FY23Q3 Report

logs goes 4 months back

2023-05-03

Contents

Other **11**

IROH

lead

Guillaume Buisson [25]

ctia [5]

- Fixed Riemann ES configuration #1360
- Allow setting `allow_partial_search_results` in ES queries #1359
- Bump CTIM to 1.3.6 #1355
- Note Entity API changes #1342

between 3 and 4 months old

- CTIM Note entity Support #1330

iroh [16]

- Initial Incident Response Design Draft #7398
- Fix Target enrichment feature flag check #7740

- Bump clj-momo to 0.4.0 #7723
- Update Orchestration Workflow Event fixtures #7677
- Observe-Targets route Enhancements #7668
- Temporary implementation of observe-targets in the Relay module #7656
- Revert ”Enrich WebService route”
- Revert ”Initial WebService for testing”
- Initial WebService for testing
- Enrich WebService route
- Additional Note/Event sample data #7654
- Support the Note Entity in Private Intel #7605
- Mitre and Risk Score based Incidents Review #6990
- Properly define the OpenAPI metadata for the Enrich API #7532
- Unhide Swagger UI Responses #7529
- Updated Note designs #7508

tenzin-config [4]

- Add the SXO clients to the High Impact allowed sources #876

between 3 and 4 months old

- CTIA Note Entity setup #836
- Disable the Kafka Event Hook for Private Intel #835
- Double the rate limit of the dcloud organization #824

data

Mario Aquino [30]

iroh [17]

- Add audiences to client #7812
- OrgTokenProviderService #7731
- Handle additional variation on mitre-attack source_name #7755
- Match on mitre-attack as source_name to find variations #7754
- Remove high impact severity checking #7580
- Iterate over all orgs for threat hunt execution #7601
- Check authorization header #7597
- Fix test broken by missing auth header #7588
- Use mk-int-request-context for calls that may go to modules #7587
- Improve logging for risk score asset resolution #7581
- Update CTIM to align w version used by CTIA #7576
- Reduce threat hunt ctia investigate module timeouts #7527
- Error handling around risk score calculation attempt #7512

between 3 and 4 months old

- Replace unsupported trojan source detector #7481
- Service interface tech-debt #7475
- One iroh-async session queue for all tasks #7472
- CTIM v1.2.0 #7459

tenzin-config [13]

- Enable config for incident enrichment #880
- Removes AWS Auth credentials no longer needed by queue-monitor #867
- Update async worker count for new server specs #861
- AWS Credentials for CloudWatch interaction #842
- Remove configs to allow threat hunting for all orgs #853
- Make all incidents imported via Swagger UI high impact #847
- Remove iroh-investigate and iroh-incident configs #837

between 3 and 4 months old

- Use correct urls for PROD iroh #832

- Updates sessions-config for iroh-investigate and iroh-incident #826
- iroh-queue-monitor config update #820
- Increases number of threat hunt orgs #812
- Redis for iroh-async #815
- Adds config for iroh-async deployment group

Guillaume Erétéo [16]

ctia [6]

- add total-hits headers to metric responses #1363
- add tactics/techniques to incident search filters #1356
- Incident score schema check #1353
- Relationships: add target_ref and source_ref as enumerable field #1354

between 3 and 4 months old

- verdict fix #1333
- add techniques to enumerable fields #1331

iroh [5]

- introduce aggregation in crud store #7734
- Add Scott to CODEOWNERS #7782
- first stats #7765
- Incident summary design #7704
- threat hunt status incident status Open #7709

tenzin-config [5]

- Activate scoring in TEST and PROD for 1.116 #851
- Add PCTIA as high impact by default #849

between 3 and 4 months old

- update incident mappings #822
- IROH Swagger UI to high impact sources #830
- prepare actor migration #814

Ambrose Bonnaire-Sergeant [11]

ctia [7]

- Push sighting store’s coercion pattern into def-es-store #1361
- Remove log4j #1347
- Fix bulk relationships between transient asset mappings/fields #1343
- Filter by scores test #1341
- Scores dynamic mapping #1340
- Don’t mix user params with internal extensions #1339

between 3 and 4 months old

- Sort on incident score #1327

iroh [4]

- new incident scores format #7578
- Strip ctia keys #7521

between 3 and 4 months old

- Improve stubservice error messages #7478
- Prep Mia for incident scoring impl #7397

integrations

Matthieu Sprunck [32]

iroh [17]

- E7469: Event API extension design #7462
- Implements OR, AND, NOT boolean combinators for ElasticSearch #7752
- Add a dedicated IROH Auth configuration to Swagger #7738
- Remote: Return an error when tiles/data is not supported #7732
- Remove support for access token in Swagger UI #7729
- Remote: IROH Proxy handler should not be called in case of errors #7717
- Add missing dependency to int-web-service #7712
- Configures ModuleRecords with a map #7690
- Bump to CTIM 1.3.7 #7696
- Create High Impact incident event #7679
- Bump to CTIM 1.3.5 #7642
- Add new High Impact Incident event types #7606
- Bump to CTIM 1.3.4 #7626
- Bump to CTIM 1.3.3 #7616
- Allow settings prefixed by custom_ to be derived in proxy config #7509

between 3 and 4 months old

- Fix client credentials auth for CrowdStrike integration #7502
- Add API Key auth type to the Relay module #7488

tenzin-config [15]

