Cyber Threat Analytics

On this

The Cyber Threat Analytics app monitors security logs and network flows to detect malware infections (for example, zero day attacks and ransomware), system compromise, lateral movement, pass-the-hash, pass-the-ticket, and other advanced threats. SNYPR ingests data from sources such as firewalls, proxy, VPN, IDS, DNS, endpoints, and Netflow devices to baseline normal behavior and detect malicious patterns such as beaconing; connections to digitally generated domains; robotic behavior; rare executables; and programs, lateral connections, and unusual web activity.

Actionable Security Intelligence

The Securonix platform mines, enriches, and transforms SIEM events from HP ArcSight, IBM Radar, McAfee ESM, Splunk, and others into actionable intelligence on threats against the entire IT environment including critical business applications. Securonix integrates with SIEM products through a direct API connection, syslog, or a database connection where it picks up activity and event data. The platform has connectors leading to HR and identity management systems, bringing in more than 75 standard and custom identity attributes, and pulls in detailed activity and entitlement information for application level deep monitoring from enterprise management systems such as SAP, SharePoint, and EPIC.

Business Impact

- Faster breach detection
- Reduce breach impact
- Comprehensive threat response and investigation
- Lower monitoring and management costs
- Lower compliance costs
- Receive quantified, non-subjective threat and risk reporting

Key Use Cases

- Anomalous program execution (rare process, path, MD5)
- Robotic traffic pattern to a malicious, uncategorized, or suspicious website

- Connections to digitally generated domains
- Unusual DNS queries
- Possible command and control (C&C) activity
- Spike in bytes out to external destinations
- Unusual traffic pattern (application / port)
- Anglr exploit detections
- Rare user agents
- Unusual session duration
- Connections to blacklisted IP or domains
- DDOS / port scan activity
- Abnormal number of failed or redirected requests
- Targeted SPAM / phishing attempts

Key Threat Models

Multiple threat indicators that occur in a pattern and involve similar entities tend to have a much higher risk of being a real threat. Threat Models define these patterns, and combine policies and threat indicators to detect related behavior across multiple data sources to detect threats that might otherwise go unnoticed.

Threat Model Name	Description	Stage	Threat Indicators
LATERAL MOVEMENT DETECTION	This threat model detects possible network lateral movement scenarios which are deployed by attackers to progressively spread through a network as they search for key assets and data	AUTHENTICATION ANOMALY	Account accessing a host never accessed before
			Host enumeration detected
			Use of explicit account credentials across multiple hosts
			Suspicious authentication type/process detected
			Anomalous provisioning activity detected
		SUSPICIOUS USE OF PRIVILEGES	Suspicious escalation of privileges detected
			Anomalous network share objects accessed
		PROCESS ANOMALY	Rare process/MD5 detected

Threat Model Name	Description	Stage	Threat Indicators
COMPROMISED HOST DETECTION	This threat model aims to identify hosts that show signs of infection and compromise by correlating host and network based anomalies on the same entity	OUTBOUND TRAFFIC ANOMALY	Suspicious creation of scheduled tasks
			Suspicious changes to registry setting detected
			Traffic to randomly generated domains
			Traffic to known malicious hosts detected
			Abnormal number of rare domains accessed
			Possible C2 communication detected
			Rare process/MD5 detected
		ENDPOINT ANOMALY	Suspicious port/protocol usage by process detected
			Rare user agent detected
APT DETECTION	This threat model aims to identify stealthy computer network attacks in which a malicious actor gains unauthorized access to a network with an intention to remain undetected for an extended period	RECON	Possible phishing attempt
			Network scanning and enumeration detected
			Circumvention of controls detected
			Traffic to randomly generated domains
		DELIVERY	DHCP traffic anomaly detected
			Traffic to known malicious hosts detected
		EXPLOIT	Activity by terminated/dormant accounts detected
			DNS traffic anomaly detected
			Suspicious authentication type/process detected
			Account accessing a host never accessed before

