ultraviolet

MANAGED DETECTION AND RESPONSE (MDR)

Simply generating alerts is not enough to thwart your adversaries. For true protection, shift to focusing on outcomes... at machine-speed!

BROAD VISIBILITY

UltraViolet MDR integrates with existing technology investments from firewalls, IDS to host data sources like EDR. With particular focus on our comprehensive log analytics platform, all relevant information systems, networks, IoT, cloud (AWS, GCP, Azure, etc.) and/or applications (web, mobile, etc.) are ingested into a comprehensive security data lake.

RELENTLESS HUNTING

The window to find your adversary before they spread in your organization is very narrow. UltraViolet's cloud native MDR takes full advantage of the power of the cloud by scaling out thousands of concurrent queries to bring down the Mean Time to Detection.

ULTRAVIOLET PLATFORM

UltraViolet Cyber Platform delivers cloud focused adversary simulation, detection and prevention services. Uncover attackers and vulnerabilities with our robust security data lake that uses microservice to apply security analytics, Red Team-as-Code, Detections-as-Code, and threat intelligence.

INNOVATION & EDUCATION

ELIMINATE ALERT FATIGUE

While others filter event ingestion to reduce costs, our solution embraces the security data lake concept and ingests all relevant data to quickly mines for atomic indicators while running over 3,000+ complex behavioral hunt detections across your entire data set every 3 minutes. We enrich all events with SOAR integrations to refine alerts for comprehensive and actionable alerts.

SIEM MANAGEMENT

Our SIEM agnostic Detections as Code library enables a flexible deployment strategy which enables us to integrate and manage your existing SIEM (Splunk ES, Azure Sentinel, Elastic, etc.) with our SOAR platform, OR replace your SIEM entirely using our proprietary UltraViolet Cyber Platform. UltraViolet provides deeper insights into your security data to uncover the adversary not just produce alerts.

OUTCOMES NOT ALERTS

It is not enough to simply receive true positive alerts, but to mitigate your risk, you need to respond to those alerts—therefore, UltraViolet focuses on outcomes and not simply generating alerts. UltraViolet has decades of expertise designing and operating SOCs for the U.S. Federal Government as well as fortune 500 companies. With our Security Orchestration and Automated Response (SOAR) playbooks and integrations—we put the R in MDR!

MDR IS NO LONGER A LUXURY

MDR Key Features

$6.2M

AVERAGE COST OF COMPROMISED CLOUD ACCOUNTS

3,000+

DETECTIONS AS CODE

51%

BUSINESSES HIT WITH RANSOMWARE IN 2020

<48 HOURS

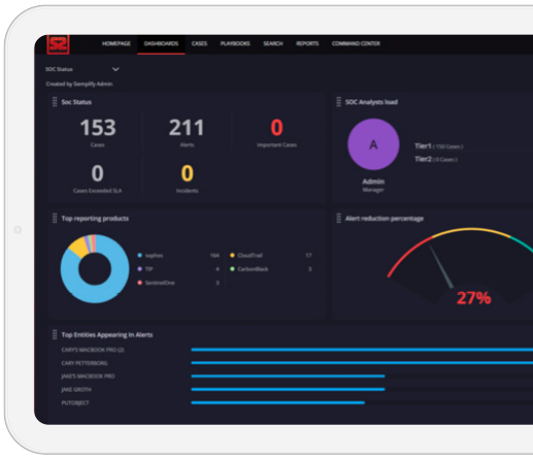
TIME FROM EXPLOITATION TO DETECTION

CLOUD NATIVE PLATFORM W/AUTOMATION

Our cloud native platform starts with observability. We ingest and transform any machine data (Cloud, SaaS, EDR, firewalls, IDS, etc.) from digital exhaust to insights. Our Detections engine married to our SOAR platform automatically generates and refines the alert with threat intelligence and our cyber warriors corroborate the incident to recommend and act.

DETECTIONS AS CODE

A true microservices approach weaponizes thousands of detections by scaling out how many concurrent queries can be made on an ongoing basis. This “Detections as Code” process enables us to find that initial penetration before the adversary has a chance to spread. We ensure that we will have a Detection written to deploy for every critical CVE within 48 hours.



MDR KEY BENEFITS AT A GLANCE

REAL WORLD EXPERTISE

UltraViolet is comprised of industry experts having implemented and operated SOCs for DHS and other security focused U.S. Government Agencies. Coupled with our NSA offensive pedigree we know the adversary because we used to be the Adversary.

SECURITY PARTNER NOT SERVICE PROVIDER

We partner with our clients to deliver secure outcomes. We don’t hide behind SLAs or service descriptions. We work with you to understand your environment and maximize detection capabilities that improve your cyber resilience.

RELENTLESS HUNTING

If you have to pay extra for hunting, what is it that your MDR is doing? UltraViolet MDR provides relentless hunting of your security data lake to uncover the attackers and not just the alarms they know you know about.

ABOUT ULTRAVIOLET

ultraviolet

UltraViolet Cyber is a leading platform enabled unified security operations company providing a comprehensive suite of security operations solutions. Founded and operated by security practitioners with decades of experience, the UltraViolet Cyber security-as- code platform combines technology innovation and human expertise to make advanced real time cybersecurity accessible for all organizations by eliminating risks of separate red and blue teams. By creating continuously optimized identification, detection and resilience from today’s dynamic threat landscape, UltraViolet Cyber provides both managed and custom-tailored unified security operations solutions to the Fortune 500, Federal Government, and Commercial clients. UltraViolet Cyber is headquartered in McLean, Virginia with global offices across the U.S. and in India.

443.351.7630 / info@uvcyber.com / @uv_cyber / UltraViolet Cybersecurity