info@example.com
https://example.com

GDPR report

General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.

2019-09-11T16:19:37 to 2019-09-11T18:19:37

manager.name: S-DEMO-SEC01.example.com AND rule.gdpr: exists

Most common GDPR requirements alerts found

Requirement IV_32.2

Account management tools that closely monitor actions taken by standard administrators and users who use standard or privileged account credentials are required to control access to data.

Top rules for IV_32.2 requirement

Rule ID	Description
87907	Docker: Command launched in container k8s_calico-kube-controllers_calico-kube-controllers-65b8787765-b5n5v_kube-system_b48ca686-bc9d-4cce-b6a0-9bacccca21fc_0. Action: "exec_start: /usr/bin/check-status -r"
87907	Docker: Command launched in container k8s_calico-node_calico-node-7jldd_kube-system_60276a08-3097-424a-91a6-440d6e2a3679_0. Action: "exec_start: /bin/calico-node -bird-ready -felix-ready"
87907	Docker: Command launched in container k8s_calico-node_calico-node-q76xw_kube-system_ef2bf11c-9c8f-43e4-867b-ab6ec5d20048_0. Action: "exec_start: /bin/calico-node -bird-ready -felix-ready"

Requirement IV_35.7.d

Capabilities for identification, blocking and forensic investigation of data breaches by malicious actors, through compromised credentials, unauthorized network access, persistent threats and verification of the correct operation of all components. Network perimeter and endpoint security tools to prevent unauthorized access to the network, prevent the entry of unwanted data types and malicious threats. Anti-malware and anti-ransomware to prevent malware and ransomware threats from entering your devices. A behavioral analysis that uses machine intelligence to identify people who do anomalous things on the network, in order to give early visibility and alert employees who start to become corrupt.

Top rules for IV_35.7.d requirement

Rule ID	Description

Rule ID	Description
60104	Windows audit failure event
23503	Kernel: KVM: leak of uninitialized stack contents to guest
23505	Kernel: page cache side channel attacks

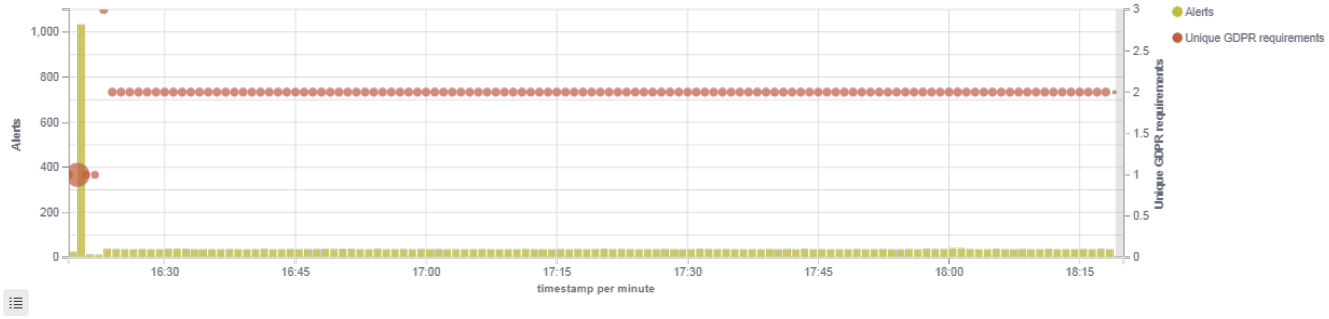
Requirement II_5.1.f

Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, verifying its modifications, accesses, locations and guarantee the safety of them. File sharing protection and file sharing technologies that meet the requirements of data protection.

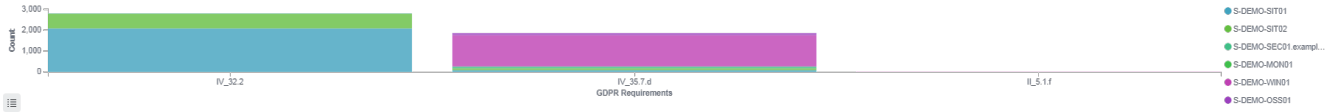
Top rules for II_5.1.f requirement

Rule ID	Description
550	Integrity checksum changed.

