Internal Release Notes

Version: 3.6.0

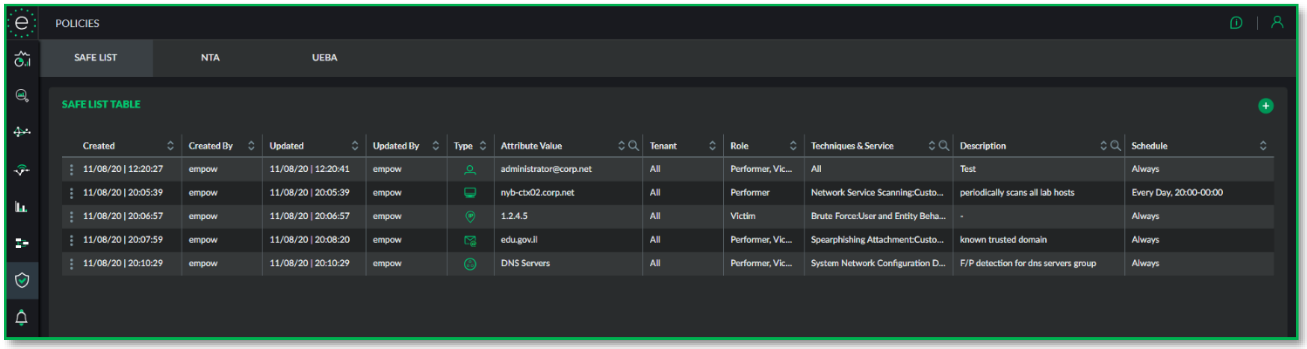
Version Bundle

SST	ELK
3.6.0	7.9.2

New Features

1. Safe List Enhancements

- **Safe List Improvements**
  - Features: Add the ability to add entity entry to the safe list via click from Attack, Top Entities and Entity Card views.
    - Once clicking on 'Add to Safe List' button, a new setting window will open populated with the entity's name.
    - Added the ability to add user identity to the safe list.
    - Added the ability to add description to safe list policy.
    - Settings of safe-list according to the entity's role, victim or performer, or both.
    - All changes made in safe-list policies will be recorded in the entity journal.
    - Any entity which already exists in the safe list will have link to "see safe list".
  - Value:
    - Improved UX during the user's investigation flow
    - A more intuitive whitelisting settings based on the role of the subject entity, agnostic to the underlined security technology the generates the leads.
    - Adding granularity of user identity to allow user based safe listing



SAFE LIST TABLE

Created	Created By	Updated	Updated By	Type	Attribute Value	Tenant	Role	Techniques & Service	Description	Schedule
11/08/20 | 12:20:27	empow	11/08/20 | 12:20:41	empow	👤	administrator@corp.net	All	Performer, Vic...	All	Test	Always
11/08/20 | 20:05:39	empow	11/08/20 | 20:05:39	empow	🖥	nyb-ctx02.corp.net	All	Performer	Network Service Scanning:Custo...	periodically scans all lab hosts	Every Day, 20:00-00:00
11/08/20 | 20:06:57	empow	11/08/20 | 20:06:57	empow	📍	1.2.4.5	All	Victim	Brute Force:User and Entity Beha...	-	Always
11/08/20 | 20:07:59	empow	11/08/20 | 20:08:20	empow	✉	edu.gov.il	All	Performer, Vic...	Spearphishing Attachment:Custo...	known trusted domain	Always
11/08/20 | 20:10:29	empow	11/08/20 | 20:10:29	empow	◎	DNS Servers	All	Performer, Vic...	System Network Configuration D...	F/P detection for dns servers group	Always

