CYBRAICS

Exhibits to nLighten™ V4 User Manual

Current as of 15 March 2021

VERSION CONTROL

Version	Date	Comments	Updated by
1.0	3-8-2021	Initial document	R Rounsavall

TABLE OF CONTENTS

EXHIBIT A: DETECTABLE BEHAVIORS 4

EXHIBIT B: SUPPORTED SERVICES AND DEVICES 14

EXHIBIT A: DETECTABLE BEHAVIORS

Additional analytics are being developed on a continual basis. The column "Data Type" identifies the general type of data that the analytic ingests. For example, "windows" is very specifically "Windows Active Directory", but "URL" could be any data source that provides a full URL (e.g., Palo Alto THREAT logs, Meraki firewall logs, Bluecoat logs, etc.). "Flow" is any type of log that has source and destination IP traffic, the most common being NetFlow, Cisco ASA, and Palo Alto TRAFFIC logs. Endpoint examples would be Carbon Black and Symantec Endpoint. Finally, "catchall" is any logs that do not fit into the above categories.

Analytic Name	Behavior	Description	Data Type
Account Enumeration	• Account Enumeration	Account Enumeration finds workstations/IPs where a large number of distinct accounts fails to login.	Windows
Advanced Beacon	• Multistage Beacon	Advanced beacon detects beacons to common ports with varying intervals	Flow AWS VPC
Advanced Beacon	• Multistage Beacon Blacklist	Advanced beacon detects beacons to common ports with varying intervals	Flow AWS VPC
AlertX	• Symantec Endpoint Alert	AlertX forwards alert logs from Symantec Endpoint	Endpoint Catchall
Cohort Anomaly	• Failed /O365 Access from Anomalous Location	Flags actions from O365 users that are originating from geographical anomalous locations for that user	O365 CloudTrail
Cohort Anomaly	• Successful/Failed Anomalous Login Location	Flags new login locations for a user that are also anomalous based on similar users' behavior	Windows
Data Loss	• Unusual Data Transfer	The data loss analytic detects excessive bytes transfer to anomalous ASN	Flow AWS VPC
Domain Beacon	• Large Number of Subdomains	Detects if many subdomains are being requested on the same domain name in a given period of time	URL DNS
Domain Beacon	• Periodic Domain Beaconing	Domain beacon detects beacons to domain names, regardless of destination IP. It has additional	URL DNS
FAIL	• Failed Logins 10/100/1000 (After Password Reset)	FAIL identifies when a user fails to login X times or more in a row without a success. A separate behavior is created if these failures occur after an account had its password reset/changed.	Windows O365 Flow (Fortinet VPN)

Analytic Name	Behavior	Description	Data Type
FAIL	- Privileged User Failed Logins 10/100/1000 (After Password Reset)	Identifies when a user with adminlevel privileges fails to login multiple times without a successful attempt. A separate behavior is created if these failures occur after an account had its password reset/changed.	Windows O365 Flow (Fortinet VPN)
Kumo	- (Allow All) Ingress/Egress on Sensitive Port(s)	Identifies when a user has changed security group rules so that traffic has been allowed inbound or outbound over sensitive ports (e.g. SSH, Telnet, etc.). A separate behavior flags if the traffic is allowed to/from the entire internet.	CloudTrail
Kumo	- (Failed) Console Login without MFA	Identifies when a user attempts to login to the AWS console without MFA, excluding SSO/SAML authentication	CloudTrail
Kumo	- Anomalous Number of S3 Bucket Object Access 10/100/1000	Identifies when a user has accessed a number of unique objects from S3 buckets that is anomalously large for their typical access patterns	CloudTrail
Kumo	- Anomalous Number of Access Denied Attempts 10/100/1000	Identifies when a user has performed a large number of actions that have been denied	CloudTrail
Kumo	- CloudTrail Logs Stopped	Alerts when logging for a trail has been stopped	CloudTrail
Kumo	- CloudTrail Trail Deleted	Alerts when a trail has been deleted entirely	CloudTrail
Kumo	- S3 Bucket Granted Public Access	Alerts when a user has granted public access to an S3 bucket	CloudTrail
Metalytic	- Anomalous Username and Account Enumeration	Alerts when an account with an anomalous username attempts to login and is also part of a possible account enumeration attempt.	Windows
Metalytic	- Brute Force and Account Enumeration	Alerts when an account fails to login a large number of times and is also part of a possible account enumeration attempt.	Windows
Metalytic	- Failed Anomalous Login Location and Brute Force	Alerts when a user has had a large number of failed login attempts to a host, and that host is anomalous for the user.	Windows