- Revert ”Revert ”Remove support for access token in Swagger UI (#868)” (#871)” #874
- Allow SXO internal hosts for webhook calls #872
- Revert ”Remove support for access token in Swagger UI (#868)” #871
- Remove invalid module configuration keys #870
- Remove support for access token in Swagger UI #868
- Remove one-click-module services from iroh application #865
- Change the IROH modules configuration format #864
- Change Orbital URL in TEST #848
- Remove the tiles APIs from the Orbital module record #845
- Add CrowdStrike proxy configuration #841

between 3 and 4 months old

- Fix SentinelOne module record conf #834
- Support of IROH Proxy for SentinelOne #828
- Revert connection manager changes in PROD (2nd attempt) #827
- Revert changes in PROD and reduce nb of threads in INT and TEST #825
- Increase the number of threads used by the connection manager of the Relay module #823

Kirill Chernyshov [11]

ctia [2]

- Exception handling for bundle export #1351

between 3 and 4 months old

- Default ”no-pagination” for feed #1336

iroh [9]

- Fix configuration option for event signer #7777
- Add signer options for EventService #7776
- Simplify kafka-producer integration test #7769
- Send event from EventService to kafka topic #7552
- Return promise after sending event to kafka #7556
- IROH-crypto lib #7544
- KafkaProducerService #7524

- Introduce iroh-kafka library #7505

between 3 and 4 months old

- Remove Onyx and Aeron services #7489

Shafiq [5]

iroh [4]

- Add create-event HTTP API #7557
- Add search endpoint for iroh-events #7528
- Add integration test-case for iroh-events search #7513

between 3 and 4 months old

- Separate event-handlers from EventNotifierService #7437

tenzin-config [1]

- Configure internal-event-web-service #844

auth

Olivier Barbeau [23]

iroh [22]

- fix http status code #7838
- Rework of the script `check-changelog-update-time` #7658
- RBAC: additional XDR tests #7634
- GitHub Actions: do test coverage only once #7607
- Increase Java Heap size for code coverage - Github Actions workflow #7585
- add workdir for the check #7573
- disable test #7566
- Fail build if html not updated #7559
- RBAC: enable the new XDR role 'Security Analyst Tier 2' #7545
- Issue 7538 refactor of role retrieval #7540
- automated 'revert role' operation with test #7537
- RBAC: Retrocompatibility of the Provisioning API #7507

between 3 and 4 months old

- Refactor around `ifn-pred` #7491
- set job timeouts to 90 minutes #7506
- set job timeouts to 60 minutes #7504
- Test coverage v2 #7498
- wait for hook to be finished before testing #7497
- Add test coverage report to the Iroh GitHub Actions workflow #7453
- RBAC for Org Access Request #7465
- Issue 7333 rbac invitation service #7454
- RBAC: new XDR tests for login and oauth-clients #7418
- Issue 7413 move steps out of setup job #7414

tenzin-config [1]

- sets the `:xdr-roles` feature flag in INT and TEST #840

(Yogsototh) [5]

xdr-provisioning [5]

- Improve help regarding setting env vars
- Improve the command line parsing
- rename script to .sh
- Add onboarding of DI and CSC
- Initial provisioning Script

bartuka [15]

iroh [13]

- [IROH Auth] introducing `TimeService` in `AuthService` #7806
- [IROH Auth] allow only `iroh-core.time` in oauth2.core ns #7793
- [IROH Auth] - Update IROH Web middleware to build short JWTs with profile data #7671
- [IROH Auth] - update `check-refresh-token` function #7669
- [IROH Auth] - Update Design docs for Short JWT Epic #7670
- [IROH Auth] `/profile/permissions` endpoint #7562
- Patch `compojure-api` to allow endpoints with string-keys (without keywordize the request `:body`) #7574
- [IROH Auth] Include route `/profile/scopes` #7553
- [IROH Auth] - Store Short JWTs #7476

between 3 and 4 months old

- [IROH Auth] refactor `gen-short-tokens` to avoid code duplication #7485
- Allow wildcard login origin in TEST env #7474
- [IROH Auth] Generate Short JWT tokens #7450
- [IROH Auth] Short JWT design #7436

tenzin [1] between 3 and 4 months old

- Update GPG Wanderson Ferreira #2648

tenzin-config [1]

- add postgres and redis-cache store for IROH Auth JWTs #839

Yann Esposito [44]

ctia [1]

- bump snakeyaml to address CVE-2022-38751 #1346

iroh [30]

- Add a missing option to disable default configs #7805
- Add a script to init tokens without login in #7794
- Fix schema for Response #7804
- Add support to onboard a single app #7796
- Add a role instrospection route to help the UI and other clients #7785
- Fix scopes declaration for execute-workflow route #7799
- Fix a Swagger bug due to schema name conflict #7790
- Web api search improvements #7728
- add profile and notification to ao-jwt #7726
- Tk store combinator search queries (AND, OR, NOT) #7691
- Fix a case where the body is `nil` #7685
- Add xdr-instance-id field to the orgs #7707
- PIAM: Provisioning onboard endpoint #7659
- Add ff scope script #7680
- added a script to add feature-flag scopes from command line #7676
- prefer to use client from DB than client from config #7672
- Align scopes to SXO behaviour #7673
- fix lein start #7663
- PIAM provisioning no idp-mapping for create user #7655
- Default bootstrap & config #6868
- Add Entitlements to Orgs #7631
- Remove yaml to supported format for profile API #7632
- Fix a flaky test in either_test.clj #7610
- Role Matrix representation in the code. #7583
- fix some wording only for admin users view #7579
- Improve User login logs situation #7555
- Added a composable redis.nix #7535

between 3 and 4 months old

- Fix template rendering during invite confirmation #7480
- Display virtual users in the batch get users #7473
- Add the UI session logout into IROH-Auth #7431

tenzin [2]

- use iroh.main for all nodes types #2862
- Update iroh.job.jinja #2861

tenzin-config [6]