Threat Model Name	Description	Stage	Threat Indicators
			Landspeed anomaly detected
			Rare process/MD5 detected
			Possible C2 communication detected
		EXECUTE	DNS amplification anomaly
			Covert channel exfiltration detected
		EXFILTRATION	Data egress via network uploads detected
PHISHING	This threat model aims to identify possible phishing attempts to target users within the organization		Detection of targeted/spear phishing campaigns
			Detection of possible spray phishing
			Detection of persistent phishing campaigns – Similar sender from multiple domains
		SUSPICIOUS INBOUND EMAIL	Emails from known blacklisted senders/domains/IP addresses
			Detection of suspicious email attachments
			Traffic to randomly generated domains
			Traffic to known malicious hosts detected
		OUTBOUND TRAFFIC ANOMALY	Abnormal number of rare domains accessed
			Possible C2 communication detected
			Suspicious proxy redirects detected

Threat Model Name	Description	Stage	Threat Indicators
HOST/ACCOUNT ENUMERATION ON LDAP	This threat model aims to identify potential assets or accounts enumeration on the network by malicious entities	PROCESS ANOMALY	Rare process/MD5 detected
			Suspicious creation of scheduled tasks
			Suspicious changes to registry setting detected
		SUSPICIOUS PROCESS EXECUTION	Rare process/MD5 detected
			Use of possible AD enumeration toolsets
			Use of malicious tools and utilities detected
		NETWORK SCANNING	Detection of possible AD account/privilege enumeration
			Detection of LDAP or SMB services enumeration
			Detection of abnormal number of Kerberos service ticket requests
			Detection of port scanning
		AUTHENTICATION ANOMALY	Accounts accessing a host for the first time
			Use of previously unseen accounts on the network
			Abnormal number of failed authentication requests
			Detection of possible password spraying
RECON FOLLOWED BY POTENTIAL EXPLOITATION	This threat model aims to identify successful network reconnaissance attempts followed by indicators of exploit	EXTERNAL SCAN	Port scan from external hosts
			Host enumeration from external hosts
		NETWORK SCANNING	Detection of possible AD account/privilege enumeration
			Detection of LDAP services enumeration

Threat Model Name	Description	Stage	Threat Indicators
			Detection of abnormal number of Kerberos service ticket requests
			Detection of spike in LDAP traffic
			Detection of SMB services enumeration
			Rare process/MD5 detected
		PROCESS ANOMALY	Suspicious creation of scheduled tasks
			Suspicious changes to registry setting detected
			Account accessing a host never accessed before
		NETWORK SCANNING DETECTION	Abnormal number of SMBv1 network activity
			SMBv1 scanning anomaly detection
			Traffic to rare domains
WANNACRY MALWARE DETECTION	This targeted threat model aims to identify Wannacry malware behavior	OUTBOUND TRAFFIC ANOMALY	Traffic to randomly generated domains
			Traffic to known malicious hosts detected
			Traffic to TOR exit nodes
			Rare process/MD5 detected
		PROCESS ANOMALY	Suspicious creation of scheduled tasks
			Suspicious changes to registry setting detected
NETWORK ANOMALY FOLLOWED BY DATA EXFILTRATION	This threat model aims to identify successful network data aggregation attempts followed by signs of data exfiltration	NETWORK SCANNING	Detection of possible AD account/privilege enumeration
			Detection of LDAP services enumeration