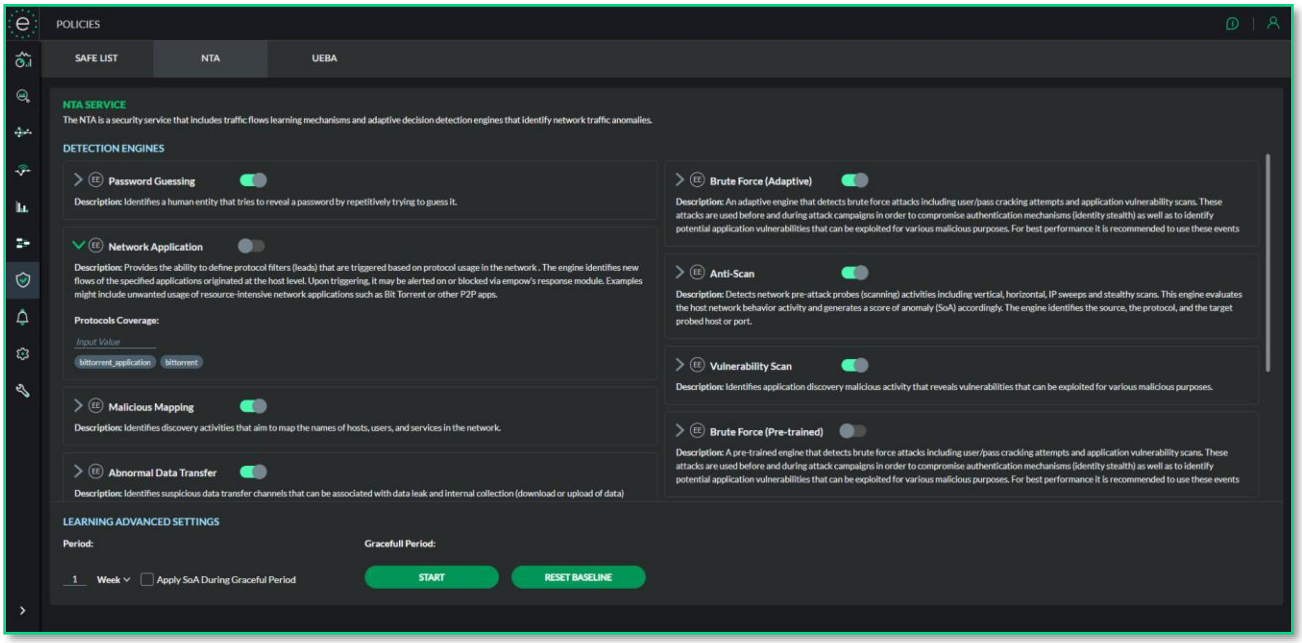
- **Safe List Migration Notes**
    - Feature: convert the old safe list from source and destination roles to victim and performer roles, and allow safe listing a technique across multiple security services.
    - Value: Easy migration from old safe list setting to the new victim/performer role-based one
    - Deployment Notes:
        - IP type support both range and subnet mask, while valid mask is between 16 to 32.
        - Any entry of "IP-RANGE" type will be documented in a JSON form in the description column.
        - Post upgrade, the solution architect must validate the white list policies (e.g., description field will hold old schedule details if were configured)
        - Any entry of "URL" type will be permanently deleted as this type is not supported.
        - Any entry value of "HOST" type will be empty if the host name does not exist anymore in the "IDENTITIES" table and will not be considered in the whitelist logic.

2. Triage Detection

- **Added Triage Scoring**
    - Feature: The risk-chain correlation engine can now identify “Triage-event” and increase the entity’s score and associated attack risk level accordingly.
      “Triage event” is defined as different data sources that report the same attack technique (and in some exceptions the same attack stage) on the same victim or performer entity.
    - Triage-event automation counter was added to the existing C-Level report.
    - Value: Automate events validation and prioritization according to detected triage-events indications.

3. NTA & UEBA Configurations

- **New NTA and UEBA configuration sections**
  - Features:
    - The NTA and UEBA services policy configurations are now supported in a new dedicated configurations screen. The new policy configurations are available within new POLICIES module in the global menu.
    - The new configurations allow:
      - To enable expert engine for forensics only without consuming its events by a security application
      - Excluding specific protocol of an active expert engine both from attacks and forensics (in previous version could only be excluded from attacks).
    - Any changes made requires APPLY, to send updated configuration to the relevant UEBA or NTA services.
  - Value: provide independent configurations between forensics and security application policy of NTA and UEBA service.



The NTA is a security service that includes traffic flows learning mechanisms and adaptive decision detection engines that identify network traffic anomalies.

Password Guessing

Description: Identifies a human entity that tries to reveal a password by repetitively trying to guess it.

Network Application

Description: Provides the ability to define protocol filters (leads) that are triggered based on protocol usage in the network . The engine identifies new flows of the specified applications originated at the host level. Upon triggering, it may be alerted on or blocked via empow's response module. Examples might include unwanted usage of resource-intensive network applications such as Bit Torrent or other P2P apps.

Protocols Coverage: Input Value

bittorrent_application bittorrent

Malicious Mapping

Description: Identifies discovery activities that aim to map the names of hosts, users, and services in the network.

Abnormal Data Transfer

Description: Identifies suspicious data transfer channels that can be associated with data leak and internal collection (download or upload of data)

Brute Force (Adaptive)

Description: An adaptive engine that detects brute force attacks including user/pass cracking attempts and application vulnerability scans. These attacks are used before and during attack campaigns in order to compromise authentication mechanisms (identity stealth) as well as to identify potential application vulnerabilities that can be exploited for various malicious purposes. For best performance it is recommended to use these events

Anti-Scan

Description: Detects network pre-attack probes (scanning) activities including vertical, horizontal, IP sweeps and stealthy scans. This engine evaluates the host network behavior activity and generates a score of anomaly (SoA) accordingly. The engine identifies the source, the protocol, and the target probed host or port.