- fix missing iroh-async web-services #884
- align iroh and iroh-async confs #883
- Add CSC onboarding URLs #875
- fix provisioning service #863
- PIAM config change (+ boostrap cleanup) #677
- add perf.orbital.threatgrid.com to allowed login origin #854

xdr-provisioning [5]

- Improve help regarding setting env vars
- Improve the command line parsing
- rename script to .sh
- Add onboarding of DI and CSC
- Initial provisioning Script

iroh-ops

Patrick Patat [19]

iroh-ops [18]

- Merge pull request #69 from advthreat/riemann-asg
- Merge pull request #66 from advthreat/pg-cname
- Merge pull request #65 from advthreat/minor-fix
- Merge pull request #64 from advthreat/vector-docker
- Merge pull request #63 from advthreat/asg-refresh
- Merge pull request #61 from advthreat/auto-deploy
- Merge pull request #60 from advthreat/webex-notif
- Merge pull request #57 from advthreat/qualys
- Merge pull request #56 from advthreat/dynamodb_backup
- Merge pull request #55 from advthreat/iroh-queue
- Merge pull request #52 from advthreat/nomad-job
- Merge pull request #54 from advthreat/vault-stats
- Merge pull request #48 from advthreat/vault-pki
- Merge pull request #47 from advthreat/nomad-docker-config

between 3 and 4 months old

- Merge pull request #41 from advthreat/codebuild-fix
- Merge pull request #40 from advthreat/ansible-codebuild
- Merge pull request #37 from advthreat/fix-host
- Merge pull request #35 from advthreat/instances_route53

tenzin [1]

- allows iroh-ops dev platform to access redis #2755

Jerome Schneider [81]

iroh-ops [24]

- render s3 artefacts generic and create a releases bucket

- datadog: improve logging
- add vector support for os logging
- tf peering: don't peering public subnets
- Add Datadog agent on all instances and specific setup for Nomad and Consul

between 3 and 4 months old

- vpnator: remove cloudtrail support for the moment
- ansible: migrate jerschne on master
- iam_lambda_ec2_route53: re-add rights on EC2
- improve iam management and adapt Ansible for it
- tfw: manage correctly workspaces
- switch jerschne on ansible master
- Create a new env and manage terraform workspaces
- dev: cleaning configuration
- only one s3 bucket and dynamodb table per account for tfstates
- Ansible: add Mitogen to improve performances (issue #26)
- requirements.txt: add missing dependencies
- vim: add a vimrc example
- scripts/tfw: fixed json debugging message and exit message when it failed
- README is a markdown file
- README.md: fix path
- Migrate iroh-ops TF to Terraform Wrapper (tfw)
- Add a Terraform Wrapper (tfw) that improve Terraform var files
- ansible add a quick readme and a requirements.txt
- TF: add kafka support

tenzin [57]

- Upgrade TF AWS provider
- iroh-async: resize ASG and add downscaling support
- iroh: add iroh signer certificates
- ASG: Drain Nomad nodes before terminating instances
- PROD AP: allows iroh-queue-monitor to put metric in Cloudwatch
- PROD EU: allows iroh-queue-monitor to put metric in Cloudwatch
- PROD US: allows iroh-queue-monitor to put metric in Cloudwatch
- STAGE: allows iroh-queue-monitor to put metric in Cloudwatch
- TEST: allows iroh-queue-monitor to put metric in Cloudwatch
- INT: allows iroh-queue-monitor to put metric in Cloudwatch
- Terraform: configure vault provider
- iroh-async: resize instances and memory usage
- PROD EU: Conure add IAM policy
- PROD APJC: Conure add IAM policy
- PROD NAM: Conure add IAM policy
- STAGE: add Conure support
- TEST: add new Conure IAM role
- INT: add new Conure IAM role
- iroh allows iroh-internal.*.iroh.site domains
- add private-ctia-update-index-state on TEST,STAGE and PROD
- STAGE: add iroh-internal support
- PROD US: add iroh-internal support
- PROD EU: add iroh-internal support
- PROD APJC: add iroh-internal support
- TEST: add iroh-internal support
- INT: add iroh-internal support
- RDS PostgreSQL: force SSL connections by default
- add private-ctia-update-index-state job to update ES index mapping
- Iroh Async use custom metrics to scale
- remove iroh-tooling
- iroh-admin INT: revert breaking instance change
- Caddy private: allow es-metrics for iroh-ops
- allows iroh-ops dev platform to access to private caddy

- PostgreSQL Conure change instances for PROD and TEST
- add Conure RDS PostgreSQL on PROD and TEST
- PROD EU: destroy iroh-investigate and iroh-incident
- PROD APJC: destroy iroh-incident and iroh-investigate
- PROD NAM: remove iroh-incident and iroh-investigate
- TEST: destroy iroh-incident and iroh-investigate
- improve
- iroh-async: add downscaling!
- INT/TEST: fixed iroh-admin conf to allow iroh-queue-monitor
- INT: new RDS PostgreSQL for Conure
- INT: remove iroh-incident and iroh-investigate

between 3 and 4 months old

- Nomad jobs: fix MaxParallel when auto scaling is enabled!
- iroh job: change the grace period from 120s to 180s
- iroh-queue-monitor: migrate it on full https and allow access from private rp
- elasticache: change creation timeout
- add dedicated Elasticache Redis for iroh-async
- PROD APJC: add iroh-async support
- PROD EU: add iroh-async support
- PROD US: add iroh-async support
- TEST: add iroh-async support
- add a new iroh-async to replace iroh-investigate and iroh-incident
- iroh-admin nomad job: extend grace delay and add one more status check
- prod US: this PR allows tier3 engineers to manage SES suppression list
- allow iroh-tooling to access to RDS PostgreSQL

Other

Other

krishna Ganugapenta [32]

tenzin [31]

