SERVICE DESCRIPTION

Threat Detection & Response: Co-Managed SOC

Service Scope

Trustwave’s Threat Detection & Response: Co-Managed SOC service (the “Service”) offers Client threat detection services operating in conjunction with its own SIEM/SOC infrastructure. The Service includes the following:

- Transitional project consulting and provisioning to plan, build, and optimize threat detection and response solutions to steady state.
- Investigation into high fidelity alerts on Client’s SIEM/SOC, enrichment of the use of other telemetry integrated into the SIEM/SOC, determination of a final actionability disposition and appropriate response escalations.
- SIEM maintenance, tuning, and use case implementation.
- Access to a Trustwave Information Security Advisor (ISA) for ongoing management and maintenance of the co-managed SOC environment, including guidance on maturing system and process capabilities.

Threat Detection & Response Consulting

SIEM Jumpstart

The Service includes a required on-boarding process (“Jumpstart”). Jumpstart relates to supported SIEM technologies and includes the sub-services listed in the table below (depending on which version of Jumpstart is applicable). A maturity and capabilities assessment may be included in the Service and helps Clients measure and optimize their SIEM capabilities. This, in turn, helps Client to better define its cybersecurity posture and enhance its strategy and vision to build and scale a best practice, cybersecurity operations program. As a part of Jumpstart, Trustwave will also verify alert volumes received from Client to determine if such volumes are within defined limits before moving to steady state. Client will clearly identify the use cases that are to be forwarded to Trustwave’s Global Threat Operations (GTO) team for analysis.

The following table summarizes the differences between Jumpstart and Jumpstart Lite (our cost-efficient variant):

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

Please refer to the applicable Statement of Work or Order Form for our full descriptions for Jumpstart and Jumpstart Lite.

**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 put strain on Client’s capacity and time. The optional Threat Detection & Response (TDR) Agility Program provides Client with access to our SOC consulting teams’ engineering skills and experiences.

Trustwave and Client will establish a phased project plan over the duration of the Service to advise, design, and drive new use cases, technologies, and processes to proactively adapt to Client’s business.
Trustwave will provide the following as first-time drafts or updated versions each quarter:

- 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*

* The TDR Agility Program represents 640 hours of labor per year (typically 160 hours per quarter) and will be deducted from Client’s subscription accordingly.

Please refer to the applicable Statement of Work or Order Form for our full descriptions for TDR Agility Program.

**Threat Detection & Response – Global Threat Operations**

Trustwave’s TDR Global Threat Operations service (the “GTO Service”) allows Client’s SIEM ruleset to generate alerts that Trustwave’s GTO analysts may investigate, enrich, and determine appropriate escalation priorities for. GTO analysts will monitor such events and alerts 24x7x365 and will provide GTO Tier 1 analysis and investigation (as described below) and escalate events to GTO Tier 2 as needed.

**Scope and Responsibilities**

In the GTO Service, GTO analysts will utilize Trustwave’s threat intelligence footprint to enrich Client SIEM’s output, as needed. 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 and displayed in the Fusion Platform for additional investigation by Client and Trustwave. Initial triage and analysis is based on these alerts.
- When Trustwave deems necessary, GTO analysts will investigate events and alerts in the local SIEM environment directly to access more detailed or contextualized information. All base log events will remain in the SIEM instance.
- GTO analysts will review the generated alerts, collected events, and activity trends to identify suspicious behavior in the environment. If GTO analysts find suspicious activity, they will generate a ticket in the Fusion Platform, and Client will be notified by email, via the Fusion Mobile App, or by phone through the incident response process defined with the Client during the onboarding phase. The ticket information is available in the Fusion Platform.
GTO analysts will categorize the alerts and will notify Client of those alerts which are determined to be a potential security threat and are of a high or critical severity. GTO analysts may follow up by phone, following the incident response process defined with the Client during the onboarding phase. Trustwave will categorize incidents and notifications based on the priority levels 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 (Sev1)</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 Client’s environment. Investigations that result in this priority require immediate action to contain the threat.</td>
</tr>
<tr>
<td>High (Sev2)</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 (Sev3)</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 (Sev4)</td>
<td>Email</td>
<td>Informational Only</td>
<td>Incidents at this level are not immediately actionable and may require further investigation by the client to determine possible actions.</td>
</tr>
</tbody>
</table>

