REFERENZBERICHT

BAE Systems verschafft sich Visibilität in Endpunkte, reduziert Risiken und schützt vor Sicherheitsbedrohungen

BAE SYSTEMS

Branche
Luft- und Raumfahrt, Rüstungsindustrie, Informationssicherheit

Größe
90.500 Mitarbeiter

Hauptsitz
London, Vereinigtes Königreich

Tanium-Produkte
Discover, Asset, Patch, Deploy, Comply

Die Herausforderung

Applied Intelligence, ein Unternehmen von BAE Systems, das heute als Digital Intelligence bekannt ist, benötigte Visibilität in seiner Flotte von Laptops, virtuellen Maschinen (VMs) und anderen digitalen Endpunkten. Die Führungskräfte der Gruppe wussten, dass sie Unsichtbares nicht schützen können.

Digital Intelligence hatte Tausende Geräte, die es auf potenzielle Schwachstellen scannen wollte. Mit diesen Informationen wisse das Team, ob einer seiner Endpunkte anfällig für Ransomware, Computerviren und andere feindselige Angriffe sei. Die IT- und Sicherheitsteams suchten auch nach einer effektiven Möglichkeit, infizierte Systeme bei einem Angriff in Quarantäne zu stellen oder anderweitig zu beheben.

> „Ohne die Transparenz, die Tanium bietet, wären wir nicht in der Lage, uns mit den allgegenwärtigen Sicherheits-bedrohungen auseinanderzusetzen."
>
> **Tom Barker**
> Chief Security Officer bei BAE Digital Intelligence

Die Lösung von Tanium

Das Team von BAE Digital Intelligence hat zum Erreichen dieser Lösung Tanium eingeführt. Tanium wurde 2007 gegründet und bietet Softwarelösungen, die nicht verwaltete Endpunkte finden, nach Schwachstellen suchen, kompromittierte Geräte verwalten und steuern – und vieles mehr erreichen können. Die Lösungen von Tanium werden von der Hälfte der Fortune 100, acht der zehn größten Finanzinstitute und fünf Teilstreitkräften des US-Militärs verwendet.

Die Implementierung von Tanium unterstützten technische Account Manager (TAMs), die eng mit den IT- und Sicherheitsteams von Digital Intelligence zusammenarbeiteten. Gemeinsam installierten sie die Tanium-Plattform, schulten Mitarbeiter in der Nutzung und führten Berechnungen mit den von der Tanium-Software generierten Zahlen durch."

„Die Unterstützung der technischen Account Manager von Tanium war für unseren Erfolg unerlässlich“

Simon Whibberley
Leiter Engineering Operations bei BAE

Ergebnisse und Vorteile

Der erste Scan mit Tanium identifizierte mehrere potenzielle Schwachstellen, darunter veraltete Patches, offene Ports usw. Innerhalb weniger Monate nutzte das Team Tanium und reduzierte diese Schwachstellen signifikant. In den folgenden Monaten verringerte das Team die Anzahl der verbleibenden Schwachstellen weiter, sodass der Risiko-Schwellenwert des Unternehmens eingehalten wird. „Obwohl die Anzahl der von uns eingesetzten Endpunkte gestiegen ist und wir gegen eine kontinuierliche Flut neu veröffentlichter CVEs [häufige Schwachstellen und Sicherheitslücken] kämpfen, sind insgesamt unsere Schwachstellen und unsere Risikolage niedrig geblieben“, so Whibberley.

BAE Digital Intelligence profitierte auch von den enormen Einsparungen beim Zeitaufwand. Vor der Implementierung von Tanium erstellte das Team von Digital Intelligence einen monatlichen Bericht über potenzielle Cyber-Schwachstellen. Die Berichterstellung erfolgte manuell, was mehr als zwei Wochen pro Monat dauerte. Nach der Implementierung von Tanium wird der Schwachstellenreport automatisch generiert und wöchentlich bereitgestellt.

Dank Tanium arbeitet das Unternehmen sicherer und effizienter. Bei Identifikation eines anfälligen Endpunkts wird der Eigentümer des Geräts aufgefordert, das Problem in der festgelegten Anzahl an Tagen zu beheben. „Jetzt sind die Benutzer dafür verantwortlich, die VMs mit Patches auf dem neuesten Stand zu halten“, sagt Whibberley.

Das war eine echte Veränderung der Unternehmenskultur für das BAE-Team. „Unsere Ingenieure und IT-Mitarbeiter sind sicherheitsbewusst, aber zunächst sahen sie die speziellen Vorteile für sie nicht“, erklärt Barker. Mit Tanium können sie nun einzelne Systeme detailliert betrachten. Diese Art granularer Daten zeigt Einzelnen die Gründe für die Relevanz. „Dank Tanium bilden wir aus den Punkten eine rote Linie und können unsere Sicherheitslage wirklich verbessern“, ergänzt Barker.

Als zukünftige, gerade in der Entwicklung befindliche Fähigkeit soll es dem IT-Team möglich sein, ein System mit Tanium unter Quarantäne zu stellen, damit alle potenziell kompromittierten Geräte daran gehindert werden, Schadsoftware über das Netzwerk des Unternehmens zu verbreiten. Auf diese Weise haben die IT- und Sicherheitsteams nicht nur eine bessere Visibilität in ihre Endpunkte, sondern können diese auch verwalten.