- Mia Lehrer(milhrer) gpg key updated #2725
- Securex-news decommission from tenzin #2876
- ASG size bumped to negate excessive CPU useage #2869
- updated SG rules count for iroh-front-end #2866
- IAM policy to access cloudtrail logs s3 bucket #2840
- Fixing asea modules not in sync with AWS infra #2828
- logstash-cloudtrail versions updated in jobs.sls #2812
- IROH_ASYNC asg capacity increase #2813
- Logstash-cloudtrail filter settings have modified #2808
- Asea services tf modules removed from TEST to sync with AWS infra #2800
- tenzin-config files updated to intelligence app #2779
- Fixing logstash config file permission issue #2765
- Added read and write permission to logstash.yml #2763
- prestart task added to prevent permissions error #2762
- Added a new set variable for logstash-cloudtrail #2760
- Fixing logstash-cloudtrail nomad job config temp #2759
- Added a missing template for logstash-cloudtrail #2757
- Logstash-cloudtrail job to collect logs #2756
- XDR decommission from nomad cluster #2684
- SQS queue url fixed for logstash-cloudtrail nomad job #2710
- SQS queue url has got updated to logstash-cloudtrail job #2709
- filebeat and beats configuration updated #2707

between 3 and 4 months old

- Removal of accesskey/secret key from logstash-cloudtrail job #2702
- Added vault policy to oss nodes to fix logstash-cloudtrail nomad job issue #2700

- Caddy port lable fix for logstash-cloudtrail job #2698
- Logstash job to retrieve cloudtrail logs from S3 #2696
- Enabled securex-ui-incidents for PROD #2650
- XDR shell app PROD config added #2624
- Conure DB access policy updated #2627
- xdr-apps configuration removed form caddy public #2649
- Caddy Path based routing changes reverted #2623

tenzin-config [1]

- Securex-news removal from tenzin and tenzin-config #869

Tancredi Orlando [1]

easy-purescript-nix [1]

- purs-tidy: 0.9.0 -> 0.9.2

milehrer [15]

iroh-engine [15]

- move forward if no new targets or asset
- prepare for 0.15.4
- decouple first asset check from asset enrichment
- change ->instant to parse
- write asset-enrich pipeline v1
- Prepare for v0.14.6
- update iroh service-wrapper to expect resolve-latest
- add resolve-latest-assets iroh protocol and endpoint

between 3 and 4 months old

- prepare for v0.14.5
- the less we talk about this, the better
- prepare for version 0.14.4
- make data in enrichment bundles align with real life
- prepare for 0.14.3
- remove deprecated trojansource step from github workflow
- remove transient id generation from assets as DI now does it instead

Joel Holdbrooks [2]

iroh-engine [2]

- Merge pull request #1373 from advthreat/noprompt-patch-1
- Update unit_test.yml

Michael Whitley [3]

response [3]

- Update access-request.md
- Update access-request.md
- Update access-request.md

Sofiia Mykytiuk [43]

tenzin [43]

- Update VPNator in TEST, STAGE and PROD #2932
- Update STAGE docs S3 bucket #2938
- Update VPNator lambda functions in INT #2929
- Update min capacity for ASG in backup regions #2917
- Update readme in terraform folders for backup regions #2896
- Saltstack changes for backup regions #2822

- ROAdmin role for STAGE and PROD #2909
- Update saml in terraform to sync with AWS STAGE and PROD accounts #2910
- ROAdmin role for INT #2903
- Add nodes to ES-metrics cluster in EU #2905
- Remove Data VPNator from PROD #2868
- Terraform changes for backup regions #2882
- Remove modules needed for S3 batch operations #2884
- Disable replication for es-metrics #2850
- Update infrastructure diagram with second VPN #2871
- Remove data-vpnator from INT #2855
- PKI update for backup regions #2842
- Update vpnator script for new OPS setup #2817
- Fix module deletition #2825
- Remove cleaner lambda setup from INT, TEST #2823
- Module to setup new vpnator for OPS VPN in INT #2816
- Modules to setup VPNator for OPS VPN in PROD #2814
- BCP: Update readme with bastion info #2456
- Terraform modules update for TEST backup region #2796
- New PROD VPNator setup for non-ops VPN setup #2748
- Remove not needed permissions for kms-ssm in STAGE #2733
- Changing KMS key in Vault unseal config in STAGE #2732
- Adding permissions to kms-vault key #2712
- Remove permissions for kms-ssm from hashistack policy INT and TEST #2719
- Terraform modules update for TEST backup region #2724
- Changing unseal configuration for Vault in INT #2718
- Permissions for kms-vault key in INT and STAGE #2706
- KMS vault key material for INT and STAGE #2705
- New kms-vault key material #2711

between 3 and 4 months old

- Permissions for new kms-vault key in TEST backup region #2695
- Fix permissions for kms-vault key #2692
- Changing kms key in autounseal Vault config for TEST #2680
- Update README.md #2686
- Update salt to read datadog api key from SSM #2679
- Adding permissions for new kms-vault key for hashistack nodes in TEST env #2670
- Adding permissions for datadog ssm parameter #2663
- Comment not needed references #2656
- KMS Vault key #2668

Will Lorand [1]

iroh [1]

- Update summary.org #7603

Dmytro Budko [5]

tenzin [5]

- SXOPS-630 Invalidate a CloudFront cache for INT/TEST after push changes #2897
- SXOPS-191 Terraform: Bring INT and Test into sync with AWS (DOCS INT/TEST) #2889
- SXOPS-616 DataDog agent not able to collect metrics (SLM) from ES #2878
- SXOPS-539 EC2 Keypair rotation for INT and TEST #2787
- SXOPS-539 Offboard Vadym Kiz #2784

