BLUE CANYON TECHNOLOGIES

Automation Menu

AlienVault Central API
- Take in AlienVault Central alarms

AlienVault OTX
- Enrich an IP, hostname, url, hash or domain
- Identify the reputation of an IP address

Anomali ThreatStream
- Fetch recent threat intelligence
- Search for an indicator by name
- Create an incident
- Import an indicator into ThreatStream, to be approved in the UI
- Add an indicator to an incident

AutoFocus API
- Take in AutoFocus samples as alerts

AWS
- Retrieve all Guard Duty Findings, report as an alert.

BMC Remedy
- Retrieval of existing incident info
- Creation of incidents
- Updating incidents
- Resolving incidents
- Closing incidents

CA Service
- Create, update, and delete change order tickets in CA Service Desk

Carbon Black Defense
- Get the status of a device on Cb Defense
- Change the policy on a device on an instance of Cb Defense
- Find all the events, according to a set of filters, on Cb Defense
- Add/remove a rule from a policy on Cb Defense

Carbon Black Protection
- Get computer info using CB Protection
- Get CB Protection user info
- Get a specific file instance's info looking through all the computers on the CB Protection instance
- Assign a policy to a computer being managed under CB Protection

Changegear
- Create a service request, provided field information
  Retrieve an incident, provided a ticket ID

Check Point Intelligence Feeds
- Check for the presence of an indicator in an intel feed
- Add IOCs of the following types to an Intelligence Feed:
  - MD5 Hash
  - URL
  - IP(v4)
  - IP Range (v4)
  - Mail-subject header values
  - Mail-from header values
  - Mail-to header values
  - Mail-cc header values
  - Mail-reply-to header values
- Manage the Intelligence Feed by culling old entries at regular intervals

CheckPoint SandBlast API
- Submit a file to CheckPoint SandBlast for sandboxing
- Retrieve the result of sandboxing

Cisco AMP
- Pull new file activity in as alerts
- Move computers between groups
- Add or remove file hashes from blacklists

Cisco ATA
Tickets created via the `ata_create_ticket.py` script will contain the fact data contained within the alert the action was fired on. Tickets updated via the `ata_update_ticket.py` script are updated with information that will be placed in the `Notes` field of the ticket, and can have their status changed (optionally) to *Resolved* or *In Progress.*

Cisco ESA
- Block Emails and Senders (add items to content dictionaries and sender groups)
- Unblock Emails and Senders (remove items from content dictionaries and sender groups)
- Query Emails and Senders (Determine if items exist within content dictionaries or sender groups)
- provide secure and authenticated access to the Email Security appliance reports and report counters

BLUE CANYON TECHNOLOGIES

Automation Menu

Cisco FirePower
- Create IP address networkobjects, and add them to network groups
- Create deployment requests for managed devices

Cisco Threat Response Integration
- Get data about an indicator

Cisco Umbrella
- Check if a domain is present on the block list.
- Add, update or delete a domain from the block list.

Crowdstrike Falcon Host
- Pull new detections as alerts
- Update the status of existing detections

Crowdstrike Intel
- Query for specific indicators

Crowdstrike Query
- Upload IOCs for detection
- Get a list of devices an IOC has run on
- Get details about an uploaded IOC
- Get details about a device

Cylance
- Add a hash to the Cylance Global Quarantine List or the Global Safe List
- Remove a hash from the Cylance Global Quarantine List or the Global Safe List
- Retrieve device information given the device's name
- Retrieve threat details given the threat's sha256 hash
- Update a device's given policy
- Retrieve new threats from the Cylance API, and report them as alerts
- Retrieve new detections from the Cylance API, and report them as alerts

DNS Lookup
- Automatically retrieve DNS lookup information on suspected malicious IPs/Hosts for further enrichment

Facebook Threat Exchange
- Search for information on the Source IP of a SIEM alarm or other alert

File Hashing
- Hash a potentially malicious file and submit the hash to a Threat Intelligence tool to enrich further
- Hash a known malicious file and add the hash to an EDRtool

Forcepoint Integration
- Create and remove Forcepoint categories
- Adding URLs and IP addresses to an existing category
- Removing URLs and IP addresses from an existing category
- Querying categories for URLs and IPaddresses

Graylog API
- Take in Graylog messages from a stream as alerts

Guardicore
- Retrieve Guardicore incidents given optional filters that are ANDed together in the query: tag (multiple tags can be a comma separated), severity (low, me- dium, high), and incident group. Incidents are then reported as an alert.

HP Service Manager Integration
- Retrieve a master list of incidents
- Retrieve information from a specific incident
- Create a new incident with a title and description
- Update an incident
- Resolve an incident
- Close an incident

Hybrid Analysis Falcon
- Retrieve a master list of incidents
- Retrieve information from a specific incident
- Create a new incident with a title and description
- Update an incident
- Resolve an incident
- Close an incident

IBM QRadar
- Pull QRadar SIEM Offenses (that have yet to be ingested) as alerts.
- Filter which QRadar SIEM Offenses should be submitted.
- Optionally give ingested Offenses a "Closed" status on QRadar SIEM.
- Mark any QRadar SIEM Offense as "Closed" with a Closing Reason ID and an optional closing note.
- Add/Check/Purge/Delete items from Qradar Reference Sets.