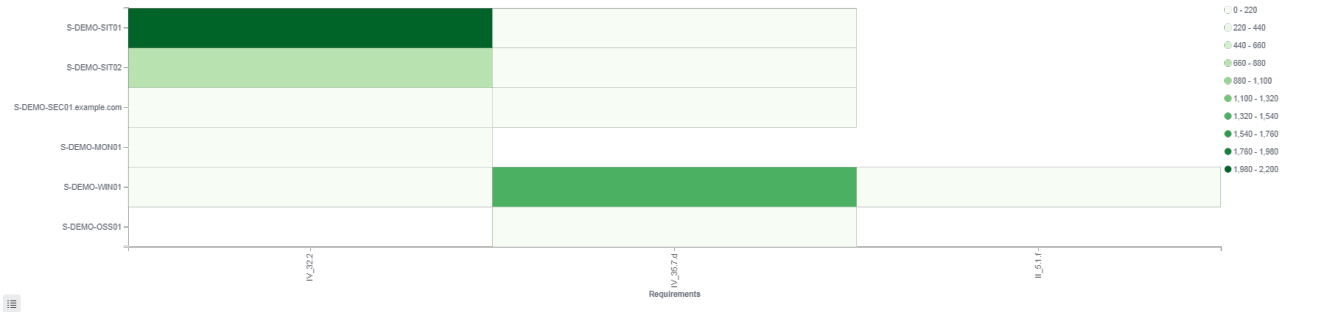
GDPR Requirements



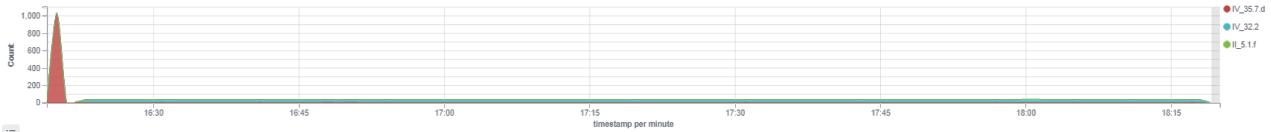
GDPR Requirements by agent



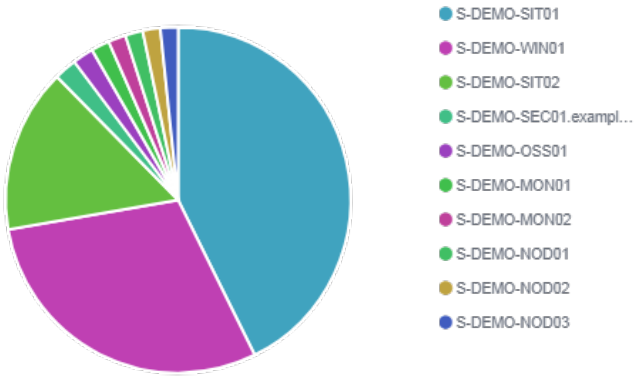
Last alerts



GDPR requirements over time



GDPR Agents



Alerts summary

Agent name	Requirement	Rule description	Count
S-DEMO-WIN01	IV_35.7.d	Windows audit failure event	1483
S-DEMO-SIT01	IV_32.2	Docker: Command launched in container k8s_calico-kube-controllers_calico-kube-controllers-65b8787765-b5n5v_kube-system_b48ca686-bc9d-4cce-b6a0-9bacccca21fc_0. Action: "exec_start: /usr/bin/check-status -r"	696
S-DEMO-SIT01	IV_32.2	Docker: Command launched in container k8s_calico-node_calico-node-q76xw_kube-system_ef2bf11c-9c8f-43e4-867b-ab6ec5d20048_0. Action: "exec_start: /bin/calico-node -bird-ready -felix-ready"	696
S-DEMO-SIT01	IV_32.2	Docker: Command launched in container k8s_etcd_etcd-s-demo-sit01.example.com_kube-system_ebcc081ed9b81785642758bc6ada4f36_0. Action: "exec_start: /bin/sh -ec ETCDCTL_API=3 etcdctl --endpoints=https://[127.0.0.1]:2379 --cacert=/etc/kubernetes/pki/etcd/ca.crt --cert=/etc/kubernetes/pki/etcd/healthcheck-client.crt --key=/etc/kubernetes/pki/etcd/healthcheck-client.key get foo"	696
S-DEMO-SIT02	IV_32.2	Docker: Command launched in container k8s_calico-node_calico-node-7jldd_kube-system_60276a08-3097-424a-91a6-440d6e2a3679_0. Action: "exec_start: /bin/calico-node -bird-ready -felix-ready"	696
S-DEMO-SEC01.example.com	IV_32.2	PAM: Login session closed.	7
S-DEMO-SEC01.example.com	IV_32.2	PAM: Login session opened.	7
S-DEMO-WIN01	II_5.1.f	Integrity checksum changed.	3
S-DEMO-SEC01.example.com	IV_32.2	sshd: authentication success.	3
