Alert Severity Levels

At Lumifi, we categorize security alerts into three distinct tiers based on their severity and impact. Understanding these tiers helps us prioritize and respond to security incidents effectively.

Tier 1 - High

These notifications are immediate calls to the organization. The Lumifi team has determined that this activity requires immediate action by the organization due to a confirmed malicious action. The security incident has immediate consequences for the organization. This can involve a loss of data or a privacy breach, or at the very least, it indicates that a threat actor has gained access to the organization's assets. These occur far less frequently than tier 2 normal notifications.

Tier 2 - Normal

These notifications are emails to the organization. The Lumifi team has determined that this requires the organization's intervention to determine its true severity. These are unusual events that are being observed by the Lumifi team, which can affect the organization but may also be expected actions by the assets in question. We require insight from the customer to determine whether this is a known event or if an asset is engaging in malicious activity that is not approved. These occur less frequently than Tier 3 but typically constitute the majority of notifications for the organizations we support.

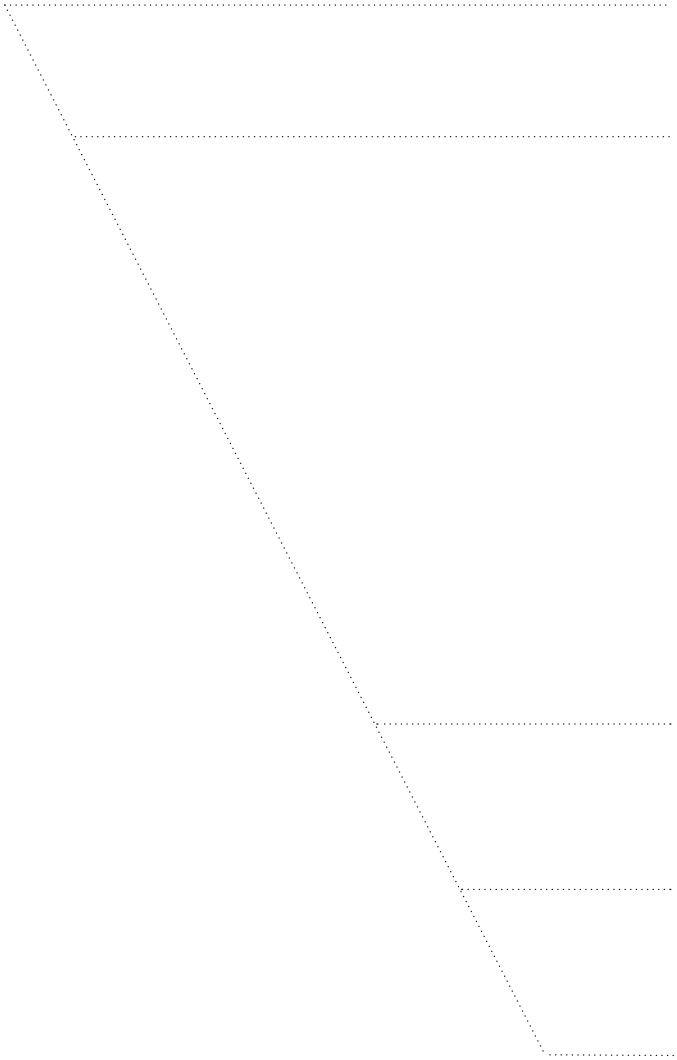
Tier 3 - Low

These are not sent to the organization but are marked as tickets that the Lumifi team has investigated. The Lumifi team has determined that the action is expected and benign, requiring no further organizational intervention. It is simply logged to indicate that we observed the activity but determined it to be expected. These constitute the majority of investigations and alerts.

1475 N Scottsdale Rd STE 410
Scottsdale, AZ 85257

877.388.4984
lumificyber.com

SOC Escalation Documentation



1. Create a Ticket in ZenDesk

Call into the SOC at 623.624.3335
Email soc@lumifi.zendesk.com

2. Reach out to CSM Team

Morgan Folk | Renewals Specialist
mfolk@lumificyber.com | 610.513.1019

Keegan Lass | Account Executive
klass@lumificyber.com | 563.320.7744

Suethi Tham | Account Executive
stham@lumificyber.com | 952.215.5458

Aaron Daniels | Channel Manager
adaniels@lumificyber.com | 402.610.6192

Chris Williams | Sr. Technical Account Manager
cwilliams@lumificyber.com | 727.744.3042

Calieb Simmons | Technical Account Manager
csimmons@lumificyber.com | 832.248.3687

Travis Goddard | Technical Account Manager
tgoddard@lumificyber.com | 402.578.8187

3. Contact SOC Manager

Sean Hanson
508.850.6151
shanson@lumificyber.com

4. Contact SOC Director

Johnathon Miller
480.620.6860
jmiller@lumificyber.com

5. Final: Escalate to CISO and CTO

Grant Leonard | Field CISO
gleonard@lumificyber.com
919.949.4002

David Norlin | CTO
dnorlin@lumificyber.com
765.721.3027

1475 N Scottsdale Rd STE 410
Scottsdale, AZ 85257

877.388.4984
lumificyber.com