BLUE CANYON TECHNOLOGIES

Automation Menu

IBM X-Force
- Fetch the reputation of an IP address via IBM X-Force and submit it.

JASK
- Ingest Insights/Alerts
- Assign an alert to a JASK user
- Search JASK for an indicator

JIRA Integration
- Create a new JIRA issue given a project key, summary, description, and issue type.
- Update an existing JIRA issue - a comment is required along with the issue's ID. In addition, one can change the issue's assignee, the issue's status, and the resolution of the issue if need be.
- Query the API for the issue's present status.

JoeSandbox File Analysis
- Submit a file for analysis
- Lookup a previously run analysis
- Fetch file analysis results

LogRhythm Integration
- Ingest alarms from LogRyhthm for further enrichment and tracking

McAfee DXL
- Fetch system details
- Fetch available tags
- Wakeup a system
- Apply or clear tags from a system
- Set a system's health indicator
- Set or remove reputations
- Get file refs
- Query projections

Microsoft Graph API
- Get email messages service
- Get security alerts service
- Enable or disable user
- Get info about a user
- Get a user's group membership
- Add a user to a group or remove a user from a group

MISP Integration
- Search for an indicator

Netskope
- Retrieve Netskope alerts, report each alert as an alert (see the alert object below).

PAN External Dynamic Lists
- Add a URL, domain name, or URL to block list.
- Remove a URL, domain name, or URL from block list.
- Determine if an indicator exists in a block list.

PAN External Dynamic Lists
- Add domains, IP addresses, and URLs to PAN blocking lists

PAN Firewall
- Get interface descriptions
- Block IPs
- Search URLs

PAN WildFire
- Submit a local/remote file or a link to PAN WildFire for analysis.
- Submit a file to PAN WildFire.
- Get the PAN WildFire verdict for the file/link or send the PAN WildFire report over to an alert.

Phishing Analysis
- Extract information from an e-mail
- Extract urls from pdf and Word files
- DNS, SPF, Spam Score, and Blacklist lookup

Proofpoint TAP
- Receive alerts for links clicked in emails tracked by Proofpoint that are potentially malicious
- Receive alerts for messages delivered to a user's inbox that are potentially malicious
- Selectively receive alerts for any combination of the spam, malware, phishing, and imposter message categories defined in Proofpoint
- Decode a rewritten URL

Qualys
- Retrieve information on scans and detections for a host

BLUE CANYON TECHNOLOGIES

Automation Menu

Rapid7
- Retrieve asset information
- Initiate a scan on an asset within a site
- Get a scan's current status
- Update IDR investigation status

Recorded Future
- Query for a domain, url, ip, hash, or malware name

RSA NetWitness
- Pull new RSA NetWitness incidents
- Download PCAPfiles from decoders

SentinelOne Integration
- Retrieve information about a SentinelOne managed device (agent)
- Move agents between groups
- Get SentinelOne's reputation and classification data for a file hash
- Add a file hash to blacklist
- Remove a file hash from blacklist

Service Now
- Manage items in the incidents table from
- Receive status updates on incidents, having configured the appropriate SNow objects
- Perform CMDBLookups on assets

Shodan Integration
- Query an IPaddress for Shodan host information
- Forward DNS lookup on a list of hostname(s)
- Reverse DNS lookup on a list of IP address(es)
- Get API and account information

Sophos
- Ingest Events and Alerts from Sophos

Symantec Endpoint Protection
- Get all the group names on an SEPM
- Retrieve information about an SEP managed client.
- Start a quick/full scan on a client.
- Search a computer or group of computers for a specific file hash (SAH256, SHA1, or MD5).
- Move clients between groups.
- Retrieve the status of a scan.

Syslog Integration
- Given a CEF log file, each line will be parsed individually and sent as an alert.

Tanium Patch Integration
- Trigger a patch list deployment to one or more machines managed by Tanium

Tenable Security Center
- Launch scans against specified machines
- Fetch results of scans

Tenable.io
- Fetch information about an asset covered by Tenable.io
- Launch a prepared scan against a Tenable.io asset
- Fetch results of scans
- Fetch vulnerability data

Threat Quotient
- Query indicator records
- Submit a new indicator
- Add an indicator to a watchlist
- Markan indicator as a false positive

ThreatGrid
- Do a ThreatGrid submission search
- Submit a file to ThreatGrid for analysis
- Fetch the results for a ThreatGrid analysis

TruSTAR
- Add indicator to whitelist
- Remove indicator from whitelist
- Search for details about an indicator
- Submit an indicator to TruSTAR
- See the available enclaves in TruSTAR
- Submit a report to specified enclaves or the community

URLScan.io
- Search for an existing submission (via URL)
- Submit a URL
- Retrieve Results of a submission (via GUID)

Automation Menu

Virustotal

- Enrich supported indicators (domains, hashes, ip addresses, urls)
- Submit files from alert attachments
- Submit URLs for analysis by Virustotal

VMware vSphere

- Enrich supported indicators (domains, hashes, ip addresses, urls)
- Submit files from alert attachments
- Submit URLs for analysis by Virustotal

Zoho Desk Integration

- Create a Zoho Desk ticket
- Update any one of a Zoho Deskticket's fields
- Add a comment to a ticket
- Resolve a ticket
- Close a ticket

Zscaler Security Policy Managem ent Integration

- Query URL presence
- Add a URL to a policy list
- Remove a URL from a policy list