MDR ESCALATION PROCESS

HOW US SIGNAL ENGAGES WITH MDR CUSTOMERS

US Signal's Managed Detection and Response (MDR) service is designed to augment the capabilities of overstretched IT / Security teams.

US Signal's MDR service pairs an industry leading EDR platform (Sentinel One) along with the US Signal Security Operations Center to deliver around the clock protection for your organization from evolving cyber threats. The US Signal Security Operations Center is staffed with qualified analysts that ensure that every threat is reviewed, acted upon, documented, and escalated as needed. This ensures that no critical detection is missed and urgent matters that require further intervention are escalated to you as needed.

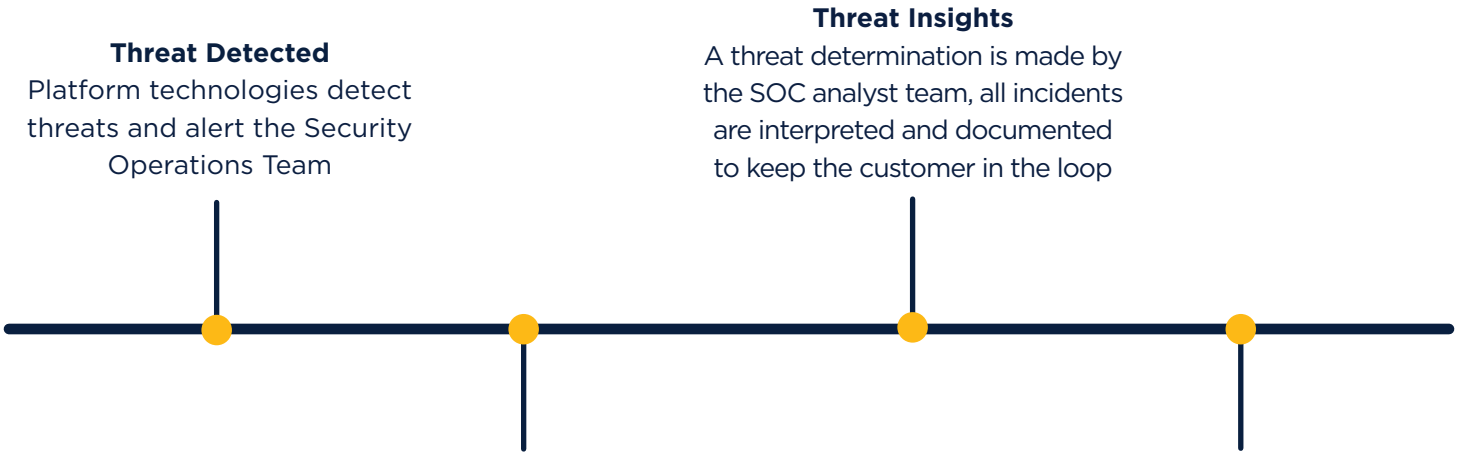
Need more info?

Contact US Signal's Soc!

secops@ussignal.com | 616.233.5701

US SIGNAL MDR: FROM DETECTION TO RESOLUTION

The US Signal Security Operations Center uses a documented, controlled process to work through incidents to ensure focused attention is placed into what is most important.



Threat Detected
Platform technologies detect threats and alert the Security Operations Team

Analyst Deep Dive
Threats are surfaced to SOC analysts, combined with enrichment data where applicable

Threat Insights
A threat determination is made by the SOC analyst team, all incidents are interpreted and documented to keep the customer in the loop

Action + Next Steps
US Signal mitigates and resolves the threat where necessary and opens proactive escalation communications as needed

THREAT HANDLING HIERARCHY

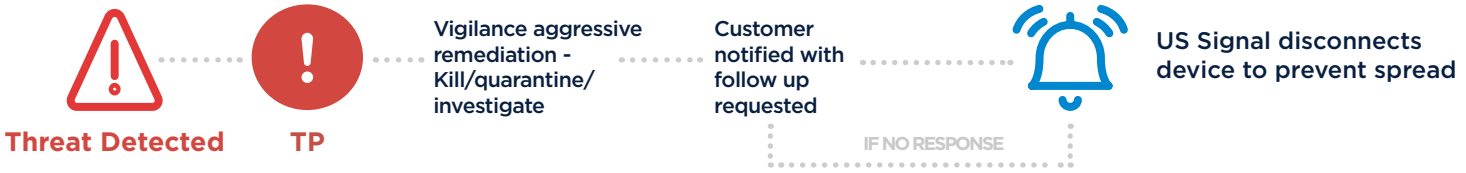
Appropriate actions and resolutions are made by US Signal analysts depending on the situation's severity. All threats receive some level of response / follow up. From Benign to Urgent True Positive threat classification, this is what you can expect:

Benign Alert - False Positive

Malicious Alert (TP/PUP) - True Positive PuP / No Action Needed

Malicious Alert (TP) Non-Urgent - Action Needed

Malicious Alert (TP) Urgent - Action Needed



THREAT HANDLING HIERARCHY DEFINITIONS

BENIGN ALERT (FP)

Alert is classified as Benign False Positive

US Signal takes proper action to resolve and annotate the console. No further actions or notifications are needed. Recurrent False alerts will be escalated to the customer to offer or approve an appropriate exclusion or agent upgrade as needed.

MALICIOUS ALERT (TP/PUP) – NO ACTION NEEDED

Alert is classified as a Malicious True Positive / No Action or Potentially Unwanted Program

US Signal takes proper action to ensure that the threat is block listed, resolved, and documented, as well as isolation and remediation steps as applicable. The analyst will communicate the incident details to the customer with no further action required.

MALICIOUS ALERT (TP) - NO ACTION NEEDED

Alert is classified as Malicious True Positive / No Action

US Signal takes proper actions including Remediation to ensure the threat is isolated. Once the Analyst confirms that remediations eliminate the threat, the Analyst will send a notification to the customer's email alias alerting them to the incident as a courtesy.

MALICIOUS ALERT (TP) NON-URGENT - ACTION NEEDED

Alert is classified as Malicious True Positive Non-Urgent / Action Needed

US Signal takes proper actions including Remediation to ensure the threat is isolated. Once the Analyst confirms that remediations eliminate the threat, the Analyst will send a notification to the customer's email alias alerting them to the incident as a courtesy. Follow up actions such as re-imaging may be recommended in some cases.

MALICIOUS ALERT (TP) URGENT - ACTION NEEDED

Alert is classified as Malicious True Positive Urgent / Action Needed

US Signal may take aggressive actions in high priority breach cases including agent Remediation actions and disconnecting affected network* devices to isolate the attack and prevent further lateral movement and spread. The Analysts will send a Proactive Notification alerting the customer to the situation and request immediate Response.

NO RESPONSE

If there is no response from the customer related to a Proactive Ticket, especially one classified as Urgent - Action Needed, the Analyst may attempt further customer contact via a ranked set of contact telephone numbers and backup email addresses.

**In urgent cases, US Signal will disconnect machine(s) before approval from the customer due to the risk to the organization.*

THE US SIGNAL DIFFERENCE

US Signal provides industry-leading data center technologies, cloud solutions and managed services to help companies transform their IT operations and meet ever-changing technology and business needs. Drawing from a portfolio of colocation, IT infrastructure, endpoint monitoring, data management, disaster recovery and security services, US Signal's data center solutions can meet even the most unique or complex technical requirements.

info@ussignal.com | 866.2.SIGNAL

US SIGNAL®