Alert fatigue is a well known problem in cybersecurity. Many organizations are flooded with so many security notifications, they are at significant risk of missing actual threats.

Tanium Threat Response gives organization threat hunting, security operations, and incident response teams the deep visibility to surface valuable security endpoint data and telemetry.

Events are generated, providing security teams with various insights into their environment, including risky behavior, suspicious usage, vulnerabilities, misconfigured settings, as well as serious indications of compromise. A client with no previous visibility on enterprise-wide endpoint security data may be overwhelmed with the thousands of new insights they receive from Tanium.

Recently, Chuco helped a client reduce the volume of security events they were receiving from Tanium Threat Response.

The client, a large business unit within one of the world's largest multinational corporations, had been receiving over 10,000 event alerts a day.

The good news is that you can tune your security events to dial down the "noise" and make it easier to identify relevant threats. We helped our client reduce the number of events to between 10 and 50 a day by filtering out benign behaviors and low priority items.

A Multi-Phase Iterative Approach

How did we do it? We followed a multi-phase iterative method to test and tune the types of alerts the client was receiving from Tanium.

The Tanium Event Recorder collects very valuable data – every process, every file change, and every modification on the system is captured. Tanium Signals then applies intelligence to let you know when anomalies happen, so you can investigate for possible attacks, breaches, misconfigurations and other vulnerabilities.

The challenge for IT and security teams is to prepare so that they aren't immediately overwhelmed by the alerts that are generated.

Creating a test environment to confirm that the intelligence is useful is the best way to start. It gives you a chance to identify any benign behavior in your environment that may initially trigger false positives.

For example, there may be actions your sysadmins perform periodically which should be filtered out.

Many clients have asked whether AI and machine learning can be used to separate the signals from the noise. While much progress has been made in applying machine learning to identify potential security threats, AI is only as smart as people teach it to be.

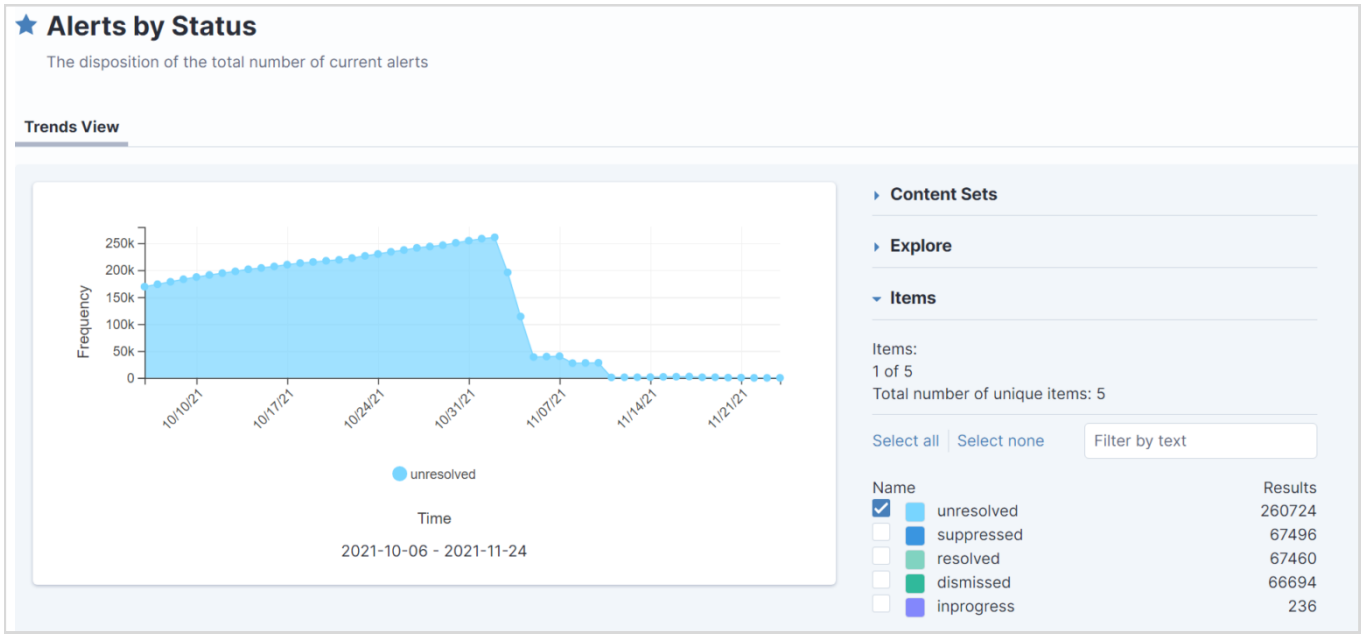
So for trying to prevent novel sophisticated attacks, if the AI isn't learning the right algorithms, it could end up making your defenses weaker.

By and large, it still makes sense to adopt new security innovations like AI, but you also need to have the human touch from experienced professionals to ensure AI isn't causing security problems instead of solving them.

A Typical Engagement

In a typical Chuco engagement, we work with clients to understand their business risk profile and evaluate the alerts they are receiving in the test environment to sort the low priority or benign activity from the high priority and potentially malicious.