Analytic Name	Behavior	Description	Data Type
Metalytic	• First Time Adding Members and Changing Universal Groups	Alerts the first time in X days the user has both added members to universal groups and changed universal groups.	Windows
Metalytic	• First Time Removing Members from Universal and Global Groups	Alerts the first time in X days the user has removed members from both universal and global groups.	Windows
Metalytic	• Port Vuln and AdvBeacon	Metalytic identifies when multiple analytic behaviors flag for a certain entity that have been deemed high severity if found in combination	All
Metalytic	• Successful Anomalous Login Location and Brute Force	Alerts when a user logs in to a host anomalous for the user, but also had a large number of failed attempts.	Windows
Metalytic	• VIP Behavior	Alerts on analytic hits with a user entity that has been labeled by the customer as a VIP.	All
MinerX	• Known Cryptomining Domain	Identifies known cryptomining domains	URL DNS
MinerX	• Known Cryptomining Exchange	Identifies known cryptomining exchange sites	URL DNS
P2PX	• BitTorrent	Identifies P2P traffic	Flow AWS VPC
P2PX	• P2P	Identifies P2P traffic	Flow AWS VPC
PAX	• Palo Alto Command and-control Alert	PAX forwards alert logs from Palo Alto	Catchall (Palo Alto only)
PAX	• Palo Alto Critical Alert	PAX forwards alert logs from Palo Alto	Catchall (Palo Alto only)
PAX	• Palo Alto Peer-to-peer Alert	PAX forwards alert logs from Palo Alto	Catchall (Palo Alto only)
PhishX	• Phishing Domain	This analytic attempts to detect phishing domains using known patterns of major brands and commonly used keywords in historical phishing attempts. The WHOISXML API service is used to check registration date in order to reduce false positives.	URL DNS
PortVuln	• Anomalous Database Server Behavior	Identifies successful connections inbound/outbound on vulnerable	Flow AWS VPC

Analytic Name	Behavior	Description	Data Type
		ports and prioritizes via PMI of the internal/external IP pair.	
PortVuln	• Anomalous DNS Behavior	Identifies successful connections inbound/outbound on vulnerable ports and prioritizes via PMI of the internal/external IP pair.	Flow AWS VPC
PortVuln	• Anomalous Domain Controller Behavior	Identifies successful connections inbound/outbound on vulnerable ports and prioritizes via PMI of the internal/external IP pair.	Flow AWS VPC
PortVuln	• Anomalous FTP Behavior	Identifies successful connections inbound/outbound on vulnerable ports and prioritizes via PMI of the internal/external IP pair.	Flow AWS VPC
PortVuln	• Anomalous IRC Behavior	Identifies successful connections inbound/outbound on vulnerable ports and prioritizes via PMI of the internal/external IP pair.	Flow AWS VPC
PortVuln	• Anomalous Mail Server Behavior	Identifies successful connections inbound/outbound on vulnerable ports and prioritizes via PMI of the internal/external IP pair.	Flow AWS VPC
PortVuln	• Anomalous NetBIOS Behavior	Identifies successful connections inbound/outbound on vulnerable ports and prioritizes via PMI of the internal/external IP pair.	Flow AWS VPC
PortVuln	• Anomalous Remote Desktop Behavior	Identifies successful connections inbound/outbound on vulnerable ports and prioritizes via PMI of the internal/external IP pair.	Flow AWS VPC
PortVuln	• Anomalous SMB Behavior	Identifies successful connections inbound/outbound on vulnerable ports and prioritizes via PMI of the internal/external IP pair.	Flow AWS VPC
PortVuln	• Anomalous SSH Behavior	Identifies successful connections inbound/outbound on vulnerable ports and prioritizes via PMI of the internal/external IP pair.	Flow AWS VPC
PortVuln	• Anomalous STUN Behavior	Identifies successful connections inbound/outbound on vulnerable ports and prioritizes via PMI of the internal/external IP pair.	Flow AWS VPC