Vulnerability Scan

Description: Identifies application discovery malicious activity that reveals vulnerabilities that can be exploited for various malicious purposes.

Brute Force (Pre-trained)

Description: A pre-trained engine that detects brute force attacks including user/pass cracking attempts and application vulnerability scans. These attacks are used before and during attack campaigns in order to compromise authentication mechanisms (identity stealth) as well as to identify potential application vulnerabilities that can be exploited for various malicious purposes. For best performance it is recommended to use these events

Period: 1 Week ☐ Apply SoA During Graceful Period

Gracefull Period:

4. Configurable Retention Policy

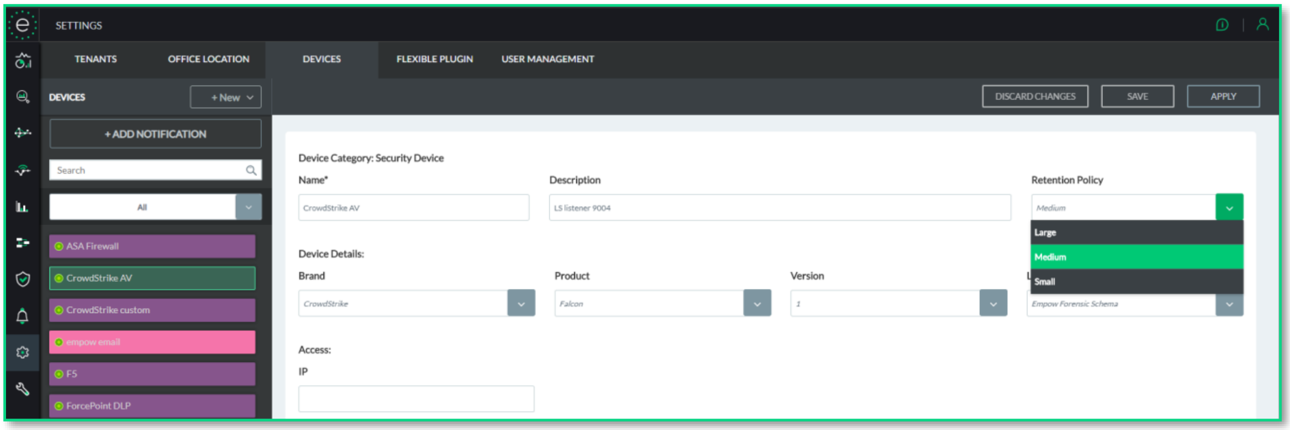
- **Add the Ability to Set Retention Policy per Data Source**

  Feature: It is now possible to choose the desired level of logs retention per security device through the i-SIEM setting device form. There are 3 possible periods, each set with a default retention time:

    - Small → 30 days
    - Medium → 90 days
    - Large → 13 month

  The user can easily change it through Kibana Stack Management in the ILM Policy.

    - Value: Maintaining a more efficient data storage policy according to the type of logs. Thus, provide optimization of both the data search performance, as well as the storage cost.



Device Category: Security Device

Name*: CrowdStrike AV

Description: LS listener 9004

Retention Policy: Medium

Device Details:

Brand: CrowdStrike

Product: Falcon

Version: 1

Empow Forensic Schema

Access:

IP:

5. Log Ingestion Service Improvements

- **Added several performance improvements:**
    - The system was set with a maximum of 10 identity enrichments per entity (e.g., up to 10 users on host, up to 10 hosts on user)
    - System was set with a max time of 15sec for enrichment. If the enrichment is not completed in 15 seconds, then the log will be further processed without an identity enrichment. This new behavior improves the ingestion performance as well.
- **Extended enrichment sources:**
    - We extended the types of logs from which the system learns user-host relationships (Additional types: DLP and EDR logs).
    - Migration Notes:
        - user-host relationships learning will start from scratch based on logs received from the upgrade time and go.
        - Any log used as learning source of user-host relationships will populate forensics fields “empow.isDstLogin” or “empow.isSrcLogin” with value true.

Enhancements

- **Forensic Schema Version 1.5 –** this schema version includes new cloud and services related fields to support clous-based integrations such as Microsoft Azure, AWS and more. To see the full list of fields please refer to the user guide.
- **Enable Elastic Security Features –** it is possible to set all Elastic Security features to be enabled by default as part of the installation.
  New installation requires to run the following command as part of the installation after setting up the dockers: `./elk_security_configuration.sh`. Make sure to change the default password through Kibana User Management.
  Upgrade of existing setup shall follow a manual procedure.
- **Forensics Writer Service –** improvements made for stabilizing the forensics writer and have better tracking of logs in processing. Part of the changes include:
  - In case Kafka or Elasticsearch is down for some reason the forensics writer will still be up and after they up again, the forensics writer will continue write logs to elastic index.
  - Statistics about logs that are collected and stored in empow-metric index.
    Elasticsearch cluster is now using sniffer, which is enabled by default in the forensics.yml `(FORENSIC_SNIFFER_ENABLE=true)`. This configuration is relevant both for multi or single node deployment.
- **UEBA Logs Routing –** until today logs that intended to empow UEBA engine was forced to have observer.service UEBA although log originated by different observer type such as VPN, IAM, OS, etc.
  From now on logs routing to UEBA service happens according to other fields values:
  - event.action – 'Login' or 'User Locked' or 'Logout'
  - event.outcome – 'Success' or 'Fail'

