SERVICE DESCRIPTION

Threat Detection & Response: Co-Managed SOC

Service Scope
Clients desiring threat detection services in conjunction with their own SIEM/SOC infrastructure may subscribe to the Threat Detection and Response services under the Co-Managed SOC platform (the “Services”). The Services include the following:

- Transitional project consulting and provisioning to plan, build, and/or optimize threat detection and response solutions to steady state. This entails consulting and provisioning to assist in the transition project (the Plan and Build functions) and to optimize threat detection and response operations in preparation for steady state services.
- The Services will investigate high fidelity alerts on the Client’s SIEM, enrich the use of other telemetry integrated into the SIEM, determine a final actionability disposition, and perform appropriate response escalations.
- SIEM Management includes maintenance, tuning and use case implementation.
- A Trustwave Information Security Advisor (ISA) for ongoing management and maintenance of the Co-Managed SOC environment, guidance in maturing system and process capabilities (required).

Threat Detection & Response Consulting

SIEM Jumpstart
Service on-boarding requires a discovery and transformation project as provided by the Trustwave TDR Consulting’s SIEM Jumpstart offering (“Jumpstart”). The Jumpstart provides a comprehensive SIEM onboarding service for supported SIEM technologies and provides the options in the table below. The SIEM Jumpstart program includes a maturity and capabilities assessment that helps Clients measure and maintain their SIEM capabilities, thereby, enabling Clients to better define their cybersecurity posture and enhance their strategy and vision to build and scale a best practices cybersecurity operations program.

SIEM Jumpstart services available:

<table>
<thead>
<tr>
<th></th>
<th>Jumpstart Lite</th>
<th>Jumpstart</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Management</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Applicable Service Description</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>Jumpstart</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jumpstart Lite</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 1: Jumpstart services available options**

*Restricted to supported event sources per SIEM platform. Number of use cases to be implemented in one time project. Additional work plans can be provided on request.

Full Project scope for Trustwave Jumpstart can be found at:

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning and Transition to Trustwave</td>
<td>X X</td>
</tr>
<tr>
<td>Threat Detection and Response services</td>
<td></td>
</tr>
<tr>
<td>SIEM Clean up and configuration</td>
<td>X X</td>
</tr>
<tr>
<td>Architecture &amp; use case documentation</td>
<td>X X</td>
</tr>
<tr>
<td>Standard use cases</td>
<td>X X</td>
</tr>
<tr>
<td>Custom use cases*</td>
<td>X</td>
</tr>
<tr>
<td>Use case strategy</td>
<td>X</td>
</tr>
<tr>
<td>Custom correlations*</td>
<td>X</td>
</tr>
<tr>
<td>Process creation / Optimization</td>
<td>X</td>
</tr>
<tr>
<td>Data Source on boarding</td>
<td></td>
</tr>
<tr>
<td>Threat detection &amp; Response Gap Assessment</td>
<td>X</td>
</tr>
<tr>
<td>report</td>
<td></td>
</tr>
</tbody>
</table>

**Threat Detection & Response Agility Program (Optional)**

Trustwave recognizes that organizations are not static, and their businesses are continuously adapting and evolving through organic and inorganic innovation. New lines of business, mergers and acquisitions, and geographic markets all strain capacity and time from our Clients’ resources. The Threat Detection & Response (TDR) Agility Program provides full access to the entire SOC consulting and engineering skills and experiences.
Under the Agility Program, Trustwave will facilitate an advisory and project execution program to steer and adapt new SOC technologies and relevant people, and process to partner with your security team.

The TDR Agility Program will establish a phased project plan over the duration of the Co-Managed SOC program to advise, design, and drive new use cases, technologies, and processes to proactively adapt to the speed of the Client’s business.

The following deliverables will be created and evolved with each quarterly engagement:
- Threat detection and response maturity report
- Use case library, pipeline and technology implementation roadmap
- SOC processes and playbook manual
- People and technology capacity modelling

Example timeline for TDR Agility Program

Note: The TDR Agility Program represents 640 hours of labor per year with a standard approach recommending 160 hours per quarter. Per project need, the Client may utilize more, or less, than the 160 hours per quarter.

