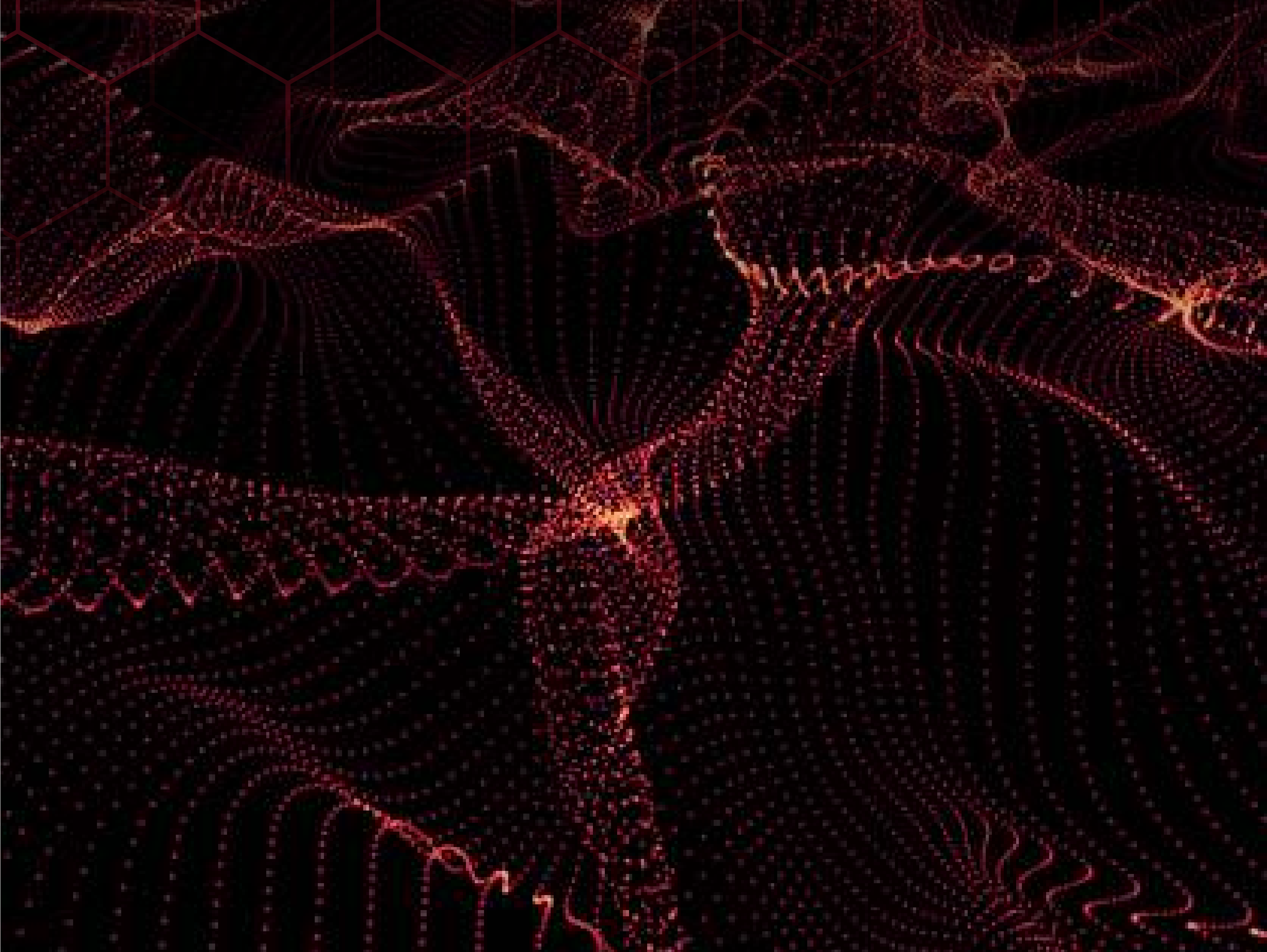
CyberKnight

SecOps & Threat Hunting

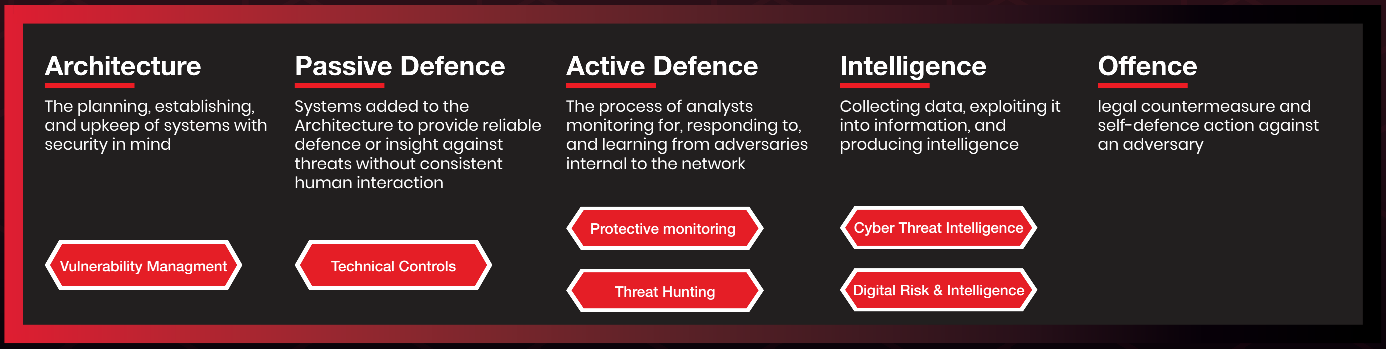


SecOps & Threat Hunting

The chances are very high that hidden threats are already in your organization's networks. Organizations can't afford to believe that their security measures are perfect and impenetrable, irrespective of how thorough their security precautions can be. Having a fringe and defending it aren't enough because the perimeter has faded away as new technologies and interconnected devices have emerged. Prevention systems alone are insufficient to counter focused human adversaries who understand how to make around most security and monitoring tools by, for instance, making their attacks seem like normal activity.

Customers that operate an advanced threat detection and response capabilities will improve their security posture and hence reduce risk, as malicious activity can be identified earlier on in an attack, thereby minimizing the opportunity for adversaries to disrupt, damage or steal.

As per SANS the cyber security maturity journey takes five phases or stages in terms of cyber capabilities. Customers first need to sufficiently mature their Architecture (e.g. Vulnerability Management & patch Managements). Passive Defense capabilities are those tools and systems added to the architecture that give insight into the network or provide some aspect of security without constant human interaction, such as firewalls, intrusion detection systems and endpoint security solutions. Active Defense (e.g. Protective Monitoring), covers a wide array of activities relating to analysts monitoring for threats, responding to them, learning from them and leveraging that information internal to their environment. Intelligence is the process and product resulting from collecting data, turning it into information and analyzing potentially competing sources of information to produce useful knowledge. The last category, offence, relates to countermeasures that organizations or states may take for self-defense purposes according to their laws.



Architecture

