Exhibits to

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

E R	F	H	H X
E M	• 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)
O	• (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	

E R	F	H	H X
	• 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
	• 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
	• 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
	• 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
	• VIP Behavior	Alerts on analytic hits with a user entity that has been labeled by the customer as a VIP.	All

E R	F	H	H X
T	• Anomalous Telnet Behavior	Identifies successful connections inbound/outbound on vulnerable ports and prioritizes via PMI of the internal/external IP pair.	Flow AWS VPC
TW	• New LOLBIN Process	A fsut x i fo b [Ljwjoh-off-the-Land" process is seen running for the first time in the environment.	Endpoint Sysmon Windows
TW	• Suspicious LOLBIN Usage	Alerts when a user runs one or more bop n bpv t [Ljwjoh-off-the-Land" processes compared to their baseline behavior.	Endpoint Sysmon Windows
TW	• Suspicious Process Spawn	Pspawn detects suspicious executables that are spawned from known processes like notepad.exe	Endpoint Sysmon Windows
W	• External Horizontal Scanning	This analytic looks for internal and external scanning behavior in flow data (firewall, netflow, etc.).	Flow AWS VPC
W	• External Targeted Scanning	This analytic looks for internal and external scanning behavior in flow data (firewall, netflow, etc.).	Flow AWS VPC
W	• External Vertical Scanning	This analytic looks for internal and external scanning behavior in flow data (firewall, netflow, etc.).	Flow AWS VPC

E R	F	H	H X
W	• Directory Traversal Attempt	WebServerX looks at Webserver logs and WAF detections to determine targeted attacks	URL
W	• Excessive Client HTTP Errors	WebServerX looks at Webserver logs and WAF detections to determine targeted attacks	URL
W	• Excessive File HTTP Errors	WebServerX looks at Webserver logs and WAF detections to determine targeted attacks	URL
W	• Excessive URL HTTP Errors	WebServerX looks at Webserver logs and WAF detections to determine targeted attacks	URL
W	• Non-Standard Characters in URL	WebServerX looks at Webserver logs and WAF detections to determine targeted attacks	URL
W	• Web9.96 .08 89.96 reW		

EXHIBIT B: SUPPORTED SERVICES AND DEVICES

Enterprise Services

P	W	P	X	W
E	**H**	EVT	Windows Rsyslog Agent	Windows SreW0 0 1 344.769.38 18.9