Full Project scope for the TDR Agility Program can be found at:

<table>
<thead>
<tr>
<th>Applicable Service Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TDR Agility Program</td>
</tr>
</tbody>
</table>

Threat Detection & Response – Global Threat Operations

Trustwave’s Threat Detection & Response – Global Threat Operations service (the “GTO Service”) allows a Client’s SIEM ruleset to generate alerts that Trustwave’s Global Threat Operations (GTO) Analysts will investigate, enrich, and determine appropriate escalation priority. Events and Alerts generated by the SIEM will be monitored 24x7x365 by GTO who provide tier 1 analysis and investigation of security alerts as well as escalate events to the tier 2 team, in accordance with the Communication Plan & Runbook.

Service scope and responsibilities

In the Threat Detection & Response GTO service, Trustwave Analysts will utilize Trustwave’s threat intelligence footprint to enrich the SIEM’s output as applicable. Over time, alerts are tuned and suppressed to remove as
much noise as possible. New alerts and use cases can be created as the environment matures. During the GTO Service:

- Analyzed events may generate alerts in the supported SIEM. These alerts are forwarded to Trustwave’s Fusion Platform, where they are presented to GTO Analysts as “Findings” and displayed in the Fusion Platform for additional investigation by the Client and Trustwave. Initial Triage and Analysis is based on these Findings/Alerts within the Fusion Platform.

- When deemed necessary, Trustwave GTO Analysts will investigate events and alerts in the local SIEM environment directly in order to access more detailed or contextual information; all base log events will remain in the SIEM instance.

- GTO Analysts review the generated alerts, collected events, and trends of activity to identify any suspicious behavior in the environment. If suspicious activity is found, a ticket is generated in the Trustwave Fusion Platform, and Client is notified by email, the Fusion Mobile App, or by phone through the incident response process defined with the Client. The ticket information is displayed in the Fusion Platform.

- The Trustwave GTO Analyst categorizes the alerts. Notifications of Alerts that are determined to be a potential security threat and are of a high and critical severity are emailed to Client and followed up by a phone call, following Client’s pre-defined escalation procedures. Criticality of incidents and notifications are described in the table below:

<table>
<thead>
<tr>
<th>Priority</th>
<th>Analyst Response</th>
<th>Recommended client Response</th>
<th>Priority Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Phone call &amp; Email</td>
<td>Immediate</td>
<td>Incidents at this level are actionable, high risk events which are actively compromising or damaging the Client environment. Investigations that result in this priority require immediate action to contain the threat.</td>
</tr>
<tr>
<td>High</td>
<td>Phone call &amp; Email</td>
<td>One to four hours</td>
<td>Incidents at this level are actionable, high risk events that have the potential to cause severe damage to Client environments. Investigations that result in priority require clients to take nearly immediate defensive actions.</td>
</tr>
<tr>
<td>Medium</td>
<td>Email</td>
<td>Twelve to twenty-four hours</td>
<td>Incidents at this level are actionable, medium-risk events that have the potential to cause limited damage to Client environments. Investigations that result in priority require clients to take timely, but not necessarily immediate action.</td>
</tr>
<tr>
<td>Low</td>
<td>Email</td>
<td>Informational Only</td>
<td>Incidents at this level are not immediately actionable and may require further</td>
</tr>
</tbody>
</table>
Table 2: Incident Criticality

Threat Intelligence

Trustwave Analysts utilize intelligence provided by Trustwave’s SpiderLabs to help identify emerging threats. SpiderLabs Research (SLR) collects Threat Intelligence telemetry daily from multiple sources both internally and through third-party relationships. Internal sources include direct research, multiple service-specific honeynets (web, email, remote services) as well as telemetry directly from Trustwave’s customer base.