S-DEMO-MON01	IV_32.2	PAM: Login session closed.	3
S-DEMO-SEC01.example.com	IV_32.2	Successful sudo to ROOT executed	2
S-DEMO-SIT01	IV_35.7.d	Kernel: KVM: leak of uninitialized stack contents to guest	1
S-DEMO-SIT01	IV_35.7.d	Kernel: page cache side channel attacks	1
S-DEMO-SIT01	IV_35.7.d	Kernel: tcp: excessive resource consumption while processing SACK blocks allows remote denial of service	1
S-DEMO-SIT01	IV_35.7.d	Kernel: tcp: integer overflow while processing SACK blocks allows remote denial of service	1
S-DEMO-SIT01	IV_35.7.d	Kernel: vhost_net: infinite loop while receiving packets leads to DoS	1
S-DEMO-SIT01	IV_35.7.d	ROHNP: Key Extraction Side Channel in Multiple Crypto Libraries	1
S-DEMO-SIT01	IV_35.7.d	binutils: NULL pointer dereference in work_stuff_copy_to_from in cplus-dem.c.	1
S-DEMO-SIT01	IV_35.7.d	binutils: Stack Exhaustion in the demangling functions provided by libiberty	1
S-DEMO-SIT01	IV_35.7.d	binutils: integer overflow leads to heap-based buffer overflow in objdump	1
S-DEMO-SIT01	IV_35.7.d	blktrace: buffer overflow in the dev_map_read function in btt/devmap.c	1
S-DEMO-WIN01	IV_35.7.d	Ossec agent started.	1
S-DEMO-WIN01	IV_35.7.d	Session reconnected/disconnected to winstation	1
S-DEMO-WIN01	IV_32.2	Windows User Logoff	1
S-DEMO-SIT02	IV_35.7.d	Kernel: KVM: leak of uninitialized stack contents to guest	1
S-DEMO-SIT02	IV_35.7.d	Kernel: page cache side channel attacks	1
S-DEMO-SIT02	IV_35.7.d	Kernel: tcp: excessive resource consumption while processing SACK blocks allows remote denial of service	1
S-DEMO-SIT02	IV_35.7.d	Kernel: tcp: integer overflow while processing SACK blocks allows remote denial of service	1

