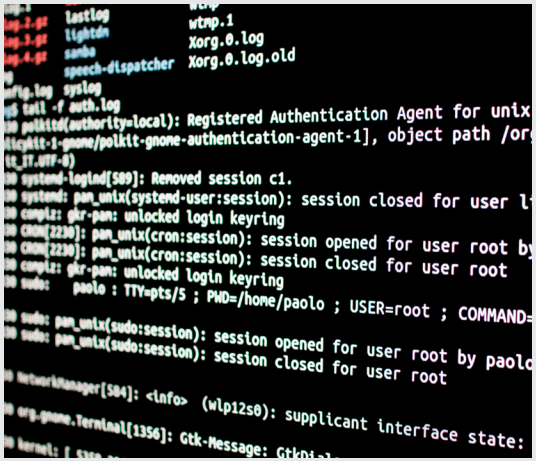
KNIGHTVISION CAM

Compliance | Alerting | Monitoring

A multi-tiered solution to
multiple cybersecurity challenges

AVALONCyber

KNIGHTVISION CAM BY AVALONCyber



KnightVision CAM

COMPLIANCE, ALERTING, MONITORING

The constant evolution of cyberattacks – and the everchanging compliance regulations and advanced security measures needed to keep up with them – makes achieving the ideal cybersecurity program for your business challenging, perhaps, even cost prohibitive.

At Avalon Cyber, we work with a lot of small and medium-sized businesses. And we understand juggling data protection and compliance needs with, let's just say, a less than multi-million-dollar spending budget. Our passion for assisting our clients led to the creation of a service offering that delivers much-needed assistance to help solve these two issues – security and compliance – by providing advanced monitoring and reporting, at a reasonable price.

That solution is KnightVision CAM.

KnightVision CAM is based on two advanced cybersecurity offerings that address the issues of compliance and protection: a Security Information and Event Management (SIEM) platform, and a Security Operations Center (SOC). A SIEM uses hardware and software to collect, aggregate, and analyze security event log data from your network, and can also be configured to provide your security team with alerts. A SOC is a team of cybersecurity experts who, by using a SIEM system and its security alerts, can respond to detected threats immediately and effectively.

Typically, the cost of the sophisticated technology of a SIEM and the human power behind a SOC prevent many small and medium businesses from implementing these options. That's where KnightVision CAM differs. Its multi-tiered approach to multiple cybersecurity challenges is much more affordable.

So, what is KnightVision CAM, how will it address my cybersecurity concerns, and why doesn't it cost a bazillion dollars? First, let's take a closer look at SIEMs and SOCs, i.e., the technology and experts behind the service.

THE ABCS OF SIEMS AND SOCS

Security Information and Event Management (SIEM)

SIEMs have been around since the mid- to late 2000s. When they first arrived on the cyber scene, they were incredibly expensive (like, only-Fortune-500-companies-could-afford-them expensive), were impossible to configure to do the tasks security analysts wanted them to do, and inundated IT administrators and security analysts with so much data, they could barely find time to triage and respond accordingly.

Another issue with earlier versions is that SIEM reports were difficult to understand. In fact, a survey of IT professionals showed that 65% of respondents faced issues with finding necessary audit data upon request, 63% saw difficulties in understanding the reports, and 57% had to manually adjust data to make the reports understandable to non-tech stakeholders.[1]

KNIGHTVISION CAM BY AVALONCyber

1,473 CYBERATTACKS IN 2019
leading to **164.6 million** successful data breaches[2]

THE NUMBER OF UNFILLED CYBERSECURITY JOBS WILL RISE TO 3.5 MILLION BY 2021

Enter the "modern" SIEM (2017 – today), which provides a vast array of benefits, including:

- Allowing your security team to gain a holistic understanding of your assets' security status, i.e. "one pane of glass"
- Prioritizing security incidents
- Demonstrating compliance with regulations
- Log correlation with various sources (both internal and external intelligence feeds)

They also leverage opensource technology to keep costs reasonable, and streamline and funnel alerts, so only the most significant ones get through to analysts. But they still have one issue SMBs may struggle with: SIEMs are still tricky to configure – unless you happen to have an in-house security engineer on staff who can do the job – which, of course, most do not.

Security Operations Center (SOC)

A SOC brings together experts, technology (such as a SIEM), and processes to provide businesses with continuous network monitoring. Typically, a SOC is a 24/7/365 operation, providing you with round-the-clock threat hunting, alert detection, and response throughout your system, from your servers all the way to the endpoints.

A SOC offers a range of benefits, including:

- Analysis of millions of real-time events
- Prioritization of your assets, alerts, and threats and their severity levels
- Management of and response to cyberthreats

The two main concerns associated with SOCs are cost of setup (SIEM hardware, software, etc.) and the fact that finding qualified cybersecurity personnel to hire in-house is near impossible these days. According to recent estimates, there will be as many as 3.5 million unfilled positions in the industry by 2021, which means the demand for these professionals is sky-high, as are their paychecks.[3]

So, what's a SMB to do?

KNIGHTVISION CAM BY AVALONCyber

KNIGHTVISION CAM SOLUTIONS

Tier 1: SIEM Compliance

To assist your team with compliance obligations, this tier collects and retains log data, and creates reports for regulations auditors.

Includes:

- Log data collection and retention

Tier 2: SIEM Alerting

In addition to log aggregation, this tier provides autonomous alerts, which will be sent to a service desk system for your security team to review.

Includes:

- Autonomous alerting
- Log data collection and retention

Tier 3: MSOC 8-5 Monitoring

This tier offers log aggregation, alert notification, and monitoring during business hours to support your in-house security team.

