APAC CIO Outlook
VENDOR VIEWPOINT

# CYBERSECTHREAT – HOLISTIC CYBERSECURITY MONITORING SOLUTIONS

**BY KELVIN YIP, FOUNDER AND DIRECTOR OF CYBERSECTHREAT**

Organizations are facing different cyber security risks, such as APT attack, zero-day attack, ransomware attack, account compromise, physical assets stolen and secret token abuse. Enterprises already invested a lot of different physical (e.g., lock, security guard, CCTV, door access control system and signal jammer) and logical security controls (e.g., firewall, IDS, EDR) to protect their assets. However, security incidents and data breaches still occurred. If we can extend our visibility into physical security and external attack surface, the overall security posture can be greatly improved.

## CYBERSECTHREAT OFFERS EXTENDED VISIBILITY FOR CYBER ATTACK

CyberSecThreat which provides wide-range of "Cyber Security" solutions is a startup founded in 2021, headquartered in Taiwan.

The company develops an effective security monitoring solutions on top of Splunk software and Splunk Enterprise Security Add-on. It is a product combining Cyber Security Experts 's research results and deep tuning of Splunk software. Professional Service will be provided to assist customers onboarding successfully. The company's first release captured both on-premises logs as well as cloud logs to provide visibility over MITRE ATT&CK Technique and GRC (Governance, risk management, and compliance). After radars were deployed in different viewpoints and Cyber-Kill Chain stages, the deployed monitoring solutions were able to detect both real attacks and over 95% of red team operations within 4 hours. The company's latest solution also extends visibility and insight to physical security and external viewpoint.

## TRANSFORM ZERO TRUST FROM VIRTUAL WORLD BACK TO PHYSICAL WORLD

Most SOC (Security Operation Center) do not have enough visibility over physical security. In addition, SOC and PSOC (Physical Security Operation Center) work independently. For instance, if SOC can correlate door access control system and login information, then abnormalities can be observed. CyberSecThreat brings the integration to the next level and applied it to OT (Operational Technology) environments.

Critical infrastructure companies, manufacturing, healthcare and building management heavily use OT (Operational Technology) in their production environment. OT mainly comprised of Industrial Control Systems (ICS) such as Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS) and Programmable Logic Controllers (PLCs). SCADA and DCS are primarily responsible to control the PLC over network to perform the actual tasks. To protect OT environments from cyber-attack challenge, companies are adapting various new OT security controls such as OT firewall, OT IDS, OT PAM, OT network segmentation, OT Abnormal and change detection system.

Imagine if an attacker gets physical access to OT environment using social engineering, and then directly connect the ethernet cable of PLC to a Raspberry PI equipped with 4G mobile connection, the attacker can get direct control to PLC, stop the production line, cause harm to human or inject malicious command back to SCADA system.

With strategy planning & seamless integration between physical security controls and CyberSecThreat's security monitoring solutions, SOC can effective spotted abnormalities and potential security incidents.

"Zero trust, from virtual world back to physical world - through seamless integration of cyber security with modern operational technology"

## CYBERSECTHREAT OFFERS HACKER'S VIEWPOINTS FOR ORGANIZATION

Many Organizations use "Internal Views" to manage their assets and attack surface. CyberSecThreat provided Cloud Inventory Integration in the first release of security monitoring solutions, which can significantly improve the effectiveness of incident investigation and response. However, this still only provides an "Internal Views" of assets and attack surface and cannot fully discover all unknown or shadow assets. It is not possible to manage security risks without complete visibility.


The approach to conduct penetration testing or red team operation annually provides hacker's viewpoints, but also create a gap that this viewpoint not updated constantly. CyberSecThreat take further steps to offer viewpoints of hackers by integrating different OSINT resources and external monitoring tools into continuous monitoring process. Therefore, organizations can take required actions before attacker exploit vulnerabilities.

There are tons of interesting information available in OSINT resources, threat intelligence and external monitoring tools. This information includes email accounts available on public internet, SSH ports of testing machines exposed to internet, website defacement, account compromise, previous and current DNS lookups results, SSL/TLS certificate information, access key uploaded to public GitHub repository, leakage of software token, attacker discussing your organization in dark web.

By giving the name of your organization and domain name information as monitoring keywords, we can discover any shadow machines and related domain information. The resulting information can be further fed into our security monitoring solutions, and actionable alerts can be generated to 7x24 SOC. For instance, if SOC team receive an alert regarding AWS access key uploaded to public GitHub repository, SOC can remind developer team to exclude access key during commit process and reset the access key used in production.

## CYBERSECTHREAT ACCELERATES ORGANIZATION'S DETECTION AND INCIDENT RESPONSE CAPABILITIES

While blue team and security team research the behavior and technique used by attacker to improve protection and detection, adversaries also continue advance themselves and becoming stealthier to evade security controls, SOC detection, AI detection and machine learning. APT groups are willing to invest money and time on their targets. For example, attackers paid for cloud security appliance to test their zero-day, hide their C2 infrastructure behind CDN, study red team's research how to bypass security controls, conduct external reconnaissance & google dorking and conduct research to simulate user's behavior. Therefore, attackers trend not to trigger any noisy and radar due to aware of the existence of blue team and SOC.

With deep understanding of attacker's behavior, CyberSecThreat's security monitoring solutions seamlessly integrate with your 7x24 SOC operation and offers a complete visibility over different viewpoints to prevent data breaches and speed-up incident response ACO.