Agent name	Requirement	Rule description	Count
S-DEMO-SIT02	IV_35.7.d	Kernel: vhost_net: infinite loop while receiving packets leads to DoS	1
S-DEMO-SIT02	IV_35.7.d	ROHNP: Key Extraction Side Channel in Multiple Crypto Libraries	1
S-DEMO-SIT02	IV_35.7.d	binutils: NULL pointer dereference in work_stuff_copy_to_from in cplus-dem.c.	1
S-DEMO-SIT02	IV_35.7.d	binutils: Stack Exhaustion in the demangling functions provided by libiberty	1
S-DEMO-SIT02	IV_35.7.d	binutils: integer overflow leads to heap-based buffer overflow in objdump	1
S-DEMO-SIT02	IV_35.7.d	blktrace: buffer overflow in the dev_map_read function in btt/devmap.c	1
S-DEMO-SEC01.example.com	IV_35.7.d	Host-based anomaly detection event (rootcheck).	1
S-DEMO-SEC01.example.com	IV_35.7.d	Kernel: KVM: leak of uninitialized stack contents to guest	1
S-DEMO-SEC01.example.com	IV_35.7.d	Kernel: page cache side channel attacks	1
S-DEMO-SEC01.example.com	IV_35.7.d	Kernel: tcp: excessive resource consumption while processing SACK blocks allows remote denial of service	1
S-DEMO-SEC01.example.com	IV_35.7.d	Kernel: tcp: integer overflow while processing SACK blocks allows remote denial of service	1
S-DEMO-SEC01.example.com	IV_35.7.d	Kernel: vhost_net: infinite loop while receiving packets leads to DoS	1
S-DEMO-SEC01.example.com	IV_35.7.d	ROHNP: Key Extraction Side Channel in Multiple Crypto Libraries	1
S-DEMO-SEC01.example.com	IV_35.7.d	binutils: NULL pointer dereference in work_stuff_copy_to_from in cplus-dem.c.	1
S-DEMO-SEC01.example.com	IV_35.7.d	binutils: Stack Exhaustion in the demangling functions provided by libiberty	1
S-DEMO-SEC01.example.com	IV_35.7.d	binutils: integer overflow leads to heap-based buffer overflow in objdump	1
S-DEMO-OSS01	IV_35.7.d	Kernel: KVM: leak of uninitialized stack contents to guest	1
S-DEMO-OSS01	IV_35.7.d	Kernel: page cache side channel attacks	1
S-DEMO-OSS01	IV_35.7.d	Kernel: tcp: excessive resource consumption while processing SACK blocks allows remote denial of service	1
S-DEMO-OSS01	IV_35.7.d	Kernel: tcp: integer overflow while processing SACK blocks allows remote denial of service	1
S-DEMO-OSS01	IV_35.7.d	Kernel: vhost_net: infinite loop while receiving packets leads to DoS	1
S-DEMO-OSS01	IV_35.7.d	ROHNP: Key Extraction Side Channel in Multiple Crypto Libraries	1
S-DEMO-OSS01	IV_35.7.d	binutils: NULL pointer dereference in work_stuff_copy_to_from in cplus-dem.c.	1
S-DEMO-OSS01	IV_35.7.d	binutils: Stack Exhaustion in the demangling functions provided by libiberty	1
S-DEMO-OSS01	IV_35.7.d	binutils: integer overflow leads to heap-based buffer overflow in objdump	1
S-DEMO-OSS01	IV_35.7.d	blktrace: buffer overflow in the dev_map_read function in btt/devmap.c	1
S-DEMO-MON01	IV_35.7.d	Kernel: KVM: leak of uninitialized stack contents to guest	1
S-DEMO-MON01	IV_35.7.d	Kernel: page cache side channel attacks	1
S-DEMO-MON01	IV_35.7.d	Kernel: tcp: excessive resource consumption while processing SACK blocks allows remote denial of service	1
S-DEMO-MON01	IV_35.7.d	Kernel: tcp: integer overflow while processing SACK blocks allows remote denial of service	1
S-DEMO-MON01	IV_35.7.d	Kernel: vhost_net: infinite loop while receiving packets leads to DoS	1
S-DEMO-MON01	IV_35.7.d	ROHNP: Key Extraction Side Channel in Multiple Crypto Libraries	1
S-DEMO-MON01	IV_35.7.d	binutils: NULL pointer dereference in work_stuff_copy_to_from in cplus-dem.c.	1