Analytic Name	Behavior	Description	Data Type
PortVuln	• Anomalous Telnet Behavior	Identifies successful connections inbound/outbound on vulnerable ports and prioritizes via PMI of the internal/external IP pair.	Flow AWS VPC
PSpawn	• New LOLBIN Process	Alerts when a "Living-off-the-Land" process is seen running for the first time in the environment.	Endpoint Sysmon Windows
PSpawn	• Suspicious LOLBIN Usage	Alerts when a user runs one or more anomalous "Living-off-the-Land" processes compared to their baseline behavior.	Endpoint Sysmon Windows
PSpawn	• Suspicious Process Spawn	Pspawn detects suspicious executables that are spawned from known processes like notepad.exe	Endpoint Sysmon Windows
ScanX	• External Horizontal Scanning	This analytic looks for internal and external scanning behavior in flow data (firewall, netflow, etc.).	Flow AWS VPC
ScanX	• External Targeted Scanning	This analytic looks for internal and external scanning behavior in flow data (firewall, netflow, etc.).	Flow AWS VPC
ScanX	• External Vertical Scanning	This analytic looks for internal and external scanning behavior in flow data (firewall, netflow, etc.).	Flow AWS VPC
ScanX	• Internal Horizontal Scanning	This analytic looks for internal and external scanning behavior in flow data (firewall, netflow, etc.).	Flow AWS VPC
ScanX	• Internal Targeted Scanning	This analytic looks for internal and external scanning behavior in flow data (firewall, netflow, etc.).	Flow AWS VPC
ScanX	• Internal Vertical Scanning	This analytic looks for internal and external scanning behavior in flow data (firewall, netflow, etc.).	Flow AWS VPC
SED	• Unusual Executable Download	SED identifies executable files being downloaded from suspicious domains.	URL
SEF	• Suspicious_EXE_File path	SEF identifies suspicious file execution by treating their filepaths as a Markov chain. A Markov model is built over historical filepaths and low probability paths (i.e. C:\ -> weird\ -> temp\ -> folder) are reported. Thus, SEF requires access to a redis server instance to save historical state.	Endpoint Sysmon

Analytic Name	Behavior	Description	Data Type
Sentry	- Multiple	Sentry uses known-bad indicators and firewall rules to flag outliers across multiple data sets. The indicators are curated and validated by a SOC team, and the analytic is flexible to add new indicators as they are found.	Flow URL DNS o365
Sharemon	- (Anonymous Account) Anomalous Number of File Downloads/ Deletions 10/100/1000	Flags large number of file downloads/deletions from SharePoint based on a user's baseline. If the activity is coming from an anonymous account (i.e. the files were accessed by a public shared link) then a separate behavior is created.	o365
Sharemon	- Sensitive Share Folder Accessed	Alerts when a SharePoint folder deemed sensitive by the customer has been shared outside the organization.	o365
Sharemon	- Suspicious (Sensitive) Share Access	Monitors abnormal SharePoint folder access based on a user's baseline behavior. It also optionally alerts on a share being accessed that is labeled sensitive.	o365
Sloth	- Low Entropy Source Port Scanning	Sloth identifies external scanners that probe the network using primarily a single source port. Since source ports are typically randomly assigned, this behavior could point to a threat actor targeting a particular vulnerability.	Flow AWS VPC
Stranger Things	- Unregistered/ Recently Registered/ Blackholed/ Unusual Domain	This analytic uses an offline-trained character-level CNN autoencoder to detect anomalous host names being requested. It has additional behaviors for if the domain is either unregistered or recently registered according to WHOIS.	URL DNS
SWURL	- Suspicious Webserver URL	SWURL uses a deep learning algorithm trained on known-bad URL's that attackers typically use to scan for vulnerabilities. It identifies these URL's being accessed on internal webservers/resources.	URL
Sysmon Anomaly	- Curl File Upload	Monitors when a file is uploaded via the curl command.	Sysmon

Analytic Name	Behavior	Description	Data Type
Sysmon Anomaly	- Filename Spoof	Attempts to identify running processes that were potentially renamed to avoid detection.	Sysmon
Sysmon Anomaly	- Persistence via Registry Key	Alerts when the Run or RunOnce registry keys are edited, a common registry key used by attackers to persist on the device	Sysmon
Sysmon Anomaly	- Powershell Encoded Command	Alerts when powershell was given a base64 encoded command, a common method for attackers to obfuscate their actions	Sysmon
Sysmon Anomaly	- Process Injection Anomalous Call Trace	Alerts when a process loads an anomalous sequence of libraries when accessing another process	Sysmon
Sysmon Anomaly	- Security Product Disabled	Monitors when certain security products (Windows Defender, Windows Firewall, etc.) are disabled.	Sysmon
ThreatX	- Blacklist	ThreatX detects internal traffic going to blacklisted IP	Flow AWS VPC
UAAD	- Strange User Agent	User Agent Anomaly Detection (UAAD) is a character-level recurrent neural network that classifies user agents into three general categories: benign, random character, and attack-like (i.e. SQL injection). It is trained offline with static data.	URL
VPNX	- Successful/Failed VPN Multilocation	VPNx looks at VPN logins from Cisco ASA, Palo Alto, Fortinet, and OpenVPN, as well as login events from o365, and identifies logins that meet one or both of the following criteria: - Two logins are separated geographically by an impossible distance for the difference in login times. - A login is originating from an IP address on a blacklist.	Flow o365
VPNX	- VPN Blacklist	Identifies a VPN or o365 login from a blacklisted location.	Flow o365
WebServer X	- Direct to IP Server Access	WebServerX looks at Webserver logs and WAF detections to determine targeted attacks	URL

