1 Professional services project overview

1.1 Scope of Assets

SL	Device Type	Qty
1	Windows Servers	31
2	Linux Servers	212
3	MS SQL	6
4	Oracle	17
5	Mongo DB	2
6	Postgress SQL	13
7	Routers	35
8	Kubernetes Cluster	3
9	Load Balancers (GCP)	55
10	DNS Records	118
11	Trend Micro EDR	1
12	WAF	1
13	Firewall	2

1.2 Scope of Work

1.2.1 Professional Services

No.	Category	Detailed Scope	Part of SOW
1	Log Sources validation	Verify log flow from all sources into Chronicle.	✓
		Verifying Data quality and errors in logs	✓
		Checking parsing issues in logs from the log sources	✓
		Verifying user accounts and permissions.	✓
2	Finetuning and Testing	Onboarding additional devices to the chronicle which are not integrated previously as per the Info gathering sheet	✓
		Checking the logs, parsers for the new device integration	✓
		Creating user accounts and permissions	✓
		Fixing parsing issues for the log sources	✓

		Ensure that SIEM ingests threat intelligence.	✓
		Conduct thorough testing to ensure the SIEM solution functions as expected, including validating alerting, reporting, and incident response capabilities.	✓
3	Rule Detection & Alerts configuration	Validating current detection rules and finetuning	✓
		Creating customer defined detection rules (48 SIEM use cases shared by customer)	✓
		Implement multi-event correlation for complex threat detection	✓
		Fine-tune rules to minimize false positives	✓
		Testing the newly developed SIEM Use cases and Finetuning if required	✓
		Setup trigger expressions & thresholds	✓
		Define severity levels (P1, P2, P3 & P4)	✓
4	SOAR configuration.	Verifying/Establishing API connections between SOAR and Chronicle.	✓
		Configure data exchange and alert forwarding mechanisms.	✓
		Developing customer defined SOAR playbooks (8 play books shared by customer)	✓
		Testing and validation of SOAR playbooks	✓
5	Dashboards & Reports	Verifying Current dashboards and finetuning	✓
		Create 10 new custom dashboards as per customer requirement and feasibility	✓
		Adding the user permissions to the dashboard	✓
		Verifying Schedule reports are executed as expected and finetuning	✓
		Creating 10 new custom reports as per customer requirement and feasibility	✓

1.3 SIEM Usecases

SL	SIEM Usecases
1	Remote File Creation on Sensitive Directory
2	Linux Restricted Shell Breakout via Linux Binary
3	Attempt to Disable IPTables or Firewall
4	Connection to Internal Network via Telnet
5	Malicious Behavior Detection: Potential Linux Reverse Shell via Java
6	Malicious Behavior Prevention: Potential Linux Reverse Shell via Java
7	Potential Reverse Shell via Suspicious Child Process
8	Firewall VPN Authentication Failure Alert
9	Unapproved Application Execution
10	Brute Force Attack Detected
11	Unauthorized Remote Desktop Protocol (RDP) Connection
12	DNS Spoofing Detected

13	Suspicious Email Attachment
14	Web Application Firewall (WAF) Alert
15	Outbound Traffic to Blacklisted IP
16	High Number of Failed SSH Attempts
17	Sudden Increase in Network Bandwidth Usage
18	Abnormal User Behavior (UEBA)
19	Database Schema Changes Detected
20	Suspicious Network Port Opened
21	Web Shell Detected
22	Anomalous HTTP/S Traffic Detected
23	Rogue Access Point Detected
24	Connection to Known Malicious Domain
25	API Abuse Detected
26	Abnormal Increase in Database Queries
27	Zero-Day Exploit Detected
28	Suspicious Bluetooth Connection
29	Unauthorized Script Execution
30	Unexpected Traffic Spike to External Sites
31	Outdated Antivirus Definitions
32	Unauthorized API Key Usage
33	Unusual Activity in Admin Account
34	Evasion Techniques Detected
35	Decreased Traffic on Critical Services
36	Suspicious Process Execution
37	Privilege Escalation Detected
38	Remote Login Detected
39	VPN Connection Established
40	Service/Daemon Stopped Unexpectedly
41	Root Login Detected
42	Unauthorized Software Installation
43	Port Scanning Activity
44	Intrusion Detection System (IDS) Alert
45	Database Access Outside Business Hours
46	Application Crash Detected
47	Unauthorized Use of USB Devices
48	Anomalous Traffic Volume Detected