SLR also maintains third party relationships and threat exchanges with organizations like Microsoft (MAPP partners), Google/VirusTotal, the Anti-Phishing Working Group (APWG), Facebook, Malicious URL Threat Exchange (MUTE), and Team Cymru. This Threat Intelligence directly feeds threat and trend research, signatures for various security product and service offerings, as well as for direct use for event correlation by Trustwave Analysts.

Trustwave Fusion Platform

The Fusion Platform provides the Client with access to the expertise of the SOC staff, security information and analysis, and the Trustwave Platform. As a Trustwave Managed Security Services (MSS) customer, Client will automatically be enrolled in Trustwave’s Fusion Platform. Access to the Fusion Platform provides:

• Designated Client contact information.
• 24x7x365 security event and security alert reporting available in the security activity area.
• Configuration templates software applicable to the Security and Compliance Management service.
• Change and support requests creation and management.
• Method for Client to securely communicate with the Trustwave provisioning and SOC personnel; and ability to upload documentation, security policies, and more with respect to your organization to ensure a smooth ongoing service.

Dependencies and Assumptions

• GTO Tiers and roles are described as follows:
  o The Trustwave SOC Tier 1 provides initial incident analysis (5-7 minutes on average per alert). This first line of escalation provides quick analysis of the incident, primarily leveraging solution for investigation. Clear threats are remediated, when possible. Investigated potential threats are escalated to Tier 2.
  o The Trustwave SOC Tier 2 (Advanced Analysis/Response) provides deeper analysis with most threats remediated by this point (30-45 minutes on average per alert). Tier 2 activities include accessing available information from other Client specific data sources, external data sources or captured malware to understand more clearly the nature of the attack and the potential danger to the Client.
  o The Trustwave SOC Tier 3 (Threat Management and Research) leverages Trustwave’s SpiderLabs team for advanced analysis if required (up to 6 hours). Tier 3 will leverage advanced capabilities (such as malware reverse engineering) to get to the heart of the threat. In some cases, the Client will be advised that a DFIR Consulting engagement will be necessary to combat the attack.
• The volume of events processed by the SIEM system is fully dependent on the scale of the Client’s implementation. Trustwave will provide support during transition to forecast capacity impacts and concerns regarding a Client’s environment.
• Trustwave will work with the Client in identifying the triage and escalation process for the use cases agreed to by Trustwave and the Client. Only escalated Findings and supporting data is sent from the Client SIEM to Trustwave.
Trustwave Analysts will require access to the Client’s SIEM implementation to perform triage and investigation when necessary. Once the Trustwave Analyst has identified a Finding to be escalated to Client, a ticket will be created in the Fusion Platform, and the Client will be notified.

The number of Findings (alerts) processed by the Trustwave SOC is limited to that documented in the pricing section. The SOC will measure the average number of Findings per day, averaged over the course of the month. If Findings volume exceeds 125% of the limit in any two consecutive months, Trustwave may increase its fee to cover the increase based on the rates specified. The Client can reduce the number of data sources, tune the number of events or alter the alerting use cases in order limit or eliminate the fee increase.

**Trustwave Responsibilities**

- Collect and monitor Log Data via the Fusion Platform
- Maintain availability of Threat Findings in the Fusion Platform.
- Generate notifications of Threat Findings via the Trustwave Portal.
- Investigate and analyze Threat Findings, help identify false positives and notify Client in the case of a suspected actual or potential Threat.
- Help identify and prioritize Incidents and notify designated Client personnel based on the priority of the incident and the appropriate response identified. Classify Incidents according to the categories defined.
- If needed, escalate the Incident based on its priority and according to the service level agreement (“SLA”).
- Maintain updated status of Incidents in the Fusion Platform.
- Generate and publish the relevant reports to the Fusion Platform.