Analytic Name	Behavior	Description	Data Type
WebServer X	- Directory Traversal Attempt	WebServerX looks at Webserver logs and WAF detections to determine targeted attacks	URL
WebServer X	- Excessive Client HTTP Errors	WebServerX looks at Webserver logs and WAF detections to determine targeted attacks	URL
WebServer X	- Excessive File HTTP Errors	WebServerX looks at Webserver logs and WAF detections to determine targeted attacks	URL
WebServer X	- Excessive URL HTTP Errors	WebServerX looks at Webserver logs and WAF detections to determine targeted attacks	URL
WebServer X	- Non-Standard Characters in URL	WebServerX looks at Webserver logs and WAF detections to determine targeted attacks	URL
WebServer X	- Web Application Firewall Alerts	WebServerX looks at Webserver logs and WAF detections to determine targeted attacks	URL
Windows Audit	- (Non-Admin) User Password Change Successful/Failed	Audits a user attempting to change an account's password. It can optionally flag a separate behavior if the source user and target user are not the same and the source user is not a known admin.	Windows
Windows Audit	- (Non-Admin) User Password Reset Successful/Failed	Audits a user attempting to reset an account's password. It can optionally flag a separate behavior if the source user and target user are not the same and the source user is not a known admin.	Windows
Windows Audit	- Added Self to Admin Group	A user has added their own account to an admin group.	Windows
Windows Audit	- Audit Log Cleared	Audits for security logs being cleared	Windows
Windows Audit	- Default Account Activity	Identifies activity by "default" accounts that could have elevated privileges (e.g. "Administrator", "admin", "root", etc.)	Windows
Windows Audit	- Domain Controller Password Changed	Logs when a Domain Controller's password has changed. These should be relatively rare and is a common indicator for the Zerologon exploit.	Windows
Windows Audit	- Emails Set to Forward to Outside Address	Alerts when a user's mailbox is set to forward emails to an email address that is outside the organization	O365

Analytic Name	Behavior	Description	Data Type
Windows Audit	• First Time Adding/Removing Members to/from Global/Local/Universal Group	Audits the first time an account has added/removed members to/from a Global/Local/Universal group	Windows
Windows Audit	• First Time Creating/Deleting/Changing Global/Local/Universal Group	Audits the first time an account has created/deleted/changed a global/local/universal group	Windows
Windows Audit	• Large Number of Global/Local/Universal Groups Created/Deleted/Changes	Alerts when an account has created/deleted an anomalously large number of groups, or has made an anomalously large number of changes to groups	Windows
Windows Audit	• Large Number of Group Enumerations	Alerts when an account has enumerated a large number of groups	Windows
Windows Audit	• Large Number of User Group Enumerations	Alerts when an account has enumerated a large number of users' groups	Windows
Windows Audit	• Large Number of Users Added/Removed to/from Global/Local/Universal Group	Alerts when an account has added or removed an anomalously large number of users to/from a group	Windows
Windows Audit	• New Privileges	Audits for new admin privileges assigned to an account	Windows
Windows Audit	• New Privileges	Audits when an account is granted a new privilege	Windows
Windows Audit	• New Scheduled Task	Identifies when a scheduled task not previously seen has been started	Windows
Windows Audit	• New User(-Process) Enumerating User Groups	Audits when an account is seen enumerating one or more users' groups for the first time, or doing so with a new process	Windows
Windows Audit	• New User(-Process) Enumerating Groups	Audits when an account is seen enumerating groups for the first time, or doing so with a new process	Windows
Windows Audit	• Password Set to Never Expire	Audits all accounts that were modified to have their passwords never expire.	Windows
Windows Audit	• Potential Pass the Hash Attempt	Tries to identify if a pass the hash attack was attempted.	Windows

