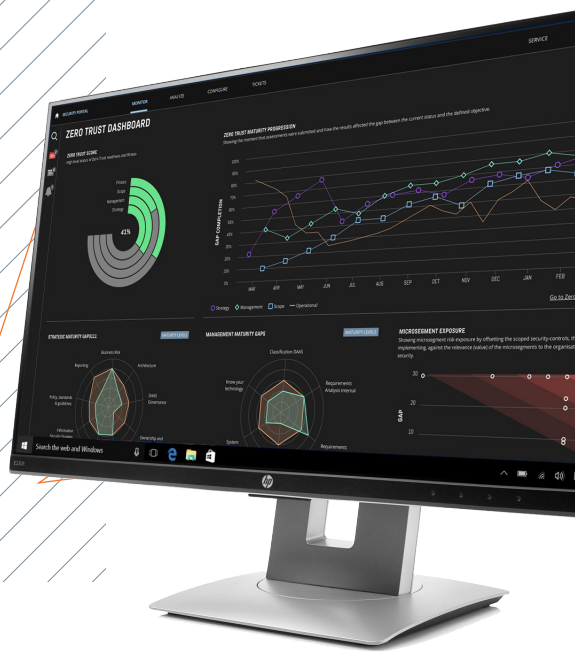
SOC-as-a-Service the next generation of cloud-based security services

Do you have the platform, capability and resources to provide 24/7 information security for the cloud transformation era? Our SOC-as-a-Service delivers the next generation of cloud-based security services in prevention, detection, response, forensics and threat-hunting.



THE CHALLENGE

cybersecurity is becoming too complex to manage in-house

As cyberattacks become more automated and complex, your IT and security departments face an event overload, a shortage of trained and experienced security analysts, lack of time and increasing staff cost.

We know you're under constant pressure to improve visibility, respond faster, and be able to mitigate threats before damage occurs. Cybersecurity is becoming increasingly difficult to manage in-house and you need a solution with clear business outcomes. That solution must reduce the time, cost and complexity of investigating, analyzing root cause and responding to security events, because after a data breach, the clock is ticking.

THE SOLUTION

SOC-as-a-Service

Cymbel has teamed up with cyberleader ON2IT to offer a new generation of SOC-as-a-Service. For a fixed monthly fee, you have access to capabilities that go far beyond the traditional managed security services of basic technology support management, basic monitoring and compliance reporting.

Our SOC-as-a-Service solution allows you to not only detect and analyze threats, but stop them. When a threat is detected, our Zero Trust based cloud platform automates most responses using battle-tested playbooks. Our forensic experts perform deep investigation of novel incidents, making recommendations for short term actions and long term security improvements.

And with the increased usage of SaaS applications and public cloud services such as AWS, Google and Microsoft, we help you deal with advanced cyberattacks that most managed security service providers are not able to address.

Powered by Zero Trust innovator ON2IT:

Our SOC-as-a-Service is powered by technology leader ON2IT, a global pure-play cybersecurity service provider. ON2IT has more than a decade of experience in developing its Zero Trust Security Automation & Orchestration Cloud Platform. Zero Trust is the industry reference in state-of-the-art cybersecurity architectures, and its principles of data protection are used the most advanced cyber teams.

24/7 access to an elite team of security professionals:

Our next-generation cloud platform gives you 24/7 transparent access to a team of cybersecurity analysts who respond in real time to disruptive security events, effectively becoming an extension of your in-house IT department. With the deep integration of our platform across leading vendors including Palo Alto Networks, Fortinet, Cisco, AWS, Azure, Google, and VMware, you can leverage your existing cybersecurity software and hardware.

No need to invest in a SIEM, and deep integration with Palo Alto Networks:

Our endpoint protection is based on the award-winning Palo Alto Networks Traps to block security breaches and ransomware attacks that use malware and exploits, known or unknown, before they can compromise endpoints.
It also builds on the new and revolutionary Palo Alto Networks Cortex XDR to provide our SOC analysts and forensic specialists with rich contextualized log and event data and threat intelligence.

YOUR MONTHLY SOC-AS-A-SERVICE SUBSCRIPTION FEE INCLUDES:

- 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

By coupling ON2IT's advanced automation techniques of deep learning, behavioral baselining and Indicators of Good© with these innovative Palo Alto Networks technologies, our 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 you.

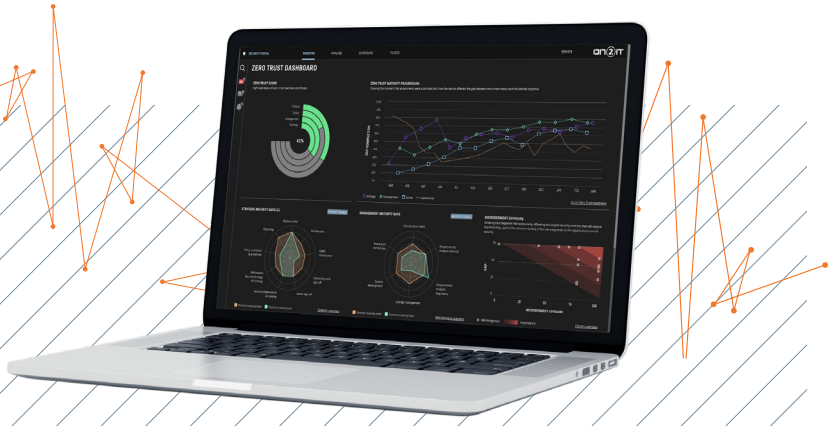
Clear business outcomes

- No worries about talent and staffing
- Faster resolve times
- The right expertise 24/7
- Cost savings

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 provides 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 Soc-as-a-Service? Call (617) 581-6633

Cymbel Corporation Headquarters / 154 Wells Avenue / Newton, Massachusetts 02459
E-mail: sales@cymbel.com / Phone: (617) 581-6633 / Fax: (617) 581-6637

www.on2it.net