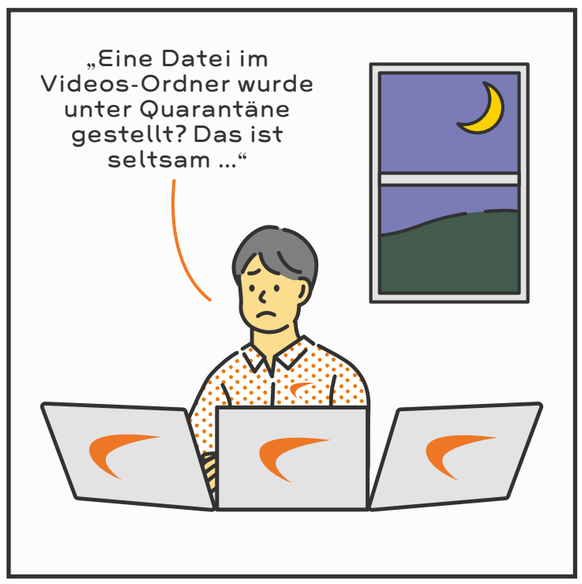
SOC in Aktion: Der Lebenszyklus einer Cyberbedrohung

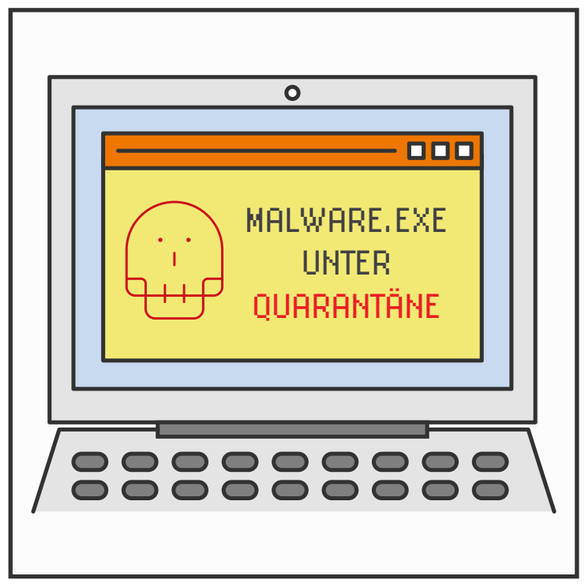
Das Security-Operations-Center (SOC) von SonicWall schützt seine Kunden 24 Stunden am Tag, 7 Tage die Woche. Wenn eine Warnung oder Bedrohung beim SOC eingeht, schreitet das Team sofort zur Tat. Wir zeigen Ihnen wie.

Das Security-Operations-Center von SonicWall beobachtet Warnungen und ungewöhnliches Verhalten rund um die Uhr, um die MSP-Partner und ihre Kunden vor Cyberbedrohungen zu schützen. Wenn Warnungen von Sicherheitstools eingehen, untersucht ein SOC-Analyst diese.

Warnungen werden als einfach, wichtig oder kritisch eingestuft. Das SOC-Team legt Regeln und Konfigurationen für die automatische Klassifizierung der Warnungen fest und der SOC-Analyst kann die Warnung dann je nach Bedarf hoch- oder herunterstufen.