Analytic Name	Behavior	Description	Data Type
Windows Audit	• Power BI Dataset/Folder/ Report Edit/ Creation/Deletion Audit	Audits any time a Power BI dataset/folder/report is created/deleted/edited	O365
Windows Audit	• SeDebugPrivilege Granted	Audits for the SeDebugPrivilege being granted, which is commonly used in process injection attacks.	Windows
Windows Audit	• SID History Injection	Alerts when an account attempts to modify the SID history of another account to include the SID for an admin-level account.	Windows
Windows Audit	• Successful/Failed Mailbox Access	Audits when a user attempts to access another user's mailbox	O365
Windows Audit	• User Account Change Audit	Audits all account changes for a specific user. For this behavior, the modified account is the entity.	Windows
Windows Audit	• User Account Management	Audits events where a user account has been created or changed	Windows
Windows Audit	• User Password Change/Reset Audit	Audits all password change/reset attempts on a specific user. For this behavior, the modified account is the entity.	Windows
WUN	• Anomalous Username	Weird Username (WUN) identifies lexically anomalous usernames that fail to login. It is trained on successful logins to determine what is a normal username structure for the environment.	Windows O365

EXHIBIT B: SUPPORTED SERVICES AND DEVICES

Enterprise Services

Log Source	Log Format(s)	Transfer Method	Supported Version(s)
Active Directory	- EVT	Windows Rsyslog Agent	- Windows Server
DNS Server	DNS Debug Logs - Syslog	Windows Rsyslog - Agent - Direct	- Microsoft DNS - BIND9 - Infoblox DDI
DHCP Server	DHCP Audit Logs - Syslog	Windows Rsyslog - Agent - Direct	- Microsoft DHCP - ISC dhcpd - Infoblox DDI
Network Access Control	- Syslog - NPS Accounting logs	Windows Rsyslog - Agent - Direct	- Aruba ClearPass - Cisco ASC - Cisco ISE - Windows Network Policy Server

Network Devices

Log Source	Log Format(s)	Transfer Method	Supported Version(s)
Network Firewall	- Syslog - Netflow / IPFIX	- Direct	- Barracuda NGFW - Check Point NGFW - Cisco ASA - Cisco FirePower - Cisco Meraki - Fortinet FortiGate - Juniper NetScreen - Juniper SRX - Palo Alto PA Series - Palo Alto VM Series - SonicWall TZ Series - VMware NSX Firewall
Web Proxy / Gateway	- Syslog	- Direct	- Barracuda Web Security Gateway - Blue Coat ProxySG - Cisco Umbrella - Cisco Web Security - Forcepoint Web Security Gateway - McAfee Web Gateway

			• Symantec Web Security Services • Trend Micro • Zscaler Internet Access
Web Application Firewall	• Syslog	• Direct	• Barracuda Web Application Firewall • Fortinet Web • Application Firewall
VPN	• Syslog	• Direct	• Cisco VPN • Fortinet VPN • OpenVPN • Palo Alto VPN • Pulse Secure VPN
Advanced Threat Protection (ATP)	• Syslog	• Direct	• Cisco FirePower FireEye • NX • Palo Alto WildFire • Symantec ATP
IDS / IPS	• Syslog	• Direct	• Cisco FirePower • Cisco FirePower • Trend Micro TippingPoint • Vectra X-Series • Zeek / Bro

Endpoint Devices

Log Source	Log Format(s)	Transfer Method	Supported Version(s)
Endpoint Protection	• JSON • Syslog	• API Direct	• Bitdefender GravityZone • Carbon Black Protection • Cisco AMP for Endpoints • CrowdStrike Falcon • Cylance CylancePROTECT • FireEye HX • McAfee Endpoint Security • Microsoft Windows Defender ATP • SentinelOne EDR • Symantec Endpoint Protection
Endpoint Detection and Response	• JSON • Syslog	• API Direct	• Carbon Black Detection • Cisco AMP • CrowdStrike Falcon • Cylance CylanceOPTICS • FireEye HX • Microsoft Windows Defender ATP • SentinelOne EDR

			- Symantec ATP

Vulnerability Tools

Log Source	Log Format(s)	Transfer Method	Supported Version(s)
Vulnerability Scanner	- Syslog	- Direct	- Rapid7 Nexpose - Tenable Nessus Network Monitor

Infrastructure as a Service (IAAS)

Log Source	Log Format(s)	Transfer Method	Supported Version(s)
AWS CloudTrail	- JSON	- S3 Bucket	- Identity and Access Management (IAM) - Client VPN
AWS CloudWatch	- JSON	- S3 Bucket	- Client VPN
AWS VPC Flow Logs	- JSON	- S3 Bucket	- VPC Flows

Software as a Service

Log Source	Log Format(s)	Transfer Method	Supported Version(s)
Microsoft 365	- JSON	- API	- Audit.AzureActiveDirectory - Audit.Exchange - Audit.General - Audit.Sharepoint - DLP.All
Okta	- JSON	- API	- Workforce Identity
Mimecast	- JSON	- API	- Email Security
Cisco AMP	- JSON	- API	- Endpoints - Email Security - Web Security