The planning, establishing, and upkeep of systems with security in mind

Passive Defence

Systems added to the Architecture to provide reliable defence or insight against threats without consistent human interaction

Active Defence

The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

Intelligence

Collecting data, exploiting it into information, and producing intelligence

Offence

legal countermeasure and self-defence action against an adversary

Figure 1 - The SANS Sliding Scale of Cyber Security

CyberKnight

CyberKnight built a portfolio of solutions and services that can aid in building mature cyber security operations, detection and response, and threat hunting capabilities that mostly align with industry best practices and standards. Our portfolio mainly focuses on critical capabilities to address the current challanges that many customers are currently facing such as shortage in cyber skills and resources, alert fatigue, and lack of automation of SecOPs. Those capabilites are as follows:

- Boost detection of early intrusions and lateral movement incidents via deception capabilities
- Gain full visibility into network traffic and detect anomalous network behaviors and extract local network intelligence
- Accelerate endpoint threat detection and response capabilities
- Have full visibility based on intelligence of real attack infrastructure and activity, and work from the same platform to address modern digital threats outside the firewall
- Collect forensic data and local intelligence (IOCs & TTPs) extracted from endpoints, network and decoy systems
- Help tier 1 SOC analysts reduce the alert fatigue they suffer from, via auto-tuning of SIEM correlation rules to reduce false positives and increase high fidelity incident rates
- Help tier 2 or tier 3 SOC analyst to automate many of their security operations via augmented AI
- Foster security posture of the corporate via attack simulation and risk-based vulnerability prioritization and validation
- Provide the required hand holding and support to conduct continuous and proactive threat hunting and to engage during major incidents to investigate and remediate accordingly