Threat Model Name	Description	Stage	Threat Indicators
	outside of the network		
			Detection of abnormal number of Kerberos service ticket requests
			Detection of spike in LDAP traffic
			Detection of SMB services enumeration
			Rare network share object accessed
		NETWORK DRIVE ANOMALY	Abnormal number of network share objects accessed
			Admin object access anomaly
			Abnormal amount of bytes downloaded via SMB Ports
		DATA AGGREGATION	Abnormal amount of bytes downloaded via FTP Ports
			Abnormal amount of bytes transmitted via FTP Ports
		DATA EXFILTRATION VIA NETWORK	Abnormal amount of bytes transmitted via covert channel
			Account accessing a host never accessed before
		NETWORK SCANNING DETECTION	Abnormal number of SMBv1 network activity
			SMBv1 scanning anomaly detection
PETRWRAP/GOLDENEYE/NYETYA MALWARE DETECTION	This targeted threat model aims to identify Petrwrap malware behavior	SUSPICIOUS PRIVILEGED ACTIVITY	Possible privilege escalation
			Unusual IPC Admin share access
			Detection of audit log tampering
			Rare process/MD5 detected
		PROCESS ANOMALY	Suspicious creation of scheduled tasks
			Suspicious changes to registry setting detected

Threat Model Name	Description	Stage	Threat Indicators
BLOODHOUND CRITICAL ATTACK	This threat model aims to identify usage of Bloodhound like utilities that are targeted towards Active Directory enumeration	Malicious Process Detection	Suspicious Process Execution Rare Process Creation
		Network Anomaly	Suspicious application detected Network Scanning and Enumeration Data aggregation over network
		Outbound Anomaly	Possible C2 communication
SAMSAM - GOLDLOWELL RANSOMWARE ATTACK	This targeted threat model aims to identify Samsam malware behavior.	Malicious Process Detected	Suspicious Process Execution Rare process execution
		Network Anomaly	Suspicious Application Detected Network Scanning and Enumeration Data aggregation over network
		Outbound Anomaly	Possible C2 Communication
SPECTRE MELTDOWN ATTACK	This targeted threat model aims to identify Spectre meltdown attack behavior	Suspicious Process Detection	Suspicious process execution Rare process creation
		Possible C2 Communication	Data egress over cloud collaboration Data aggregation over network Possible C2 communication

Supported Datasources by Functionality

The following datasources are recommended to run the applicable use cases in the application:

Functionality	Datasource(s)

Functionality	Datasource(s)
Antivirus / Malware / EDR	Check Point Anti-malware; Checkpoint SmartDefense; Cisco Intrusion Detection System; Cisco SourceFire; Cisco SourceFire FireAMP; Cisco SourceFire Intrusion Sensor; Cybereason Endpoint Sensor; Darktrace;Secureworks iSensor; FireEye EX; FireEye HX; FireEye NX; EnCase Security; McAfee EPO VirusScan; Malwarebytes; Panda Security Endpoint Protection; Qualys; Symantec Endpoint Protection; Trend Micro Deep Discovery Inspector; Trend Micro Deep Security Agent; Trend Micro Deep Security Manager; Trend Micro Control Manager
Email / Email Security (inbound)	Ironport Email Security Appliance; McAfee IronMail Email Gateway; Office 365 Exchange; Proofpoint Email Gateway; SureView Email; Symantec Message Security Gateway; Symantec MessageLabs; Symantec Messaging Security Gateway
Firewall / NGFW / WAF	Akamai Web Application Firewall; Juniper Firewall; Juniper Junos Router; Barracuda Networks Load Balancer; Check Point Firewall; Cisco Adaptive Security Appliance; Fortinet Firewall; Juniper Netscreen Firewall; Juniper SRX Firewall; JunOS Pulse Firewall; McAfee Firewall; McAfee Sidewinder; Microsoft Forefront Threat Management Gateway Firewall; Palo Alto Network Next Generation Firewall; Sonicwall Global Management System; Fortigate UTM; ASM Web Application Firewall; Imperva WAF
Netflow	NETSCOUT nGenius
Web Proxy	Bluecoat Proxy; Cisco ASA Firepower URL; Cisco Ironport Web Security Appliance; Cisco Web Security; Forefront Threat Management Gateway; iboss Proxy; IronPort Web Security Appliance; McAfee Web Gateway; SureView HTTP; Websense Proxy; Zscaler
DLP/ Endpoint	McAfee DLP; ObserveIT; Proofpoint Threat Response™; Digital Guardian; Symantec DLP; Symantec DLP Endpoint; Websense Triton DLP; McAfee nDLP; McAfee Network DLP
IDS/IPS	IBM IDS/IPS; McAfee EPO HIDS/HIP; McAfee Network IPS
TPI	Darktrace TPI;

Note: The examples listed here may not represent a complete list of datasources for these functionalities. See Connectors by Functionality to view the list of connectors by

functionality.