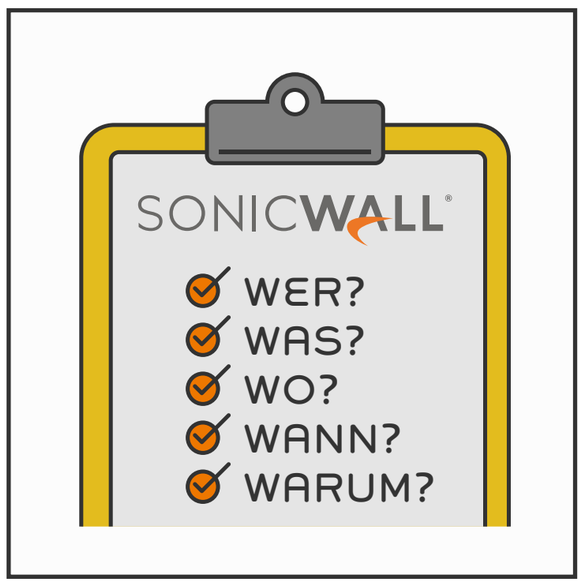
Einfache Warnungen werden für ungewöhnliche Aktivitäten auf Endpunkten verwendet, z. B. wenn Dateien in ungewöhnlichen Ordnern unter Quarantäne gestellt werden. Das sind sehr oft falsch positive Warnungen. Das SOC setzt sich per E-Mail mit Ihnen in Verbindung, wenn weitere Untersuchungen angebracht wären.



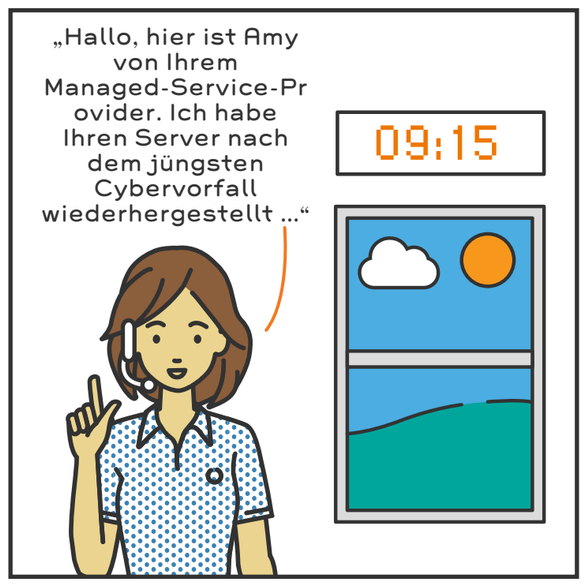
Wichtige Warnungen werden verwendet, wenn es Anzeichen für bösartige Aktivitäten auf dem Endpunkt gibt. Diese Aktivitäten werden häufig durch Sicherheitstools gestoppt, z. B. wenn Malware automatisch von einem Antivirenprogramm der neuen Generation unter Quarantäne gestellt wird. Das SOC setzt sich per E-Mail mit Ihnen in Verbindung und gibt Ihnen Empfehlungen für weitere Maßnahmen, z. B. zusätzliche Phishing-Schulungen für Endbenutzer.

Wenn mit hoher Wahrscheinlichkeit ein Sicherheitsvorfall oder eine Kompromittierung aktiv erfolgt, ergibt das eine kritische Warnung. Das SOC-Team schaltet sich ein, um den Schaden schnell zu minimieren und zu verhindern, dass sich die Kompromittierung weiter in Ihrem Netzwerk ausbreitet.

Bei einer kritischen Warnung ruft das SOC-Team die von Ihnen angegebene Notrufnummer in der ersten Stunde alle 15 Minuten an, danach stündlich, wenn es Sie nicht erreicht. Das Team wartet jedoch nicht auf Ihre Antwort, um die Initiative zu ergreifen, sondern leitet sofort alle erforderlichen Maßnahmen ein, um den Angriff zu stoppen und Ihre restliche Umgebung zu schützen, normalerweise durch Isolierung der Endpunkte.



Der SOC-Analyst erstellt einen Bericht, um den Vorfall, das Ausmaß und alle anderen betroffenen Bereiche zu dokumentieren. Das SOC spricht auch Empfehlungen für Ihre nächsten Schritte aus.



Nachdem die aktive Bedrohung beseitigt wurde, können Sie mit Ihrem Kunden zusammenarbeiten, um das Netzwerk zu reparieren, isolierte Endpunkte wiederherzustellen und alle anderen erforderlichen Gegenmaßnahmen zu ergreifen.