
USERDATA1	USERDATA2	USERDATA3	USERDATA4	USERDATA6
2	windows,authentication_success,	A Kerberos service ticket was requested: Success.	4769	DP

USERDATA7	USERDATA8	USERDATA9	USERNAME
0x0	DC-LV-01	DC-LV-01	Lu


RULES
NAME
RELIABILITY
TIMEOUT
OCCURRENCE
FROM
TO
DATA SOURCE
EVENT TYPE
[...]
ACTION
SSH authentication attempt failed detected
1
None
1
ANY
ANY
siteprotector (1611)
SIDs: 2110069
More
SSH authentication failed attempts detected
2
40
2
ANY
1:DST_IP
siteprotector (1611)
SIDs: 2110069
More
SSH authentication failed attempts detected
4
60
10
1:SRC_IP
1:DST_IP
siteprotector (1611)
SIDs: 2110069
More
SSH authentication failed attempts detected
6
3000
100
1:SRC_IP
1:DST_IP
siteprotector (1611)
SIDs: 2110069
More
SSH authentication failed attempts detected
8
36000
1000
1:SRC_IP
1:DST_IP
siteprotector (1611)
SIDs: 2110069
More
Success
10
43200
1
5:SRC_IP
5:DST_IP
ssh (4003)
SIDs: 7
More
SSH authentication failed attempts detected
10
86400
10000
1:SRC_IP
1:DST_IP
siteprotector (1611)
SIDs: 2110069
More


SECURITY EVENTS: TOP EVENTS
23%
10%
10%
27%
28%
AlienVault NIDS: "ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers"
AlienVault NIDS: "ET WEB_SERVER Possible CVE-2014-6271 Attempt"
Unifi: Generic
AlienVault HIDS: Web server 400 error code.
ASA: The ASA denied any inbound ICMP packet access
ALARM RISK
4
PRECAUTION
MALWARE EVENTS BY TYPE
100%
Worm
SIEM: TOP EVENT CATEGORIES
INFO
POLICY
SUSPICIOUS
SYSTEM
ALERT
APPLICATION
AUTHENTICATION
ACCESS
WIRELESS
EXPLOIT
SECURITY EVENTS: TOP ALARMS
20%
20%
20%
20%
20%
OTX Pulse: PULSE
AV Web attack, XSS attacks detected against DST_IP
AV Web attack, SQL injection attacks detected against DST_IP
AV Bruteforce attack, SSH service authentication attack against DST_IP
AV Bruteforce attack, login authentication
SUCCESSFUL AUTHENTICATION LOGIN VS FAILED LOGIN EVENTS
25%
74%
Login
Failed
SECURITY EVENT TREND DAYS
31 May
1 Jun
2 Jun
3 Jun
4 Jun
5 Jun
6 Jun
TOP OTX ACTIVITY IN YOUR ENVIRONMENT
50%
50%
Threat actors leverage Et...
RIG sends Ramnit payloads...


File Access
Add Widget
Preferences
Share
No refresh selected
Last data update:
10-08-2018 17:40:40
50
0
10. Sep
17. Sep
24. Sep
1. Oct
WriteData
500
250
0
10. Sep
17. Sep
24. Sep
1. Oct
DELETE
UNIQUE WRITE EVENTS (PER USER)
Unique object write (WriteData) access events per user in a month.
3.93%
4.15%
5.68%
5.79%
5.90%
12.45%
16.48%
UNIQUE DELETE EVENTS (PER USER)
Unique object delete (DELETE) access events per user in a month.
3.04%
5.05%
5.87%
7.90%
8.17%
8.23%
41.15%
14.07%


File Access
Add Widget
Preferences
Share
No refresh selected
Last data update:
10-08-2018 17:40:40
UNIQUE OBJECT WRITE EVENTS (PER HOUR)
Daily unique object write (WriteData) events by hour.
Every 1h
colors by elements of column
1
08:00 –
09:00 –
10:00 –
11:00 –
12:00 –
13:00 –
14:00 –
15:00 –
16:00 –
17:00 –
18:00 –
19:00 –
20:00 –
21:00 –
22:00 –
23:00 –
24:00 –
UNIQUE OBJECT DELETE EVENTS (PER HOUR)
Daily unique object delete (DELETE) events by hour.
Every 1h
colors by elements of column
1
09:00 –
10:00 –
11:00 –
12:00 –
13:00 –
14:00 –
15:00 –
16:00 –
17:00 –
18:00 –
19:00 –
20:00 –
21:00 –
22:00 –
23:00 –
24:00 –

Microsoft DHCP Service Activity Log

Event ID Meaning

00 The log was started.

01 The log was stopped.

02 The log was temporarily paused due to low disk space.

10 A new IP address was leased to a client.

11 A lease was renewed by a client.

12 A lease was released by a client.

DHCP: A suspicious device was assigned an internal IP address

An IP address has been assigned to a host not according to established naming schema.

DHCP Server: dc-lv-01

Time: 10/05/18 18:17:31

Hostname: null

MAC: 000D48542A53

IP address: /172.21.1.75

Lietošanas gadījumi un izmaksas

Ieviešanas projekts

- Kāds ir ieviešanas mērķis?
- Kādus riskus vēlamies samazināt?
- Kādas sistēmas uzraudzīsim?
- Kāda ir normāla uzvedība?
- Kādas kontroles uzraudzīt?
- Kādus notikumus meklēt?
- Cik ilgi jāglabā?
- Kādus protokolus izmanto?

- Cloud vai Onpremise?
- Vai tas nenoslogos tīklu?
- Cik daudz storage un CPU vajadzēs?
- Kādu risinājumu izvēlēties?

- Bloķētie izejošie savienojumi ugunsmūrī;
- Bloķētie izejošie savienojumi IPS;
- Bloķēta ļaunatūra;
- Vienlaicīgie masveida autentifikācijas vai pieslēgumu pieprasījumi no vienas IP adreses;
- Lokāla lietotāja izveide;
- Masveida autentifikācijas pieprasījumi;
- Masveida failu piekļuve, kopēšana, dzēšana;
- «Slepenie» failu piekļuve;
- Ievainojamību identificēšana;
- Ārpus normāla aplikācijas darbība.

Kādi ir mūsu ieguvumi?

Kāpēc neizdodas?

- Atšķirīgas intereses – ražotājs, konsultants, klients;
- Atšķirīga izpratne – biznesa vadītājs, IT vadītājs, drošības analītiķis;
- Nav definēts mērķis;
- Nav paredzēts atbilstošs budžets, resursi;
- Noklusētie iestatījumi;
- Nav izvēlēts atbilstošākais rīks.