24/7 ZEROTHREAT X/MDR

SOC As A Platform

Our latest ZeroThreat prevention-first solutions is at your finger tips with this platform, and you can convert your organization to an MSSP just by adopting it

SECURITY OPERATIONS CENTER AS A PLATFORM:

24/7 MANAGED DETECTION, RESPONSE AND REMEDIATION

[CODE NAME // SOCAAP]

The world's first SOC-as-a-Platform that combines people, process, and technology to deliver a completely outsourced SOC with remediation at the endpoint for less than most EDR and MDR products. Comodo SOCaaP is fully managed by our industry certified security experts around the clock. Their collective goal is to reduce attacker dwell time from hours, days, weeks or even months to zero seconds, to pre-emptively protect your endpoints. The service is a fully managed defense-in-depth solution. Event processing/environment hardening, and coordination with global threat intelligence is included. This platform provides you with visibility of the threat landscape and indicators of compromise (IOCs) on the external horizon. **This platform package includes ZeroThreat virtualization, breach protection, managed detection and attack/threat analysis, threat hunting, and response.**

These services employ Xcitium security analysts 24/7/365 who are performing deep analysis of detected events, and when required, working with clients to patch vulnerable systems as a remediation response. This service is licensed by the number of workstations to be managed by the Xcitium SOC team, and includes expanded Global SOC services to detect and resolve IoCs within endpoints.

Pre-Emptive ZeroThreat Virtualization Management - Patented kernel-level virtualization technology pre-emptively stop threats with surgical precision via default-deny of any Unknowns entering an endpoint. If it is not a known and trusted object, it is instantly contained and unable to execute malicious activity in against real resources or enumerate via lateral movement. The virtualized endpoint operates as usual with no interruption. Unknown files are executed in containers while the Xcitium verdicting engine determines if the object is malicious or benign. Innocent objects are simply released from containment. And because contained attacks are no longer threats, alert fatigue is reduced to the power of Zero!

Application Profiling (AI Support) - One of the major modern-day attack vectors are trusted applications that are used as cloaks by adversaries because they are legitimate apps not recognizable as threats by legacy AV solutions. Based on normalization techniques and time series models, SOCaaP provides user-application related baselining that allows our SOC analysts to detect and analyze anomalous threat behavior likely to be caused by memory exploits and file-less attacks. This profiling protects you by working on future threats and attack strategies.

Security Policy Management - SOCaaP provides Xcitium's recommended Security Policy, which can be tailored to meet your specific organizational needs. Recommended policy includes behavior-based alerts for file-less attacks, advanced persistent threats (APTs), and privilege-escalation attempts.

Proactive Threat Hunting (APTs, Lateral Movement, Suspicious Behaviors, ...) - SOCaaP provides security analysts with a suite of powerful tools and global threat intelligence to provide earlier detection, reduce dwell time, and improve defenses against future attacks.

Detect APTs - The greatest benefits organizations derive from threat hunting includes improved detection of advanced threats, followed closely by reduced investigation time, and time saved for not having to manually correlate events.

Process Analysis Examination - SOCaaP excels at providing analysts actionable intelligence over process hierarchies. Process hierarchies are given in tree structures and timeline views, both providing all process-related events of attack progression with context. Endpoint X/MDR also provides details about any hashes seen in the environment, including execution history, download summary, creation summary, execution trend, and basic attributes of the hash. File trajectory is also provided to show the hash's incidents as well as the alerts created by the hash and Xcitium verdicting.

Threat Validation from analysts - Because contained attacks are no longer threats, alert fatigue is a relic of the past. SOCaaP now has the freedom to do more advanced threat hunting and attack analysis, to patch and harden your environment agasint aggressive persisten threats and future attacks. Our SOC experts perform well-defined alert triaging that leaves no room for unvalidated threats.

Eliminate False Positives - With alert fatigue reduced to virtually Zero, analysts can now work on eliminating false positives so that X/MDR only escalates actionable incidents.

Integrated File Analysis (Cloud Sandbox) - Valkyrie, Xcitium's advanced cloud-based sandboxing and file-verdicting system, continuously checks files and processes executed in your environment and automatically uploads all unknown files for static and dynamic analysis verdicting.