1.4 SOAR Playbooks

SL	SOAR Playbooks	
1	Brute Force Attack Remediation	Automatically lock user accounts after detecting brute force login attempts through AD

2	Ransomware Detection and Containment	Automatically isolating/block affected machines from the network to prevent ransomware from spreading to other endpoints through EDR and block out going traffic to malicious IP through Firewall.
3	Malware-Infected Endpoint Containment	Automatically isolating/ block affected machines from the network to prevent ransomware from spreading to other endpoints through EDR
4	Suspicious VPN Connection Investigation	Use threat intelligence feeds to check reputation of the IP address used for the VPN connection and block traffic through Firewall
5	Unauthorized Administrative Access	Automated actions to lock or disable the affected administrative account to prevent further access by AD
6	Threat Intelligence Correlation and Blocking	Correlate multiple threat intels and check reputation of the source IP address or domain and block traffic to and from that IP or domain on firewalls
7	Unusual User Behavior Detection (UEBA)	Trigger actions to lock the compromised or suspicious account to prevent further access by AD
8	DDoS Attack Mitigation	Trigger actions to block malicious IP's by Firewall/WAF

2 Deliverables – Professional Services

- **Fully configured Google Chronicle SIEM environment:**
    - Operational Chronicle instance with all necessary configurations and above mentioned log sources onboarding & SIEM Usecases.
- **Integrated SOAR platform with the mentioned 8 automated playbooks:**
    - 8 automated playbooks mentioned above.

Scope of Work (SOW): Trend Micro XDR Policy Review & Modification

1. Brief Scope

- Review current **Trend Micro XDR** policies and configurations.
- Identify gaps, inconsistencies, and areas for improvement.
- Implement necessary changes to improve threat detection, response, and compliance.
- Ensure alignment with industry best practices and organizational security requirements.

2. Deliverables

- **Assessment Report** (Findings & Recommendations)
- **Updated Trend Micro XDR Policies**
- **Training Session for IT/Security Team**

S.No	**EDR Use Cases**	**Description**
1	Suspicious PowerShell Execution	Detect and block potentially malicious PowerShell scripts with obfuscated content.
2	Unauthorized Access to System Files	Monitor for unauthorized access to critical system files, indicating compromise.
3	Credential Dumping Attempt	Identify attempts to extract credentials from memory using tools like Mimikatz.
4	Brute Force Attack Detection on SSH	Detect repeated failed SSH login attempts to identify brute force attacks.
5	Suspicious Network Traffic to Malicious IPs	Monitor outbound connections to known malicious IP addresses to detect compromise.
6	Privilege Escalation via Sudo or Su Command	Track attempts to escalate privileges using unauthorized sudo or su commands.
7	Ransomware Behavior Detection	Detect ransomware-like behavior such as mass file encryption and stop it.
8	Unauthorized Software Installation	Monitor and alert on unauthorized software installations to prevent vulnerabilities.
9	Suspicious Registry Modification	Detect unauthorized or suspicious changes to the Windows registry.

10	DNS Tunneling Detection	Monitor and block DNS tunneling attempts to prevent data exfiltration.
11	Malware Beaconing Detection	Identify repetitive outbound connections indicating malware beaconing behavior.
12	Suspicious Process Execution	Detect execution of suspicious processes indicating malware or unauthorized scripts.
13	Endpoint Communication with Dark Web Servers	Flag communication between endpoints and servers on the dark web.
14	Suspicious File Download or Execution	Monitor for downloads or execution of suspicious files from untrusted sources.
15	Unusual Traffic to Tor Exit Nodes	Detect and block traffic to Tor exit nodes, indicating anonymized malicious communication.