Agent name	Requirement	Rule description	Count
S-DEMO-MON01	IV_35.7.d	binutils: Stack Exhaustion in the demangling functions provided by libiberty	1
S-DEMO-MON01	IV_35.7.d	binutils: integer overflow leads to heap-based buffer overflow in objdump	1
S-DEMO-MON01	IV_35.7.d	blktrace: buffer overflow in the dev_map_read function in btt/devmap.c	1
S-DEMO-MON02	IV_35.7.d	Kernel: KVM: leak of uninitialized stack contents to guest	1
S-DEMO-MON02	IV_35.7.d	Kernel: page cache side channel attacks	1
S-DEMO-MON02	IV_35.7.d	Kernel: tcp: excessive resource consumption while processing SACK blocks allows remote denial of service	1
S-DEMO-MON02	IV_35.7.d	Kernel: tcp: integer overflow while processing SACK blocks allows remote denial of service	1
S-DEMO-MON02	IV_35.7.d	Kernel: vhost_net: infinite loop while receiving packets leads to DoS	1
S-DEMO-MON02	IV_35.7.d	ROHNP: Key Extraction Side Channel in Multiple Crypto Libraries	1
S-DEMO-MON02	IV_35.7.d	binutils: NULL pointer dereference in work_stuff_copy_to_from in cplus-dem.c.	1
S-DEMO-MON02	IV_35.7.d	binutils: Stack Exhaustion in the demangling functions provided by libiberty	1
S-DEMO-MON02	IV_35.7.d	binutils: integer overflow leads to heap-based buffer overflow in objdump	1
S-DEMO-MON02	IV_35.7.d	blktrace: buffer overflow in the dev_map_read function in btt/devmap.c	1
S-DEMO-NOD01	IV_35.7.d	Kernel: KVM: leak of uninitialized stack contents to guest	1
S-DEMO-NOD01	IV_35.7.d	Kernel: page cache side channel attacks	1
S-DEMO-NOD01	IV_35.7.d	Kernel: tcp: excessive resource consumption while processing SACK blocks allows remote denial of service	1
S-DEMO-NOD01	IV_35.7.d	Kernel: tcp: integer overflow while processing SACK blocks allows remote denial of service	1
S-DEMO-NOD01	IV_35.7.d	Kernel: vhost_net: infinite loop while receiving packets leads to DoS	1
S-DEMO-NOD01	IV_35.7.d	ROHNP: Key Extraction Side Channel in Multiple Crypto Libraries	1
S-DEMO-NOD01	IV_35.7.d	binutils: NULL pointer dereference in work_stuff_copy_to_from in cplus-dem.c.	1
S-DEMO-NOD01	IV_35.7.d	binutils: Stack Exhaustion in the demangling functions provided by libiberty	1
S-DEMO-NOD01	IV_35.7.d	binutils: integer overflow leads to heap-based buffer overflow in objdump	1
S-DEMO-NOD01	IV_35.7.d	blktrace: buffer overflow in the dev_map_read function in btt/devmap.c	1
S-DEMO-NOD02	IV_35.7.d	Kernel: KVM: leak of uninitialized stack contents to guest	1
S-DEMO-NOD02	IV_35.7.d	Kernel: page cache side channel attacks	1
S-DEMO-NOD02	IV_35.7.d	Kernel: tcp: excessive resource consumption while processing SACK blocks allows remote denial of service	1
S-DEMO-NOD02	IV_35.7.d	Kernel: tcp: integer overflow while processing SACK blocks allows remote denial of service	1
S-DEMO-NOD02	IV_35.7.d	Kernel: vhost_net: infinite loop while receiving packets leads to DoS	1
S-DEMO-NOD02	IV_35.7.d	ROHNP: Key Extraction Side Channel in Multiple Crypto Libraries	1
S-DEMO-NOD02	IV_35.7.d	binutils: NULL pointer dereference in work_stuff_copy_to_from in cplus-dem.c.	1
S-DEMO-NOD02	IV_35.7.d	binutils: Stack Exhaustion in the demangling functions provided by libiberty	1
S-DEMO-NOD02	IV_35.7.d	binutils: integer overflow leads to heap-based buffer overflow in objdump	1
S-DEMO-NOD02	IV_35.7.d	blktrace: buffer overflow in the dev_map_read function in btt/devmap.c	1
S-DEMO-NOD03	IV_35.7.d	Kernel: KVM: leak of uninitialized stack contents to guest	1
S-DEMO-NOD03	IV_35.7.d	Kernel: page cache side channel attacks	1
S-DEMO-NOD03	IV_35.7.d	Kernel: tcp: excessive resource consumption while processing SACK blocks allows remote denial of service	1
S-DEMO-NOD03	IV_35.7.d	Kernel: tcp: integer overflow while processing SACK blocks allows remote denial of service	1
S-DEMO-NOD03	IV_35.7.d	Kernel: vhost_net: infinite loop while receiving packets leads to DoS	1