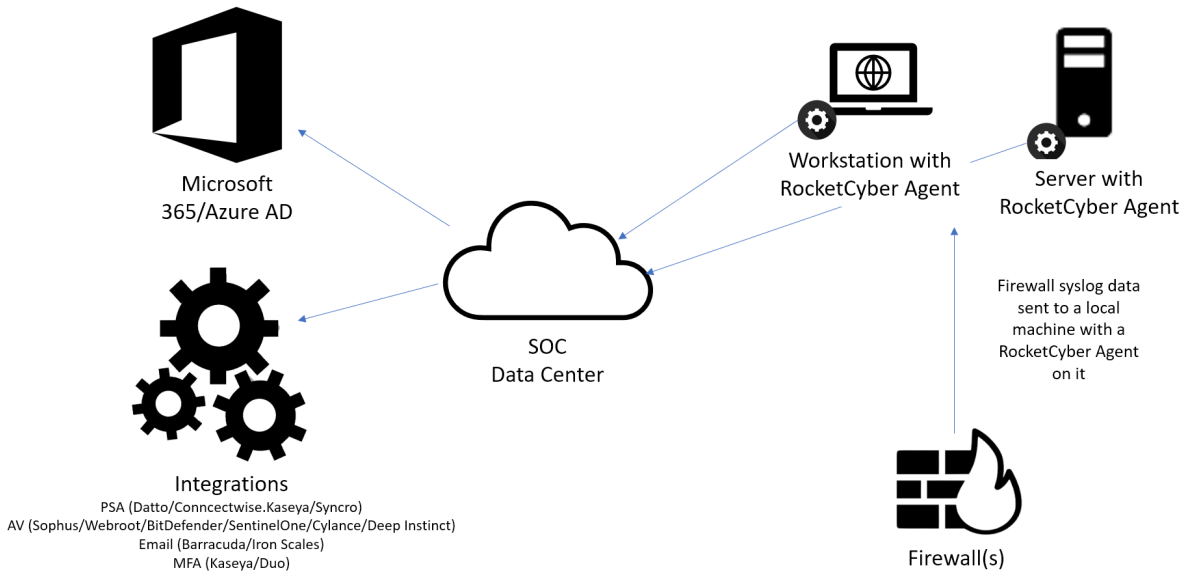
RocketCyber Managed SOC Agent Architecture & Capabilities

Overview

RocketCyber provides a managed SOC (security operation center) service that leverages the our Threat Monitoring Platform to detect malicious and suspicious activity across three critical attack vectors: Endpoint | Network | Cloud. Our elite team of security analysts hunt, triage and work with your team when actionable threats are discovered. This document provides a high-level overview of the security and architecture RocketCyber uses to gather security telemetry as diagramed below.



SOC Data Center

The RocketCyber SOC Data Center for North American customers is physically located in the US. All security data/telemetry is sent/received to this location. RocketCyber leverages Salesforce's Heroku platform which runs on Amazon AWS to host the SOC platform. Customers have web access to the platform which is encrypted between their browser and the platform using industry standard TLS. RocketCyber supports Two-Factor Authentication (2FA) and strongly recommends its usage to protect customer logins.

RocketCyber Agent Communication

In order to gather security telemetry from endpoints back to the RocketCyber SOC Data Center, customers install a RocketCyber agent that runs on Windows Servers, Windows Workstations, Linux and Mac devices. The RocketCyber agent

> **Communication**: All communication is OUTBOUND from the RocketCyber Agent to the SOC Data Center on port 443. The RocketCyber agent does not accept inbound connection which limits

the attack surface. Additionally, the RocketCyber Agent does not support Remote Control or the ability to run user generated content on endpoints.

Encryption: All communication from the RocketCyber Agent is encrypted using the TLS v1.2 protocol and only allow the following strong cipher suites:
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_AES_256_GCM_SHA384

Endpoint Event Log Monitoring

The RocketCyber agent gathers specific OS system and security logs and forwards these to the SOC in order to detect security events, provide data for SOC analysts to triage incidents and store logs for historical auditing purposes. By default, the following OS logs are collected by the RocketCyber agent:

Windows OS:
104-System Security Log was cleared
1102 - Security - Audit Log was cleared
4722 - Security - A user account was enabled
4735 - Security - Local Group Changed
7040 - System - Service was changed from auto start to disabled
7034 - System - Services Terminated Unexpectedly
4702 - Security - A scheduled task was modified
5142 - Security - A network share object was added
5144 - Security - A network share object was deleted
4625 - Security - An account failed to login
7036 - System - A defensive service was stopped
5145 - Security - A network share object was checked by PsExec
4649 - Security - A replay attack was detected
64004- System - Windows File Protection was unable to restore file to its original version
5143 - Security - A network share object was modified
4740 - Security - A user account was locked out
4698 - Security - A new scheduled task was created
7031 - System - Service terminated unexpectedly
4738 - Security - User account password was changed
4724 - Security - An attempt was made to reset an account's password
4720 - Security - Test user account created
1100 - System - Event logging was shut down

MacOS:
Log Privacy - Privatize log content that contains usernames, ip addresses, and other sensitive information.
Watch_Logon - User logins to the system
SSH_connection - Inbound SSH connections to the Mac
Watch_Logout - User logouts from the system

Failed_Auth - User authentication failure
Sudo_Usage - Privilege Escalation using sudo