Identity Detection & Response - IDR	Network Detection & Response -NDR	Network Detection & Response -EDR	Predictive XDR	Malware Sandbox
Attivo NETWORKS	GROUP-IB	CROWDSTRIKE	SecLytics.	GROUP-IB
	IronNet	GROUP-IB		

aiSOC / aiSIEM

seceon

Threat Hunting Platforms

SecLytics. | GROUP-IB | CROWDSTRIKE | IronNet

SOC Virtua Assitant / Breach Attack & Simulation

STRIKE READY

SOAR / Incident Response Platform

CYWARE™

MDR-IRR-DFIR
Adversary Simulation - Red Teaming

AXON | GROUP-IB

CyberKnight

Below is the list of vendors that Cyberknight recommends, to build a mature SecOPs, incident response and detection, and threat hunting capabilities, and where each vendor help:

Attivo NETWORKS

Attivo deception provides immediate value by providing “eyes inside the network” visibility and accurate detection alerting based upon decoy engagement or attempts to use deception credentials, most notably early in the attack cycle. For years, attackers have successfully used deception tactics for breaching networks. They masquerade as legitimate employees, using stolen credentials and deceptive measures to infiltrate a network, all while remaining undetected for lengthy dwell times. Deception brings the offense into the realm of cybersecurity with the ability to deceive and misdirect an attacker into revealing themselves. All, without false positive alert fatigue and the burden of operational overhead associated with traditional detection methods.

IronNet

IronNet advanced network based behavioral detection leverages advanced algorithms, machine learning (ML), artificial intelligence (AI), and other cutting-edge detection techniques to identify advanced threats designed to evade even the best endpoint and firewall tools. It takes decades of operational wisdom from the best cyber offensive and defensive operators and applies that tradecraft knowledge to prioritize identified anomalies based on their risk to the enterprises without the false-positives common to other behavioral analysis cybersecurity tools. Detected threats are then shared within IronNet’s IronDome environment and correlated across industry peers to identify sector-wide campaigns that would be difficult to detect in isolation.

CROWDSTRIKE

CrowdStikre EDR prevents silent failure by capturing raw events for automatic detection of malicious activity, unparalleled visibility, proactive threat hunting and forensic investigations. It unravels an entire attack, enriched with contextual and threat intelligence data. Finally, it provides powerful response action to contain, investigate and remediate compromised systems. It’s also worth mentioning that Crowdstrike has an elite team of security experts proactively hunt, investigate and advise on activity in your environment to ensure threats and high priority alerts don’t get missed, alert prioritization uniquely, pinpoints the most urgent threats and resolves false positives

SecLytics®

Seclytics Augur engine hunts adversaries in the wild during the setup stage, generating attack predictions on average 51+ days before they strike. Those predictions have been proven to be over 97% accurate and generate fewer than 0.01% false positives. Augur's patent-pending technology can even tell an organization who specifically targets them in under 72 hours. Augur scours the internet daily analyzing changes in the IP space (IPv4 and IPv6), domain name registrations, DNS resolution, and BGP announcements. Then leveraging supervised and unsupervised learning Augur generates potential cybercriminal profiles and labels these profiles. Augur's smart classifiers evaluate incoming threats, correlate them with your data, and decide which threats can be blocked with a high level of certainty (less than 0.01% false positives). Then Augur evaluates and prioritizes level 2 and 3 threats and passes them up to your SOC analysts via curated alerts. The platform also provides access to a powerful enrichment dashboard to equip your analysts with the data they need to make fast, accurate incident-response decisions.

STRIKE READY

StrikeReady offers a powerful SaaS-based platform – Cognitive Security Platform that comes along with an Intelligent System – CARA (think J.A.R.V.I.S for cyber-security), which helps optimize, consolidate and operationalize organization's cyber-security technology stack to maximize the ROI, while the Intelligent System CARA assists defenders to quickly respond to incidents, proactively defend against emerging threats or operate at lightning speed while they perform any security operations centric task. Strikeready helps Execute true-to-life attacks safely and improve layered defense, Help identify and prioritize patching of vulnerabilities via attack simulation and lastly increase security analyst efficiency and productivity, via automation and augmented intelligence

seceon

Seceon's Open Threat Management Platform uses behavioral analytics generated by an extensive set of dynamic threat models, aided by machine learning techniques to detect both known and unknown zero-day attacks. It enables organizations to see cyber threats quickly and clearly, and to stop them as they happen, preventing the infliction of extensive corporate damage. The platform was built to use elastic compute power to develop the industry's first and only fully automated threat detection and remediation system.