Required Data

SNYPR connectors include built-in parsers that split raw event data into meaningful key-value pairs and map the fields to corresponding attributes in the Securonix event schema. The following fields are required for each functionality to support the use cases for this packaged application:

Data Type	Recommended attributes
Proxy	src-address (IP) Bytes in Bytes Out Action Status Category HttpMethod (GET / POST) Destination IP Destination Host URL Source Port DestPort Username User Agent Transaction refererurl url_query Protocol
Sinkhole	Time Bytes DestinationIP DestinationPort DeviceAddress Number of Flows in Packet Number of Packets TCP Flag TCP Flag Message Description Source Address Source Port Ad_tos

Data Type	Recommended attributes
	protocol
	subnet
	severity
	src_mac
	Class_Name
	Type_Name
	objectname
	Response_Code_Name
	Raw
	DNS_Record_Type
	HostAddress
	dst_ip
	dst_mac
DNS	src_ip
	src_port
	Grid_Master_IP
	Message_Text
	hostname
	application
	domain
	dst_port
	Interface
	Datetime
	UserName
	Protocol
Firewall	DateTime
	Action
	bytes_received
	bytes_sent
	application
	category
	clientip
	protocol
	source_port
	destination_port
	direction
	dst_hostname
	dst_zone
	dest_ip

Data Type	Recommended attributes
IDS/IPS/Endpoint Protection	severity
	session_id
	Transaction
	Accountname
	app:has_known_vulnerability
	app:category
	app:subcategory
	DVS
	DGA Score
	User Agent Score
	ROC Center
	ROC Weight
	Accountname
	Source IP
	Datetime
	Filename
	Filepath
	Macaddress
	Threat description/category
	Protocol
	Threat Label
	Threat Sub Label
	Severity
	ThreatHandled/action/reason
	filehash
	Targetfilename
	Targetfilepath
	CommandLine/Parameters
	Threat name/ virus name
	msg
	dhost
	request
Sysmon	EventID
	Level
	Task
	Opcode
	Keywords
	TimeCreated
	Correlation

Data Type	Recommended attributes
	Channel
	Computer
	Security UserID
	Eventcode
	SourceIp
	SourceHostname
	SourcePort
	Image
	DestinationIp
	DestinationHostname
	DestinationPort
	Protocol
	ProcessGuid
	User
	ProcessId
	SourceImage
	Processname
	Processpath
	Filehash
	ActionTaken
	AlarmClass
	AlarmClearedBy
systrack-rpt_alarm	AlarmStartTime
	AlarmInstance
	AlarmItem
	SystemId
	ACCOUNT_ID
	ApplicationName
	ApplicationPath
	ApplicationFileDate
	ApplicationType
	CommandLine
systrack-rpt_application	ExecutionCount
	FileSize
	LoadTime
	MemoryUsed
	PageFaultCount
	SystemAccount
systrack-rpt_application_faults	ApplicationName