  It means that the service breakdown and data source status radar in the main dashboard will reflect the actual data source type segmentation.
- **Data Source Alerts Resolution** – The data sources alert resolution was changed to be based on the combination of vendor and product (previously vendor-product-hostname). This change allows to unify multiple devices (e.g., multiple product's sensors) under the same alert.

Bug Fixes

1. **Entity Card Time Filter (ESB-6490) –** customize time filter in the top entities wasn't function, although filter displayed as selected on the screen, data wasn't really refreshing.

2. **Mismatch between i-SIEM dashboard and Kibana (ESB-6513) –** events count in Kibana wasn't match the counts per data source in i-SIEM main dashboard. Issue cause was to writing to empow-forensics index directly to Elasticsearch without passing through i-SIEM ingest service.
   Migration Notes: Post upgrade to version 3.6.0, there will be temporary (7 days) inconsistency between "DATA SOURCE STATUS" widget and "TOTAL EVENTS" element. The first will represent the data starting from the upgrade point, and the second will represent data including information pre-upgrade.

3. **Email based events written to forensics with missing fields (ESB-6511) –** in previous version although the parsed log received with multiple ECS fields, once source or destination include user.email value, major part of the received fields wasn't written to forensics. Issue was fixed as part of ingest service improvements.

4. **Error popup occurs in failure to refresh dashboard data (ESB-6512) –** in previous versions failure in refreshing dashboard data popped an error window. Issue fixed and in case of failure the problematic widget will show a "An error has occurred", without prompting the user for response.

5. **Technique duplication in attack table view (ESB-6559) –** in previous versions, any attack segment that included more that single event of the same technique, displayed the technique name multiple times as the number of detected occurrences. Thus, technique column width became huge and caused an inconvenient user experience with horizontal scroll when trying to drill into the event details. Issue is solved.

6. **Username that is not FQDN dropped (ESB-6528) –** in previous versions any log received with username value in source or destination side that wasn't FQDN, was written to the forensics without the username value received. From now on ingest supports usernames without domain names, which is mainly important for cloud integration where user account isn't always associated with domain.

7. **Same event considered in attack both as detection and investigation evidence (ESB-6597) –** same event that exist in an attack story can potentially trigger history investigation and bring itself as an investigation evidence. Thus, system might have determined wrong confidence score for an entity. Issue is fixed and same event does not allow to be consumed both as detection and as investigation evidence.

Known Limitations

1. **Entities API –** Currently there is an option to filter entities by review status in get-entities call. This request will have performance impact on the platform resources and therefore do not use this filter for now.

2. **Investigation Events –** Currently any investigation event of a technique which is reversed (e.g. Webroot phishing for example) won't be displayed right in the leads details page and therefore the dynamic search in events won't find any result. **Workaround:** Edit the query: switch between the values in the source and destination fields for the following observer types and techniques: Reputation observer type, Drive-by attack technique.

3. **Investigation Lead Details** – Investigation phase leads, in the leads table, show "UNKNOWN" value in the source or destination columns, and the vendor field is set N/A. The correct information is available in the vendor event details page.

4. **Authentication Required when Navigating from i-SIEM to Kibana** – in environment with Elastic Security enabled, the link from i-SIEM to Kibana won't work seamlessly as it was until today. The user will be requested to enter the credential to login to Kibana.

Upgrade

This version supports direct upgrade from version 3.5.X, any upgrade from lower version must go through all the upgrade of minor versions between. The following steps shall be performed to complete the upgrade:

1. Before the upgrade:
    a. Backup existing configuration
    b. Pull latest swarm-installation
    c. Run the following to pull the latest plugins automation script
    `./plugin_resources.sh to get latest plugins resources`
2. Post upgrade:
    a. Manually remove the rollover of old forensics ILM
        i. Go to Kibana > Stack Management > Index Lifecycle Policies
        ii. Choose empow-forensicsv1.3 policy
        iii. Disable rollover
        iv. Save changes
    b. Validate Safe List entries created successfully as expected:
        i. In cases which the description is populated with pre upgrade entry information, manually validate that the new entry created as expected.