GROUP-IB

Group-IB is one of the leading providers of solutions aimed at detection and prevention of cyberattacks, online fraud, and IP protection. Group-IB Threat Intelligence & Attribution system was named one of the best in class by Gartner, Forrester, and IDC. Group-IB offers a full threat detection and hunting suite which comprises an EDR (Huntpoint), NDR Senser, Sandbox (Polygon), SSL Decryptor, and a central management and correlation platform (Huntbox). This whole setup can be implemented fully on-prem. In addition to that, Group-IB offers an attack surface management service (AssestZero), Digital Risk Protection (DRP), and Threat Intelligence and Attribution services. On Top of that, Group-IB offers a whole suite of cybersecurity services such as pen testing, red teaming, digital forensics, and IR services

CYWARE™

Cyware is the only company building Virtual Cyber Fusion Centers enabling end-to-end threat intelligence automation, sharing, and unprecedented threat response for organizations globally. Whether you are just getting started with threat detection and alerting, looking to make threat intelligence actionable, or searching for ways to optimize your SOC with customizable playbooks, Cyware has integrated virtual cyber fusion solutions to help you take your security operations and threat response to the next level. Cyware's virtual cyber fusion suite delivers advanced capabilities for strategic and technical threat intelligence sharing, and security orchestration, automation, and response (SOAR) in a truly modular and integrated manner.

Cyware Threat Intelligence eXchange (CTIX) - A smart, client-server threat intelligence platform (TIP) for ingestion, enrichment, analysis, and bi-directional sharing of threat data within your trusted network.

Cyware Situational Awareness Platform (CSAP) - Automate threat alert sharing and aggregation in real-time

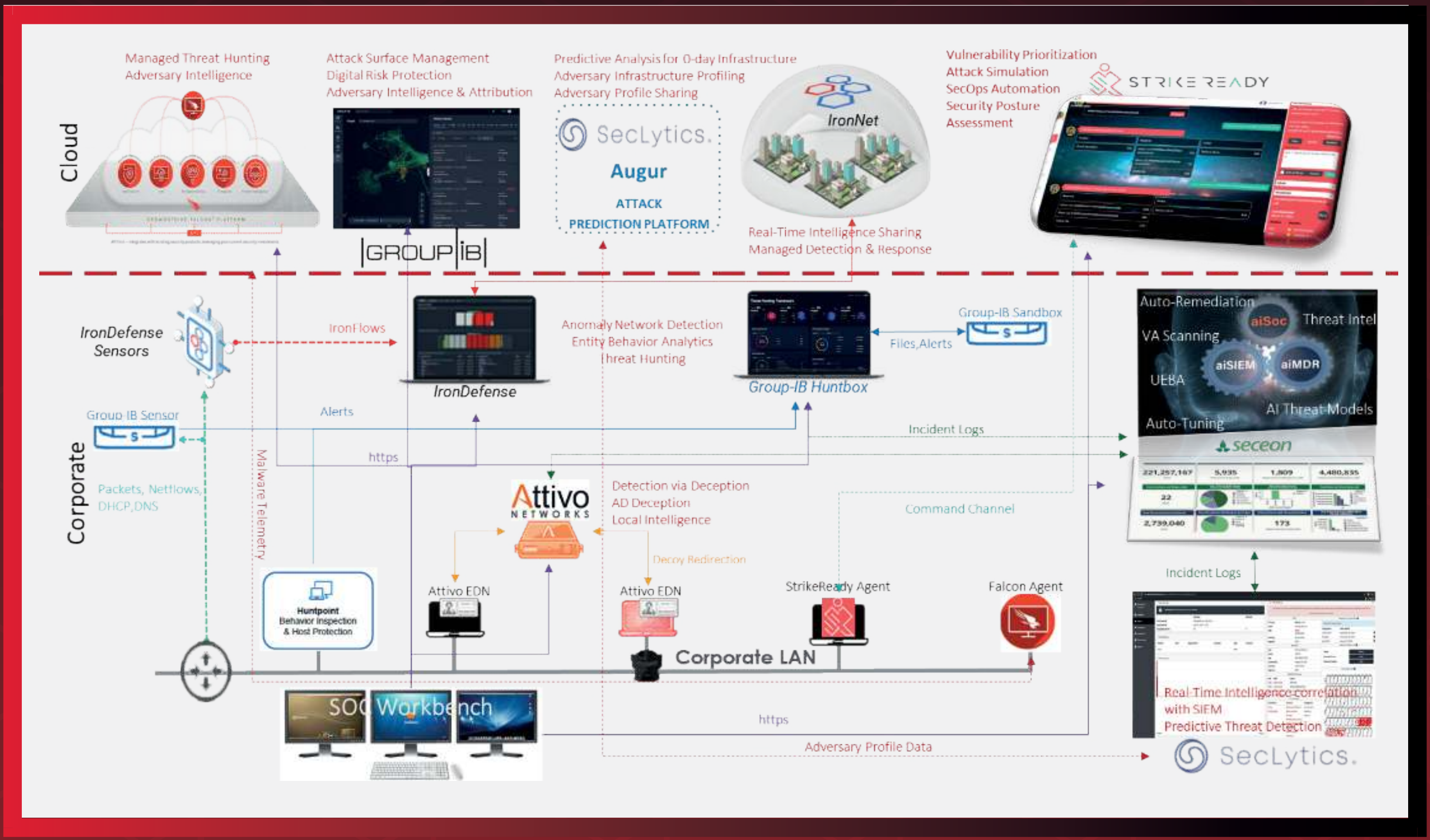
Cyware Fusion and Threat Response (CFTR) - A threat response automation platform that combines cyber fusion, advanced orchestration, and automation to stay ahead of increasingly sophisticated cyber threats affecting enterprises in real-time.