As consultants, we familiarize ourselves with your unique security environment and ask questions so we understand what's "normal" and what's not. We get to know approved host names, approved software, and the typical schedule of machines in your system. We also get to know the approved users, and how User A in your network behaves versus User B.



Once an assessment has been made of each alert, we take one of several actions: set labels, suppress the alert, remove it entirely, modify and tune it, or promote the alert to the next phase of testing.

After that, it's a case of rinsing and repeating through another phase. Once you're confident that the alerts and events you're receiving are identifying issues that require further investigation, you're ready to push out the configurations system-wide in a production environment.

Prioritizing Alert and Event Types

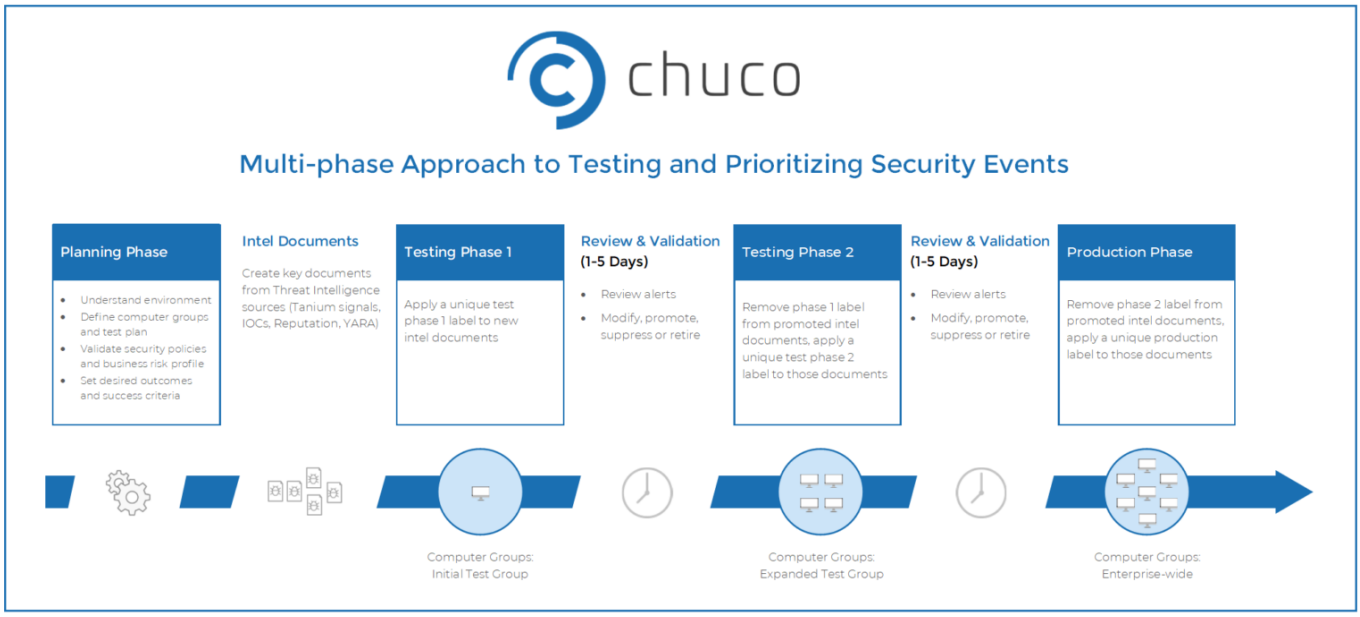
Of course, it's helpful if your CISO and/or the security ops or threat response team is able to define up front what types of activities they want to receive alerts on, such as suspicious behaviors, specific campaigns of malware, or a specific compromise called to their attention by the FBI.

Or, they may ask for general alerts on anything related to crypto mining or exfiltration of data. In some cases, we also have had clients who are mainly looking for HIPAA or SOC2 compliance alerts, so that they can fulfill their compliance obligations.

At Chuco, we can work with you to create and update customized alerts based on new attacks being reported in the wild, or based on company policy and/or priorities, as well as import known indicators of compromise.

People, Processes and Technology

Regardless of your priorities, it's essential to have processes in place to ensure that each type of alert is assigned to an analyst or other individual whose role it is to investigate and take mitigating steps as needed.



We've supported smaller organizations where each team member is wearing multiple hats – as well as larger organizations with dedicated teams focusing on threat hunting, alerts and policy, plus engineering and devops teams who contribute to security operations. Chuco experts can work with you to define roles and establish processes, and offer additional support around Tanium if needed.

The advantage of getting your Tanium security alerts under control is that you can make the most of Tanium Threat Response and quickly identify potential attacks, vulnerabilities and malicious insider behavior.

Furthermore, it makes your team more efficient – so that they're not burdened with having to manually sort through an inbox full of false positives.

Configuring Tanium Threat Response and keeping on top of updates can require a significant investment of time and attention to detail.

Contact Chuco if you need help with tuning and maintaining your security alerts — taking into account the people, process and technology considerations particular to your environment.