cymbel CORPORATION
A PINNACLE GROUP COMPANY

The next leap in EDR
Managed Cortex XDR as a Service

Managed Cortex delivers the most advanced endpoint detection and response solution, as a service. This complete solution includes integration with the network and the cloud and is offered at a fixed monthly fee.

THE CHALLENGE
Managing endpoint security is too complex and costly for inhouse teams

Attackers must complete a certain sequence of events, known as the attack lifecycle, to successfully accomplish their objectives, whether stealing information or running ransomware. To succeed, nearly every attack relies on compromising an endpoint, and although most organizations have deployed endpoint protection, infections with malware and exploits are still common.

But attackers don’t just target endpoints, they aim at an organization’s entire infrastructure. They use lateral movement and stealth techniques to exfiltrate valuable data or compromise operations.

THE SOLUTION
24/7 Managed Next Generation EDR

XDR is the next leap forward for endpoint detection and response (EDR), adding integration with the network, the cloud and other relevant agents and data sets.

It expands the capabilities of advanced endpoint solutions with machine learning and automation that reduces manual efforts, allowing our security analysts to focus on prevention and the mitigation of threats that matter most to your organization. Our Security Automation and Orchestration Platform offers comprehensive and 24/7 transparency of your security posture.

Real visibility into real threats:

As endpoint-based attacks become more automated and complex, IT and security departments face event overload, a shortage of trained security analysts, lack of time and increasing staff cost. CISOs and CSOs are under constant pressure to improve visibility across the entire infrastructure, drive faster responses and mitigate threats before damage occurs. They need outcome- based solutions that reduce the time, cost and complexity of event triage, incident investigation, response, and hunting. Instead of a sea of false positive alerts that increase workloads, they need visibility into the real threats.

Powered by Palo Alto Networks and ON2IT:

The Cymbel managed endpoint solution combines the industry's most advanced security products with ON2IT’s world class SOC-as-a-Service. This solution delivers the ideal combination of detection, pre-emptive protection, response and forensics leveraging advanced automation techniques from ON2IT and Palo Alto to block breaches and ransomware attacks before they compromise your endpoints.

Advanced automation techniques:

Cortex XDR provides the ON2IT SOC analysts and forensic specialists with rich contextualized log and event data and threat intelligence. By using automation techniques such as deep learning, behavioral baselining and Indicators of Good©, the ON2IT Security Automation and Orchestration Platform separates the noise from the relevant alerts, enabling our analysts to focus on identifying and remediating critical security events for Cymbel customers. Furthermore, we continuously strengthen prevention and reduce further risk by applying knowledge gained through detection, investigation and response.

YOUR MONTHLY CORTEX XDR PREVENT OR PRO SUBSCRIPTION FEE INCLUDES:

- Cortex XDR license fees
- ON2IT Security Automation & Orchestration Platform
- Threat Event Enrichment, Analysis & Correlation
- Incident Monitoring, Alerting & RCA
- Remote Breach Support
- Security Dashboard
- Compliance Reporting
- Automated Rules of Engagement
- AI-based Threat Hunting*
- Behavior Baselining*
- Post-Mortem Investigation*

*In combination with Cortex XDR Pro

Clear business outcomes

- No worries about talent and staffing
- Extends benefits of EDR to complete infrastructure
- The right expertise and remediation 24/7
- Cost savings
- Fast deployment and scaling

Validated by independent research

Independent research organization The MITRE Corporation recently released the final results of its MITRE ATT&CK™ cybersecurity evaluations. The evaluation, which used the MITRE ATT&CK framework, shows that Cortex XDR Prevent provide the broadest coverage with fewest missed attack techniques among 10 Endpoint Detection-and-Response (EDR) vendors.

Out of 136 attack techniques tested, 121 techniques were detected by Cortex XDR Prevent, with 93% fewer misses than the next product.

Cymbel and Palo Alto Networks: true cybersecurity innovators

Cymbel's full support for Palo Alto Networks technology reflects the importance of true cybersecurity innovation in our DNA.

We are driven by the notion that automation, innovation and a never-ending curiosity and search for improvement can actually make the Internet a safer place.

More information about Managed Cortex XDR? Call (617) 581-6633

www.on2it.net