Table 2: Incident Criticality

Threat Intelligence

GTO analysts utilize intelligence provided by Trustwave 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), and 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 information directly feeds threat and trend research, signatures for various security product, service offerings, and direct use for event correlation by GTO analysts.
Trustwave Fusion Platform

Client has access to the expertise of Trustwave’s SOC staff and its own security information and analysis through the Trustwave Fusion Platform. As a Managed Security Services (MSS) customer, Client will be automatically enrolled in the Fusion Platform. Additionally, Client will have access to the following on the Fusion Platform:

- 24x7x365 security event and security alert reporting available in the security activity area.
- Ability to submit requests for change support and management.
- Multiple methods for Client to securely communicate with Trustwave and the ability to upload documentation, security policies, and more.

Dependencies and Assumptions

- GTO Tiers are described as follows:
  o **GTO Tier 1:** This tier provides initial incident analysis, primarily by leveraging SIEM data for investigation. Clear threats are remediated, when possible. Investigated potential threats are escalated to Tier 2.
  o **GTO Tier 2:** This tier provides deeper analysis. Most threats are resolved at this level. 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 Client.
  o **GTO Tier 3:** This tier leverages Trustwave SpiderLabs for advanced analysis. Tier 3 relies on 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 Digital Forensics & Incident Response consulting engagement may be necessary to combat the attack.

- The volume of events processed by the SIEM system is fully dependent on the scale of Client’s implementation of such SIEM system. Trustwave will provide support during Client’s transition to Trustwave-managed SIEM support to forecast capacity impacts and concerns regarding Client’s environment.
- Trustwave will work with 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 will be sent from the Client SIEM to Trustwave.
- Client will provide access to Client’s SIEM implementation for GTO analysts to perform triage and investigation.
- The number of findings (alerts) processed by the Trustwave SOC is limited to that documented in the pricing section of the relevant SOW between Client and Trustwave. Trustwave will work with Client to maintain a finding volume within such limitations, however, if the volume of findings forwarded to Trustwave for real time monitoring exceeds 125% of the contracted limit in any two consecutive months and Trustwave and Client are not able to reduce the volume effectively through prioritization, tuning and optimization, Trustwave may increase its fee to cover the increase based on the rates specified.

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 Fusion Platform.
- Investigate and analyze threat findings, help identify false positives, and notify Client 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 in Table 2: Incident Criticality.
- If needed, escalate the incident based on its priority.
- Maintain updated status of incidents in the Fusion Platform.
- Generate and publish reports to the Fusion Platform as may be agreed with Client.
Client Responsibilities

- Provide Trustwave with access to third party SIEM solution relevant to the Service.
- Review event and threat activity in the Fusion Platform.
- Timely respond to escalated incidents.
- Review reports published to the Fusion Platform.
- Notify Trustwave if Client is unable to access events or reports.
- 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, track the status of, and respond to threat findings and incidents.

Security Technology Management

Co-Managed SIEM

The Service monitors the supported SIEM(s) to determine whether they are functioning as intended. The Service is provided as a co-managed model where both Client and Trustwave assume the role of administrator and manage the SIEM devices.

Log Collection Appliance

The Trustwave Log Collector (LCA) resides on the Trustwave Connect Device, our proprietary platform for collecting logs and accessing Client’s technologies. The LCA is used to facilitate alert-forwarding from Client’s SIEM solution to Trustwave’s cloud and is deployed and managed by Trustwave. The 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.

Further information on our Security Technology Management services can be found in the following services descriptions, available at https://www.trustwave.com/en-us/legal-documents/contract-documents/:

<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)

The Trustwave Information Security Advisory (ISA) service offers Client access to security expertise and enhanced service management through the availability of advanced tools and enhanced communication methods.

Scope and Responsibilities

SIEM Content Tuning and Management

When combined with the Service, an ISA will work with Client in the tuning and extension of use cases in the SIEM, focused on identifying potential attacker activity. An ISA and Client will work 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, or 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 ISA 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 included in the ISA service.


<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>

Capitalized terms used but not defined in this service description have the meaning given to them in the Trustwave Master Services Agreement found at https://www.trustwave.com/en-us/legal-documents/contract-documents/ or a similar agreement signed between Trustwave and Client.