Cisco Boz [1]

tenzin [1]

- Replace Threat Response -> XDR for 502 pages on caddy-* public & private #2934

Patrick Patat [72]

iroh-ops [71]

- install and config riemann on asg
- add riemann & reimann_telemetry servers
- add vault token for ansible
- add rds pg cname and bump tf min version to 1.4
- install vector after all (due to app log deps)
- add vector config for docker with nomad
- add auto instance refresh
- disable notready service add the end of ansible run
- remove unattended-upgrades pkg and ignore qualys server
- setup a lambda that run ansible nomad-jobs when a new app version is pushed to s3
- override nomad jobs version with versions.json from s3 bucket artefacts (needed for auto deployement)
- add codebuild fail notification via webex
- simplify sg rule and rename a boolean var
- add doc for qualys setup
- add qualys instances and extends customasation of instances, asg & sgs
- create an aws backup vault and plan for dynamodb backup
- create redis-async.iroh.dev.sh cname to tenzin's redis
- add add iroh-queue-monitor, add http check for nomad jobs
- config vault telemetry to send data to datadog
- add role nomad-jobs with exemple job iroh & hello, add related caddy config for private rp
- add python-nomad to manage job, add dogstatsd as volume & add metadata from docker
- add iroh-ro vault policy
- add vault ca to ssm, put vault ca on caddy vm & update nomad config for vault and docker
- create custom modules for vault and aws private acm & configure vault internal pki
- allow vault servers to query aws private acm
- add docker registry and app_server role for docker registry use
- move docker repo conf to linux base & update nomad config
- add .yml to group_vars files

between 3 and 4 months old

- create one codebuild job per env
- change codebuild default env var to " and fix missing env var in user_data
- create codebuild ansible-run and replace user_data local ansible with codebuild trigger
- push new admin key in user admin authorized keys
- fix hostname config
- add lambda to create/delete ec2 dns record on start and terminate
- centralize apt config & set hostname and prompt
- configure vault server & add caddy vault config
- refactor route53 lb cnames creation
- upgrade vault instances config
- split iam in mutliple file and add iam for vault instances
- add dynamodb for vault
- add CODEOWNERS file
- remove openvpn push dns (useless with iroh.sh)
- upgrade tf and ansible for caddy https with letsencrypt
- upgrade dns config with iroh.sh & iroh.services
- secure all comunications between consul nomad and rps
- do not redeploy instances on ami upgrade
- refactor pki
- fix: encode in base64 ssm parameters
- Revert "temporaly disable encrypt communication for nomad and consul"
- pki for internal certs
- use ansible-pull in user_data to config vm at first boot
- use t4.small instead of t4.nano
- add linux users config
- fix: add hashicorp apt in vaul role
- upgrade for private rp
- add role and playbook for caddy private rp

- move hashicorp's apt config to role nomad & consul (do need it on all vms)
- add bastion and openvpn role, playbook and group_vars
- temporaly disable encrypt communication for nomad and consul
- replace _ with - in node name (need to be dns compatible)
- add python3-boto3 to linux_base_pkgs
- temporary allow everything from vpn
- disable source_dest_check for vpn and add bastion dns name
- upgrade for vpn server
- ansible typos and code style
- refactoring asgs & security groups
- refactor terraform asgs
- use boolean value instead of strings, add tags in tasks and other minor fixes
- improve ansible.cfg, remove debug, fix unbound config
- add load_balancer, app_server private_rp, remove caps from ressource names
- ansible bootstrap

tenzin [1]

- allows iroh-ops dev platform to access rds

Yurii Ivanisenko [12]

tenzin [11]

- Add muhammad imran (muhammim) gpg key #2899
- Give Muhammad Imran (muhammim) SSH access #2898
- removed walkme-ci tf module files and vpn users #2841
- removed all saltstack entries with user vilakkak #2818
- removed TF module CloudWatch-lambda-sca-whitelist-testing #2804
- added diagrams for CTR_AWS and TAC-portal #2717
- align with INT lambda settings for Thousendeyes WL and TEST R53 recor… #2715

between 3 and 4 months old

- fix CSP directives for visibility.amp in APJC and EU regions #2689
- fixed tab instead of spaces in caddy.yaml NAM #2681
- Caddy public job - added templates for TAC certificates #2674
- Added configs for TAC portal prod #2666

tenzin-config [1] between 3 and 4 months old

- Added config.json for Tactical-portal in PROD regions #817

Robert Levy [5]

iroh [5]

- fix dev-resources config to use the correct key signer-ops instead of signer #7778
- Add registered trademark to MITRE tile title #7775
- Incidents' Detection Sources Tile #7725
- top-targeted assets tile for control center (ctia investigate module) #7689
- MITRE Attack incidents tile #7523

Mia [36]

iroh [22]

- Update risk score docs to include overview of enrich-targets process #7773
- log asset retrieval failure #7743
- Separate risk score engine calls #7742
- log bundle #7737
- Flag observe targets #7697
- remove verbose logs from risk score calculation #7618
- FIXME temp log bundle-import-payload #7609
- handle explicit nil cases for asset value #7604

- Correct describe assets #7600
- adjust logging #7596
- Resolve latest asset log params #7594
- add asset:read scope to token used for engine-service #7571
- Iroh engine latest assets #7554
- Update bundle import #7542
- Fix risk score bundle import #7534
- fix a typo in engine config introduce default consistent with engine #7525
- Fix risk score auth #7517
- Fix risk score auth #7516
- Fix risk score auth with tests this time #7515
- add auth token to bundle export header in risk score #7514

between 3 and 4 months old

- implement final risk score #7486
- 7342 preliminary risk score #7460

iroh-engine [13]