**Client Responsibilities**

- Provide Trustwave Access to third party SIEM solution under agreement.
- Timely respond to escalated Incidents.
- Review reports published to the Fusion Platform.
- Notify Trustwave if Events or relevant reports are not available in the Trustwave Portal, as expected.
- Work with Trustwave to focus Alert Use Cases on urgent Threat Conditions requiring monitoring with a reasonable level of fidelity.
- Work with Trustwave to resolve each Incident by providing relevant personnel and ensuring support and engagement of third parties as required.
- Provide Trustwave with requested information and confirmations in a timely manner.
- Use and access the Fusion Platform to log tickets, receive notifications, view, download and track the status of and respond to, Threat Findings and Incidents.

**Security Technology Management**

**Co-Managed SIEM**

Co-Managed SOC service features ensure that the supported SIEM(s) are performing their function within the Client environment as designed. The service is provided as a co-managed model where both Client and Trustwave assume administrator access to manage the SIEM devices.

**Log Collection Appliance**

Trustwave Log Collector (“LCA”) resides on the Trustwave Connect Device. LCA is used to facilitate alert forwarding from Client’s SIEM solution to Trustwave’s cloud and is deployed and managed by Trustwave.
LCA is hosted by the Client or its designated cloud, virtualization or data center or by Trustwave in Trustwave data centers or cloud as the deployment warrants.

**Scope and responsibilities**

Trustwave shall not be responsible for the design, implementation, effect, or any damages, direct or indirect, arising out of or related to any Client changes made on a managed device under the co-managed model. Additionally, any warranties and SLA’s provided by Trustwave are not applicable to Client changes made on such managed devices.

Further Trustwave roles and responsibilities regarding SIEM technology management and log collection appliance can be found in the following:

<table>
<thead>
<tr>
<th>Type of SIEM Architecture Set-up</th>
<th>Applicable Service Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud-based SIEM Solution</td>
<td>Security Technology Management (Cloud)</td>
</tr>
<tr>
<td>On Prem SIEM solution and Log collection appliance</td>
<td>Security Technology Management (On Prem/Hybrid)</td>
</tr>
</tbody>
</table>

**Information Security Advisor (ISA)**

Trustwave Information Security Advisory (ISA) service provides access to security expertise and enhanced service management and leverages use of advanced tools and enhanced communication methods. Trustwave ISA service is instrumental in providing the world-class customer delivery that Trustwave is known for in its global MSSP Programs.

**Scope and responsibilities**

**SIEM Content Tuning and Management**

As part of a co-managed SOC program, the ISA resource will work with the Client in the ongoing tuning and extension of use cases in the SIEM focused on identifying potential attacker activity. The goal is to improve the efficiency of the use cases designed during the initial engagement with the Client. This includes the following activities:

- Data source volume expansion support
- Rule creation and tuning (around data sources onboarded to the SIEM during the transition project)
- Active log collection
- Disk and data storage availability and capacity

**Dependencies and Assumptions**

- SIEM rules will not be added/removed/changed without approval from a Client’s primary point of contact.
- Client may request or explore additional rule content.
- Trustwave will supply rule recommendations on available SIEM integrated data sources.
- Assigned resource is a shared resource.
- The addition and integration of new data types and technologies, design or updated SIEM content to integrate that data source is not provided by ISA.

Further Trustwave ISA roles and responsibilities can be found at:

<table>
<thead>
<tr>
<th>Service</th>
<th>Applicable Service Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security Advisor – ISA50</td>
<td>Information Security Advisor</td>
</tr>
</tbody>
</table>
Definitions

**Log Collector** means a Trustwave device that automates the collection, storage, and management of Log Data.

**Event** is a normalized record of Log Data, detailing a message, record, alert or audit from a Log Source.

**Incident** means a notification to the Client to a detected threat.

**Log Data** means a record received from a Log Source.

**Threat Findings** are potential security concerns detected by Trustwave systems and Analysts.

**Trustwave Connect Device** is a physical, virtual, public-cloud or Trustwave-hosted device used to house certain features of the Service.

**Trustwave Platform** means the Trustwave managed security service infrastructure utilized in providing the Service.