Linux OS:
Sudo_Usage - Privilege Escalation using sudo
SSH_login - Inbound SSH connections to the Mac
SSH_failed login - inbound SSH logins failed
User_add - a new user account was created
Password_change - a user's password was changed
Group_change - a group was changed
Del_user_group - a user was removed from a group
Failed_Auth - User authentication failure
SSH_login_pkey - successfully public key login via ssh was detected
SSH_login_pkey_failed - a public key login via ssh failed
user_del - a user account was deleted
new_group - a new group was created
add_user_group - a user was added to a group

Breach Detection

The RocketCyber agent utilizes proprietary technology to monitor Windows and Mac devices for indicators that the device has been compromised. Leveraging the MITRE ATT&CK® framework, the agent collects data related to activity on the device and forwards events to the SOC for triage and security analysis. By default, the following techniques are monitored for Windows OS with a subset for MacOS:

Advanced Breach Detection Telemetry	
Discovery	**Persistence Privilege Escalation**
T1201 - Password Policy Discovery	T1013 - Port Monitors
Defensive Evasion Execution	T1050 - New Service
T1085 - Rundll32	T1103 - AppInit DLLs
T1117 - Regsvr32	T1182 - AppCert DLLs
T1118 - InstallUtil	**Defense Evasion Peristence**
T1121 - Regsvcs/Regasm	T1158 - Hidden Files and Directories
T1170 - Mshta	T1116 - Code Signing
T1216 - Signed Script Proxy Execution	**Defense Evasion Peristence**
T1218 - Signed Binary Proxy Execution	T1198 - SIP and Trust Provider Hijacking
Execution	**Persistence**
T1035 - Service Execution	T1004 - Winlogon Helper DLL
T1047 - Windows Management Instrumentation	T1031 - Modify Existing Service
T1059 - Command Line Interface	T1060 - Registry Run Keys / Start Folder
T1086 - Powershell	T1101 - Security Support Provider
T1173 - Dynamic Data Exchange	T1128 - Netsh Helper DLLs
Impact	T1131 - Authentication Package
T1490 - Inhibit System Recovery	T1136 - Create Account
Command And Control, Lateral Movement	T1137 - Office Application Startup
T1105 - Remote File Copy	T1180 - Screensaver
Defensive Evasion	**Lateral Movement**
T1070 - Indicator Removal on Host	T1076 - Remote Desktop Protocol
T1089 - Disabling Security Tools	T1077 - Windows Admin Shares
T1107 - File Deletion	**Execution, Lateral Movement**
T1126 - Network Share Connection and Removal	T1028 - Windows Remote Management
T1140 - Deobfuscate/Decode Files or Information	**Defense Evasion Execution**
T1202 - Indirect Command Execution	T1191 - CMSTP
Credential Access	**Execution Persistence Privilege Escalation**
T1003 - Credential Dumping	T1053 - Scheduled Task
T1081 - Credentials In Files	**Defense Evasion Privilege Escalation**
T1174 - Password Filter DLL	T1088 - Bypass User Account Control
T1214 - Credentials in Registry	**Defense Evasion Persistence Privilege Escalation**
	T1183 - Image File Execution Options Injection

Intrusion Monitoring

The RocketCyber agent monitors network ingress and egress network traffic on the monitored device and alerts the SOC for further analysis based on activity. This includes:

Cyber Terrorist Network Connections –detects network connections to various nation states that have been known to engage in cyberterrorist activities and compares IP address communications against real-time threat feeds to discover connections to malicious IPs, C2 servers, botnets and other backdoor services.

Suspicious Network Services – detects device network traffic which may be indicative of unusual activity, including Chargen, FTP, Telnet, SMTP, Finger, POP3, SOCKS, DOOM, VNC, Bit Torrent, IRC, Tor, Netbus, RDP and SSH/SFTP.

Malicious File Detection

The RocketCyber agent monitors and detects malicious files that are written to disk or executed and also monitors file communications that are indicative of cyrpto mining software. This additional layer of protection services as a backup for detecting malicious files that slip past your primary antivirus and antimalware solution.

Firewall Analyzer

The RocketCyber agent on Windows OS can serve a secondary purpose as a firewall analyzer. When enabled, the agent will provide a syslog interface to collect logs from local firewalls, parse the data in real-time, and forward a subset of security related events to the RocketCyber SOC for triage and storage. Logs not related to security events can, optionally, be configured to be stored locally on the device and/or be forwarded to an additional log storage location. In addition to capturing firewall security log events, RocketCyber can alert on firewall traffic based on geography and perform IP reputation lookups using our threat intelligence feeds to augment the firewall's built-in capabilities. The following firewalls are supported:

Cisco (Meraki, ASA, Firepower)
Fortinet
Sonicwall
Sophus XG and UTM
WatchGuard
Untangle
Barracuda
Ubiquiti
PfSense
Juniper
Zyxel
Mikrotik
Check Point
Palo Alto

Conclusion

The RocketCyber agent provides a secure, lightweight and easy to deploy capability to capture security telemetry from endpoints for the RocketCyber SOC to triage and log data. The capabilities go beyond log monitoring to incorporate breach detection, network activity and services, suspicious tools and malicious file detection to provide a comprehensive security solution enabling organizations to implement advanced detection and response capabilities to stop threats that have evaded traditional defenses.