Cyware Orchestrate (CSOL) -An Any-to-Any Vendor Agnostic Orchestration platform for connecting & automating Cyber, IT, and DevOps workflows across Cloud, On-Premise, and Hybrid environments

AXON

Axon Technologies provides industry-leading intelligence-led, risk-based cybersecurity services to help organizations predict, prevent, detect, and respond to attackers - before, during, and after an incident. Their team has a deep understanding of cyber attackers' behavior, industry standards and frameworks, technology best practice configuration, security process automation, and access to unmatched threat intelligence. With this insight and experience, they are able to provide differentiated security assessment, transformation, training, and Managed Detection and Response (MDR) services to help our customers build functional resiliency and close security gaps to reduce business risk.

Below is a high-level design that illustrates where each component fits into the security operations center, how it operates and what features and capabilities it provides


Cloud
Managed Threat Hunting
Adversary Intelligence
Attack Surface Management
Digital Risk Protection
Adversary Intelligence & Attribution
|GROUP|IB|
Predictive Analysis for 0-day Infrastructure
Adversary Infrastructure Profiling
Adversary Profile Sharing
SecLytics.
Augur
ATTACK
PREDICTION PLATFORM
IronNet
Real-Time Intelligence Sharing
Managed Detection & Response
Vulnerability Prioritization
Attack Simulation
SecOps Automation
Security Posture
Assessment
STRIKE READY
Corporate
IronDefense
Sensors
IronFlows
IronDefense
Anomaly Network Detection
Entity Behavior Analytics
Threat Hunting
Group-IB Huntbox
Files,Alerts
Group-IB Sandbox
Auto-Remediation
aiSoc
Threat Intel
VA Scanning
aiSIEM
aiMDR
UEBA
AI Threat Models
Auto-Tuning
seceon
Group IB Sensor
Alerts
Incident Logs
https
Packets, Netflows,
DHCP,DNS
Malware Telemetry
Attivo
NETWORKS
Detection via Deception
AD Deception
Local Intelligence
Command Channel
Decoy Redirection
Huntpoint
Behavior Inspection
& Host Protection
Attivo EDN
Attivo EDN
StrikeReady Agent
Falcon Agent
Incident Logs
Corporate LAN
SOC Workbench
https
Adversary Profile Data
Real-Time Intelligence correlation
with SIEM
Predictive Threat Detection
SecLytics.