- Merge pull request #1385 from advthreat/v0.15.4-rc
- Merge pull request #1384 from advthreat/separate-add-assets-and-enrich-targets
- Merge pull request #1371 from advthreat/testy-tests
- Merge pull request #1367 from advthreat/v0.14.6-rc
- Merge pull request #1366 from advthreat/add-resolve-latest-assets

between 3 and 4 months old

- Merge pull request #1365 from advthreat/v0.14.5-rc
- Merge pull request #1364 from advthreat/change-test-again
- Merge branch 'main' into change-test-again
- Merge pull request #1363 from advthreat/v0.14.4-rc
- Merge pull request #1362 from advthreat/calculate-preliminary-risk-score
- Merge pull request #1360 from advthreat/v0.14.3-rc
- Merge pull request #1359 from advthreat/remove-trojansource
- Merge pull request #1358 from advthreat/remove-transient-ids

tenzin-config [1] between 3 and 4 months old

- flip feature flag in INT for score-based incident enrichment #833

Devin Walters [5]

iroh-engine [5]

- Prepare 0.15.2
- Coerce to instant after reading as ZDT
- Assert sightings
- Let up
- Use investigable-observables, promises delivered, add verdict

Vadym Kiz [3]

tenzin [3]

- SXOPS-361 GitHub self-hosted runners for SecureX UI monorepo #2635
- Datadog: enable slm_stats #2778
- SSH access - jbusboom #2738

Ag Ibragimov [8]

iroh [4]

- Unassigned Incidents Tile should show relative time #7824
- Control center: Navigate to Incidents page from tile #7760
- Control Center – Detection Sources Tile: Fixes query parenthesizing #7759

- API work for unassigned incidents #7682

tenzin-config [4]

- adds :xdr-site-url #885
- adds detection sources config for PROD #881
- additional client_id for incident sources #877
- adds incident sources: test, int #873

Justin Woo [2]

easy-purescript-nix [2]

- Merge pull request #219 from turlando/purs-tidy-0.9.2
- Merge pull request #218 from paluh/master

dependabot[bot] [0]

Sam Waggoner [4]

ctia [1] between 3 and 4 months old

- threatgrid/ctim/#381 Migrate actor 1.2.0 #1323

tenzin-config [3]

- Add hydrant es-metrics configs for events.
- Fix hydrant-talos-ta-blog misnamed http-options.
- advthreat/hydrant#721 update talos blog http-options.

II [9]

iroh [7]

- Issue 7455 - Minor cleanup from XDR tiles merge #7695
- 6963 implements one-click module wrapper endpoint #7315
- Issue 7647 AMP observe targets #7661
- Issue 7647 - IObserveTargetModule protocol #7651
- Ao shortcut use unique names #7627
- Ao docs formatting fixes #7625
- Issue 7550 ao workflow exec shortcut #7617

tenzin-config [2]

- Adds one-click service to bootstrap.cfg files #862

between 3 and 4 months old

- Tac portal PROD login origins #821

Eric Gierach [10]

iroh [3]

- Fix attack graph simplification #7747
- latest simplification logic (edges not considered) #7662
- update notable events to match what the Engine client is producing for CTR #7614

iroh-engine [7]

- Merge pull request #1387 from advthreat/v0.15.5-rc
- Prepare for 0.15.5 release.
- Merge pull request #1386 from advthreat/enrich-all-targets
- Fix typo in log
- Merge pull request #1370 from advthreat/dependabot/npm_and_yarn/webpack-5.76.0
- Merge branch 'main' into dependabot/npm_and_yarn/webpack-5.76.0

- Merge pull request #1368 from advthreat/dependabot/npm_and_yarn/xmldom/xmldom-and-mountebank-0.8.4

Adam Sayer [26]

tenzin [25]

- webexbox fix on saltmaster #2937
- increase ES storage iops/throughput #2927
- Vercel CICD accept 409 and watch http state
- Add Vercel CI/CD to Saltmaster #2920
- Update hydrant container version #2891
- snort filename fix #2890
- Update hydrant container to 1.36 in INT #2888
- remove jq verify usage #2885
- Fix - Extract Talos Snort Rule files for Importer #2880
- github runner salt and terraform #2875
- update securex-ui in INT for latest NVM profiles #2873
- Route53 Module refactor #2851
- Revert "SXOPS-361 GitHub self-hosted runners for SecureX UI monorepo (#2635)" #2859
- github-runner ASG #2852
- Update r53 module to allow geolocation #2844
- Cloud9 ami APJC EU #2803
- Cloud9 AMI to NAM #2792
- Bash to replace ES instances #2777
- Upgrade 6th gen ec2 and cloud9 AMI for TEST #2775
- Int cloud9 ami refresh #2768
- Allow instance refresh on ASG module #2766
- VPC peer TEST-STAGE for qa-macos instance #2734
- Stage salt #2716

between 3 and 4 months old

- Allow ingress from IROH to ES private storage #2652
- Allow ingress from IROH to es private storage INT #2630

tenzin-config [1]

- Stage env configs #785

Tomasz Rybarczyk [1]

easy-purescript-nix [1]

- purs: 0.15.7 -> 0.15.8

Chris Duane [2]

response [2]

- Update access-request.md
- Create security-event.md

[9]

iroh [7]

- Issue 7455 - Minor cleanup from XDR tiles merge #7695
- 6963 implements one-click module wrapper endpoint #7315
- Issue 7647 AMP observe targets #7661
- Issue 7647 - IObserveTargetModule protocol #7651
- Ao shortcut use unique names #7627
- Ao docs formatting fixes #7625
- Issue 7550 ao workflow exec shortcut #7617

tenzin-config [2]