Data Type	Recommended attributes
systrack-rpt_firewall	Count
	FaultAddress
	ModuleName
	SystemId
	FirewallEnabled
	ExceptionsNotAllowed
	ICMPAllowInboundEchoRequest
	ICMPAllowInboundMaskRequest
	ICMPAllowInboundRouterRequest
	ICMPAllowInboundTimestampRequest
	ICMPAllowOutboundDestinationUnreachable
	ICMPAllowOutboundPacketTooBig
	ICMPAllowOutboundSourceQuench
	ICMPAllowOutboundTimeExceeded
	ICMPAllowRedirect
	ProfileType
	RAEnabled
	SystemId
systrack-rpt_firewall_data	Enabled
	ImageFileName
	Name
	RecordType
	ServiceType
	SystemId
systrack-rpt_firewall_ports	Enabled
	Name
	PortNumber
	Protocol
	RecordType
	ServiceNameofPort
	SystemId
systrack-rpt_net_port	FirstFaultTime
	Application
	Protocol
	RemoteAddress
	State
	SystemId
	FQDN
	destinationport

Data Type	Recommended attributes
systrack-rpt_network_interface	DHCPEnabled DNSServers Description IPAddress IPDefaultGateway IPSubnetMask IPwithSubnetMaskApplied MACAddress SystemId
systrack-rpt_software_package_syscomponents	AccountID ApplicationID DescriptionID SystemId
systrack-rpt_web_usage	DateFirstVisited FocusTimeOnPage NumberofTimesVisited PageLoadTime TimeOnPage TimetoLive URL UserName

Key Threat Indicators

Threat Indicators are used to categorize the type of behavior or threat for a policy and can be used across multiple policies for different datasource functionalities. Threat indicators can be chained together into threat models to identify sophisticated attacks across multiple datasources.

Threat Indicator
Abnormal Administrative Share Access Anomaly
Abnormal amount of data exfiltrated over covert channels
Abnormal application load times
Abnormal memory utilized by an application
Abnormal number of account lock out events
Abnormal number of accounts on account creation
Abnormal number of accounts on account lockouts
Abnormal number of accounts on failed authentication attempts
Abnormal number of accounts on RDP auth attempts