Host-Based Intrusion Detection - Endpoint MDR comes with Host Based Intrusion Detection (HIDS) capabilities that includes a preemptive breach prevention approach. The ZeroThreat approach utilizes advanced techniques to detect and block unknowns on endpoints using virtualized containment until verdicting returns a benign or malicious determination. HIDS incorporates signature, behavioral analysis, and stateful inspection detection techniques. Additionally, Endpoint MDR provides file integrity checking, log monitoring, and rootkit detection capabilities.

24/7 ZEROTHREAT COMPLETE X/MDR

Comprehensive 24/7 response of discovered network-based attacks. Xcitium X/MDR extends SOCaaP by offering continuous monitoring of logs from the customer's network, such as firewall, Switch, UTM, etc., as needed. This service level is applied as a package and licensed per number of network hosts and devices where up to 4GB of log monitoring per month is included. Also includes: Secure Policy Management, Proactive Threat Hunting (APTs, Lateral Movements, Suspicious Behaviors and more), Process Analysis Examination, Threat Validation from analysis, eliminates false positives, provides integrated file analysis (Cloud Sandbox), host-based intrusion detection, early warning for emerging threats, Intrusion triage, Incident analysis and management, and combines network, endpoint, cloud and web platforms (situational awareness) for maximum effectiveness. It is deployed as a simple VM and licensed by the number of endpoints.

24/7 MANAGED IDS, DPI NETWORK DETECTION AND RESPONSE

Xcitium Managed Network Detection and Response, including Intrusion Detection and Deep Packet Inspection. This is our most comprehensive and extensive network protection solution. This service is an extension of the Global SOC services and includes Xcitium's own Network Sensor that performs Network-Based Detection and Response for our customers. The sensor runs as a probe on the customer network, sniffing network traffic, decoding more than 40 protocols, including L7, and extracting meta-data information. It includes an on-prem log collector and vulnerability scanner as well. SOCaaP with IDS and DPI Network Detection and Response includes the managed network detection platform plus network intrusion detection which combines signature and heuristics-based IDSs and provides a strong mechanism that allows our SOC teams to do. Comprehensive network analysis and security monitoring, daily signature discovery, and incidents' detection rules management, Insider threat analysis, threat intelligence integration, full packet capture, protocol analyzers for 40+ different protocols such as TCP, UDP, DNS, DHCP, HTTP, HTTPS, NTLM, etc. with full decoding capability. It is deployed as a simple VM and licensed by the number of endpoints.

ZEROTHREAT ESSENTIALS: VIRTUALIZATION TECHNOLOGY THAT STOPS UNDETECTABLE ATTACKS AS THE FIRST LINE OF DEFENSE

Xcitium's industry-unique **Virtualized Containment technology isolates undetectable malware, attacker enumeration, ransomware and supply chain breaches** before any damage can be done. Damage means a hacker was able to write to a disk, a COM Interface, or the Registry, for example. All unknown malicious files that try to write on an Xcitium endpoint or network device are instantly opened in a secure virtual container and analyzed by our cloud-based verdicting engine to return a fast allow or deny decision. Benign objects are simply released from containment. Additionally, only Xcitium delivers a trusted verdict for 100% of the files already in your network to prevent hidden, resting, or embedded malware or malicious code from stealthily launching from files already on your endpoints. ZeroThreat means Zero Trust, Zero Breach, Zero Damage, Zero Dwell Time, and Zero Downtime.

ABOUT US

Xcitium, formerly known as Comodo Security Solutions, is used by more than 3,000 organizational customers & partners around the globe. Founded with one simple goal – to put an end to cyber breaches. Xcitium's patented 'ZeroThreat' technology uses Kernel API Virtualization to isolate threats like zero-day malware & ransomware before they can cause any damage. ZeroThreat is the cornerstone of Xcitium's endpoint suite which includes advanced endpoint protection (AEP), endpoint detection & response (EDR), and managed detection & response (MDR). Since its inception, Xcitium has a zero breach track record when fully configured.

CONTACT

sales@xcitium.com • support@xcitium.com