- Adds one-click service to bootstrap.cfg files #862

between 3 and 4 months old

- Tac portal PROD login origins #821

John Jardine [30]

tenzin [30]

- Update SW versions, sort changes to the top #2864
- Add instances to handle new 3rd party integrations #2870
- Add capacity in OSS to support logstash-cloudtrail #2865
- Terraform edits to deconflict some values and make more generic #2853
- Create S3 Bucket, user, group, policy #2839
- Update integrations-crowdstrike to 1.0.2 in all regions #2833
- Move all Hydrant jobs to v1.35 (adds coas support) #2826
- Bash defaults: Remove TMOUT, assign set -o vi & dir #2829
- Check single certificate #2830
- Align hydrant jobs on 4 minute multiples. #2821
- Updated ssh keypairs for EU NAM and APJC #2791
- SXOPS-529: SSH Default configuration changes #2774
- Check if integrations-healthcheck is working. #2772
- Update sumram.gpg
- Make script outputs comparable by using same sort order #2761
- SXOPS-435: Add hydrant-talos-coas fixes for other regions #2751
- Quote cron entry to prevent YAML interpolation #2750
- Default Jason Busboom to absent to prevent global access #2743
- Updated rev-proxy for securex-ui-automate.test.iroh.site #2744
- Added gpg key for Atul Anand
- SXOPS-491 Add securex ui automate support for TEST #2729
- Need to add securex-ui-automate.int.iroh.site to ACME #2723
- SXOPS-491 Add securex ui automate support #2722

between 3 and 4 months old

- Fix comment, fix error file content check #2683
- Backport v1.112 fixes to master #2682
- Initial commit #2671
- Add error handling to cert check #2651
- Initial Vercel Postman API #2633
- INT: Merge Consul overrides into jobs.sls #2646
- SXOPS-412: Trend Micro XDR Integration Relay INT and TEST #2617

Michael Pendergrass [4]

iroh [4]

- Engine 0.15.5 #7768
- add more attribute relation types #7660
- More graph changes #7643
- add graph output to incident summary #7549

Scott McLeod [4]

iroh [4]

- Improve performance of IncidentReportService #7745
- Add filters to Incident Report #7727
- Add test to verify paging #7564
- Use search_after paging for incident report (#7461) #7539

Matthieu Sprunck [3]

ctia [3]

- Bump CTIM to 1.3.7 #1357
- Bump to CTIM 1.3.5 #1349
- Bump to CTIM 1.3.4 #1345

Jerome Schneider [10]

iroh-ops [9]

- Merge pull request #68 from advthreat/split-releases-artefacts
- Merge pull request #51 from advthreat/logging-vector
- Merge pull request #46 from advthreat/datadog

between 3 and 4 months old

- Merge pull request #42 from advthreat/vpnator-rm-cloudtrail
- Merge pull request #36 from advthreat/stricter-iam
- Merge pull request #34 from advthreat/fix-tfw
- Merge pull request #16 from advthreat/tfw-fixes
- Merge pull request #13 from advthreat/tf-wrapper
- Merge pull request #12 from advthreat/ansible

tenzin [1] between 3 and 4 months old

- iroh(-async): improve memory management to avoid memory cgroup oom #2693

t2sw [1]

iroh [1]

- modify get-tiles and get-tiles-data endpoints for xdr query parameter #7757

bswanson [81]

iroh [10]

- Engine version bump. #7730
- Asset correlation #7708
- READY FOR REVIEW: observe-targets to iroh engine. #7683
- Fix empty source breaking schema. #7687
- BUG FIX: events were pulled from wrong key. #7678
- Add Assets to Summary and Events incident endpoints #7666

between 3 and 4 months old

- Add Eric and Mia to codeowners. #7501
- Add extra fields to summary events #7482
- Add optional keys owner and groups to :incident-id/events schema. #7449
- Allow port key in the private-intel service context #7435

iroh-engine [68]

- Merge pull request #1383 from advthreat/v0.15.3-rc
- Update changelog.
- Prepare for 0.15.3 release
- Merge pull request #1381 from advthreat/proper-no-op
- Merge branch 'main' into proper-no-op
- Merge pull request #1382 from advthreat/codeowners
- Add folks to codeowners, remove our previous humans.
- Update release to remove unused project.clj
- Cleanup tests.
- Update tests to reflect passthrough behavior.
- failing tests, but no-op.
- Merge pull request #1380 from advthreat/v0.15.2-rc

- Merge pull request #1379 from advthreat/superstitious-p
- Merge pull request #1378 from advthreat/v0.15.1-rc
- Release v0.15.1.
- Merge pull request #1377 from advthreat/remove-original-sightings
- Don't print 100s of sightings :D
- Add logging.
- Remove CTIM dependency.
- Data for you and data for me
- Cabinet of curiosities be gone.
- Datums test.
- new asset responses.
- Check no-op case for assets-for-new-targets.
- Add assets and asset mappings.
- Remove fake test that described itself as real.
- Use add-latest-asset-info from enrich ns.
- Add failing observe-target-observables-test.
- Do not pass back the relationships or sightings from the original bundle.
- Merge pull request #1374 from advthreat/v0.15.0-rc
- Release candidate 0.15.0
- Merge pull request #1372 from advthreat/asset-enrich
- Merge branch 'main' into asset-enrich
- Only need to wrap around exception.
- Magic sauce for cljs vs clj.
- Add test for ->instant.
- Fix let<.
- promesify everything.
- PR feedback, add p/let.
- PR feedback.
- map observable keys (this shouldn't matter, but for consistency and safety sake.)
- Refactor exists? because it's a function.
- Update src/iroh/engine/asset/enrich.cljc
- Fix IrohServiceWrapper call.
- move time fns into time ns.
- A bit more function now.
- IT LIVESSSS.
- Add emit_observe_targets_enrich.js
- Wiring through observable call.
- mountebank.
- Getting farther through the pipeline.
- Resolve linter errors.
- more promises for us.
- cleanup nested whens.
- Try to call targets.
- it puts the promise on the code.
- Smaller functions.
- Clean up more test ns.
- Cleanup tests.
- Merge branch 'main' into asset-enrich
- Move logic into previous function.
- Add resolve latest mountebank test.
- Some unit tests.
- prepare for the sightening.
- extract targets from enriched response.
- Break out a couple more small functions.
- Implement some small helper functions.
- Pull in used sighting ns and reference observable var.