Threat Indicator

Abnormal number of accounts on run

Abnormal number of application installation failures

Abnormal number of blocked events for external traffic

Abnormal number of bytes transmitted to storage based websites

Abnormal number of connections to critical ports null scan

Abnormal number of connections to critical ports xmas scan

Abnormal number of connections within a subnet

Abnormal number of device unlock attempts

Abnormal number of discover requests from a client

Abnormal number of DNS zone transfers

Abnormal number of dns zone transfers - Firewall

Abnormal number of events on LDAP port

Abnormal number of failed requests - Firewall

Abnormal number of failed requests to non Alexa domains

Abnormal number of faults for an application

Abnormal number of hosts on account creation

Abnormal number of hosts on account lockouts

Abnormal number of hosts on failed authentication attempts

Abnormal number of hosts on RDP auth attempts

Abnormal number of hosts on run

Abnormal number of ICMP connections

Abnormal number of kerberos pre authentication failures

Abnormal number of NXDOMAIN results for an endpoint

Abnormal number of packets to critical ports

Abnormal number of profile change attempts

Abnormal number of RDP connection attempts

Abnormal number of requests to a DHCP server

Abnormal number of RPC requests

Abnormal number of SSH connection attempts

Abnormal number of SYN packets transmitted

Abnormal number of telnet requests

Securonix Confidential

Abnormal number of UDP connections Fraggle Attack

Abnormal object or network share access attempts

Abnormal volume of DNS Traffic by Single IP

Account accessing a host for the first time

Account added and removed to security group

Account Created and Deleted within a short time

Account Enabled and then Disabled within a short time

Threat Indicator

Account enabled and then disabled within short time

Activity performed by terminated user

Anomalous LDAP enumeration

Anomalous NTP enumeration attempt

Anomalous SNMP enumeration

Anomalous WS Remote Management enumeration

Attempted exfiltration via ICMP

Attempts to Reset Domain Admin Password

Audit Log Tampering

Backdoor account detection

BruteForce - Higher than normal logon failure

Data exfiltration from DNS tunneling

Detect creation of local accounts

Detect cross site scripting attempts

Detect Firewall Getting Disabled

Detect possible sql injection

Detect possible sql injection

Detection directory traversal attempts

Detection of beaconing traffic pattern

Detection of Changes to Firewall Settings

Detection of Domain Trust Additions

Detection of member additions to built-in Windows admin groups

DGA host detected in DNS request

DGA host resolving to multiple IP addresses

DGA host resolving to multiple IP addresses - Firewall

DNS Server(s) not seen before

DNS Server(s) not used by Peers

Domains Resolved to Malicious IPs

Explicit credentials - Account sharing or Password misuse

Fast flux Domains / Dynamic DNS Domains

Firewall - DGA Host Detected

Firewall - Rare Domains Visited

High number of accounts from the same ipaddress for authentication failures or lockout events

High number of accounts from the same ipaddress for successful authentications or run as events

Securonix Confidential

High number of accounts used on a workstation for authentication failures or lockout events

Threat Indicator

High number of accounts used on a workstation for successful authentications or run as events

High Number of bytes transmitted

High number of bytes transmitted over DNS - firewall

High number of hosts accessed for authentication failures or lockout events

High number of hosts accessed for successful authentication events or run as events

High number of hosts accessed while enumerating critical ports

High number of redirected/blocked attempts

High number of run as activity across hosts

High number of server errors

Hosts with disabled AV

Hosts with outdated AV

Interactive Logon by Service Account

Local Account Created

Logon using Explicit Credentials by Rare Process into Rare Account

Logon using Explicit Credentials into Rare Account

Multiple DGA hosts detected for the same endpoint

Multiple DGA hosts detected for the same endpoint - Firewall

Multiple hosts accessed within a subnet

New admin account detected

Non compliant hosts

Outbound DNS requests from internal workstations

Password Reset Anomaly

Possible Account Enumeration

Possible port scan- Firewall

Possible Privilege Enumeration

Possible Privilege Escalation - Account Added and Removed from Security Enabled Groups

Possible Privilege Escalation - Self Escalation

Possible Telnet Scan Detected

Possible use of unauthorized devices - MAC address never seen before

Proxy - DGA Host Detected

Proxy - Rare Domains Visited

Proxy - Rare User Agent Used

Rare application and protocol combination - Firewall

Rare application installation detected

Rare destination port for a process on outbound connections detected

Rare DHCP server accessed

Rare dll process and path combination

Rare dll used by a process - endpoint monitoring

Threat Indicator

Rare DNS domain queried

Rare dns host used - Firewall

Securonix Confidential

Rare DNS hosts detected in the organization

Rare file hash detected across the resource

Rare function used by dll

Rare Geolocation detected by resource

Rare logon process detected for an account

Rare logon type detected for an account

Rare object access attempts

Rare parent process and process creation

Rare path for a application

Rare path of execution detected for outbound traffic

Rare Port Accessed

Rare port and application combination - Firewall

Rare port for application

Rare process creation

Rare process execution detected for outbound traffic

Rare Request Method utilized

Rare User- Agent detected

Rarity in Privilege level for new logon

Rarity in Token Elevation for Process

Registry Modification Attempts

Replay attack detection

Service account interactive logon

Service or Process creation on rare path

SMB or NetBIOS enumeration anomaly

SMB scanning anomaly detection

Spike in Account Creation

Spike in number of run-as activity

Spike in Password Resets

Spike in Remote Logon Attempts

Suspicious exfiltration attempts over known file transfer ports

Suspicious Service or Process creation

Terminated user performing activity

Threat Intel Collision - Firewall Domains Visited

Threat Intel Collision - Firewall Malicious IP

Threat Intel Collision - Proxy Domains Visited

Threat Intel Collision - Proxy Malicious IP

Threat Indicator

Unauthorized VPN usage

Unusual Process For Host Heuristics Anomaly

Use of Regedit

User accessing password hash

WIP- Unusual IPC Administrative Share Access Anomaly