tenzin-config [3]

- Add config for prod and fix test typo. #846

between 3 and 4 months old

- Add iroh base url to conure config. #829
- Add necessary conure config. #811

Pawan Bahuguna [31]

tenzin [31]

- Sxops 191 - custom_response_body #2933
- Added health check header #2921
- Added Health check header to crowdstrike for testing #2916
- Increased the Max size to 6 #2908
- Updated the version to 7.0.7 to sync with AWS #2907
- SXOPS-621 - Enable IAM Access Advisor in all envs #2894
- Removed Event Processor Role #2881
- SXOPS 191 Update TEST VPC Peering #2879
- Changed version to 7.0.5, already present in aws #2877
- Updated desired capacity, min and max size #2874
- SXOPS-490 Docker version health check #2837
- Added CU, IR, KP, SY #2854
- Added artifacts and XDR to ordered_cache_behavior - Already in AWS #2848
- SXOPS-191-Updated VPC peering connection #2835
- Added docker container version check #2815
- SAML sync with AWS #2824
- enabled intelligence in prod #2807
- SXOPS-535 Micro Frontend Ribbon #2806
- int-iroh-registration-ui User is already present in AWS #2801
- Removed CloudWatch-CSIRT.tf #2788
- updated the asg_max_size to 6 #2781
- Added instance refresh #2780
- Enabling watchdog check on Crowdstrike #2773
- SXOPS-490 Add/Update 3rd Party Integrations health checks #2767
- Added TLS - automate MFE #2753
- PROD automate MFE #2752
- [SXOPS-497] Create 3rd Party Integrations for Cybereason & Crowdstrike (INT/TEST) #2747
- Added dbudko pabahugu to VPN list #2728
- Sxops 484 onboard dmytro dbudko #2727
- SXOPS-476 Decom Nomad task securex-ui-incidents from Tenzin #2699

between 3 and 4 months old

- enable prod #2662

Trent Boyd [2]

tenzin-config [2]

- chore: add https dev urls to xdr projects #886
- feat: add configs for securex-ui-intelligence job #852

Devin Walters [12]

tenzin [7]

- Set tmpdir to /local for conure task #2930
- Mount datadog socket in conure task #2922
- Remove Conure access to IROH RDS instance #2742

between 3 and 4 months old

- Capture the rest of a log message as 'message_text' for clj stack logs #2660
- Grok pattern which captures message for the clj stack #2658
- Add RMI server hostname #2640
- Include configuration for hikari monitoring via JMX #2639

tenzin-config [5]

- Specify JWK per environment #866
- Update conure username in prod environments #860
- Update conure db username in TEST #856
- Update conure configuration #843
- Test out dedicated conure postgres instance #838

Martin Bruchanov [20]

tenzin [20]

- Adding data nodes to lower file system utilization #2940
- Adding vercel deploy to sudo for consul #2936
- Increasing number of data nodes to the current state #2935
- Security groups for OPS VPN in INT #2924
- Added CLI parameters for ES administration tools #2915
- Removing salt references for terminated OPs instance #2900
- Updated contacts of EDF team #2895
- Fixed JSON validation for IROH query #2887
- Fixed correct hostname and SSM keys #2893
- OPS OpenVPN salt deployment #2883
- Renaming data-openvpn to ops-openvpn #2845
- Increasing edf-reporting and iops-reporting memory allocation #2838
- Added list of Consul UI hostnames #2789
- Tool for quick SSH to Consul leader #2785
- Cleaning up intel2x hostname #2654
- Second VPN server for Non-OPS access #2735
- Fixed duplicated uid in user profile #2740

between 3 and 4 months old

- NAM ElasticSearch clean up: DNS, S3 bucket for snapshots #2697
- Updating hostnames, fixed error with missing authentication #2637
- Tranfer of existing roles from one ES cluter to another #2634

Michael Simonson [3]

tenzin [2]

- Adds input buckets for non-int envs #2863
- SXOPs-hydrant-talos-coa-importer #2741

tenzin-config [1]

- Issue SXOPs-562: Hydrant Manual Removal Importer #859

John Jardine [5]

tenzin [4]

- Revert ”Move all Hydrant jobs to v1.35 (adds coas support)”
- Revert ”Include STAGE in hydrant container version update”
- Include STAGE in hydrant container version update
- Move all Hydrant jobs to v1.35 (adds coas support)

tenzin-config [1]

- Importer was missing the config files #850

Gayan Jayasundara [7]

tenzin [7]

- Bump crowdstrike and SentinalOne - Ian requested #2904
- Bump crowdstrike into 1.0.2a - Bug fix from Ian #2846

- SXOPS-512 Bump crowdstrike and sentinelone versions #2802

between 3 and 4 months old

- Migrate securex-ui-incidents from Nomad to Vercel - non-prod - DNS #2691
- securex-ui-control-center - non-prod vercel #2690
- Update cyberprotect integration to latest (2.0.6) #2673
- Redirect XDR int to Vercel #2667