Includes:

- 8:00 a.m. to 5:00 p.m. monitoring
- Autonomous alerting
- Log data collection and retention

Tier 4: MSOC 24/7/365 Monitoring

A traditional Managed SOC, this tier comes complete with log data collection and retention, alerts, and round-the-clock monitoring by Avalon Cyber security experts.

Includes:

- 24/7/365 monitoring
- Autonomous alerting
- Log data collection and retention

All tiers include:

- Implementation and setup
- Updates and patches to platform

Available add-ons:

- Additional agents (computer programs that perform tasks continuously and autonomously)
- Managed Detection and Response (MDR) sensors

INTRODUCING KNIGHTVISION CAM

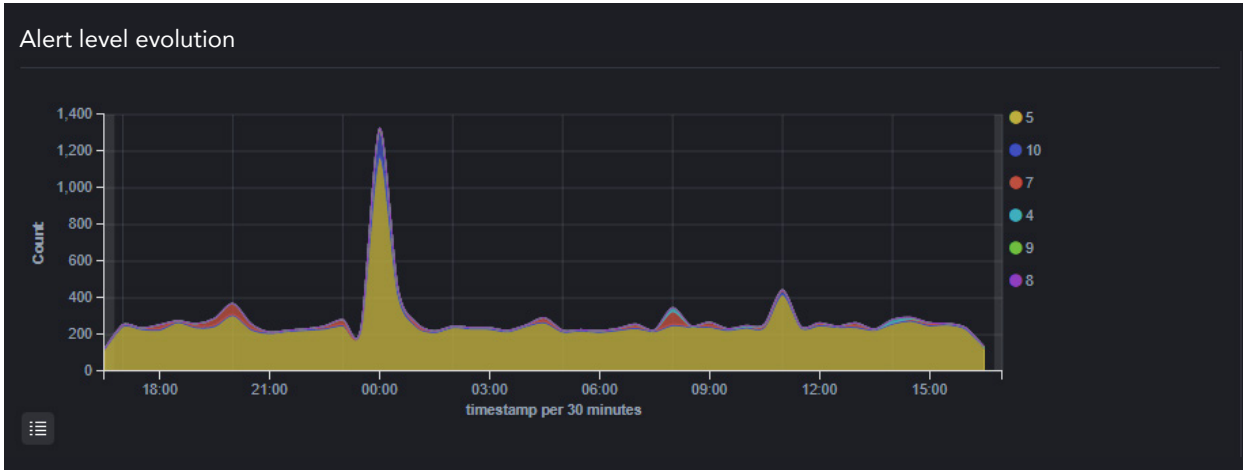
Your data is just as important as that of a giant corporation, right? We think so, too, which is why the engineers at Avalon Cyber developed KnightVision CAM, our customizable, scalable – and affordable – solution to cybersecurity challenges, including regulatory compliance and threat alerting and monitoring.

KnightVision CAM has been architected and developed based on a collection of best-of-breed opensource security technologies, which allows us to provide an impactful service, while maintaining an affordable pricing structure. Its unique tiered approach allows you to choose only the services you require. So, whether you need to just "check a box" for compliance issues or require a cyber team to monitor your network 24/7/365, KnightVision CAM addresses your security needs, as well as your budget.

The KnightVision CAM Difference

Here's why KnightVision CAM is able to provide SMBs with a solution that helps their internal IT and security teams address the challenges of regulatory compliance and threat alerting and monitoring, more efficiently and effectively.

- **Built exclusively with opensource technology.** The entire KnightVision CAM service has been architected leveraging opensource technology. (If something is "opensource," it simply means that "thing" is publicly accessible and can be shared and modified by anyone who wants to use it.) Utilizing opensource technology typically results in a product or service being more affordable, since it doesn't fall under expensive third-party licenses. Other benefits of using opensource technology are the transparency regarding vulnerabilities and the likelihood of creators finding



elasticsearch

logstash

kibana

Security Onion

WAZUH

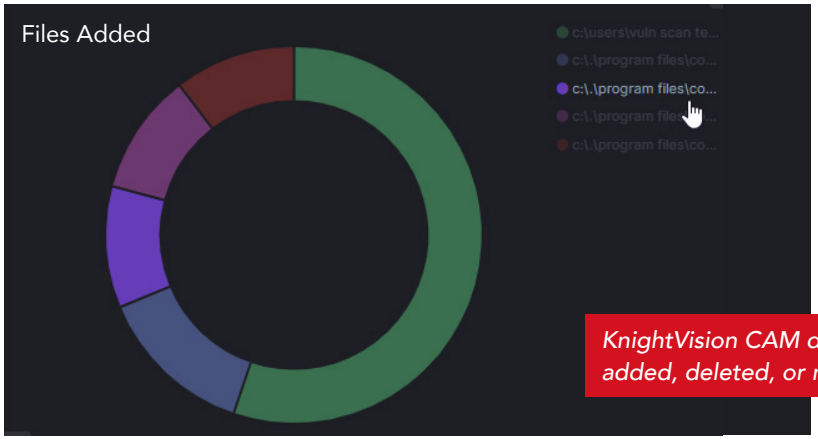
and fixing bugs quickly. A few of the opensource technologies incorporated into KnightVision CAM are the ELK stack (which stands for ElasticSearch, LogStash, and Kibana; it lets users store, search, analyze, and visualize data from any source or format, in real time) and forked-OSSEC solutions (Open Source HIDS [Host-based Intrusion Detection System] Security, which performs log analysis, time-based alerting, active response, and more).

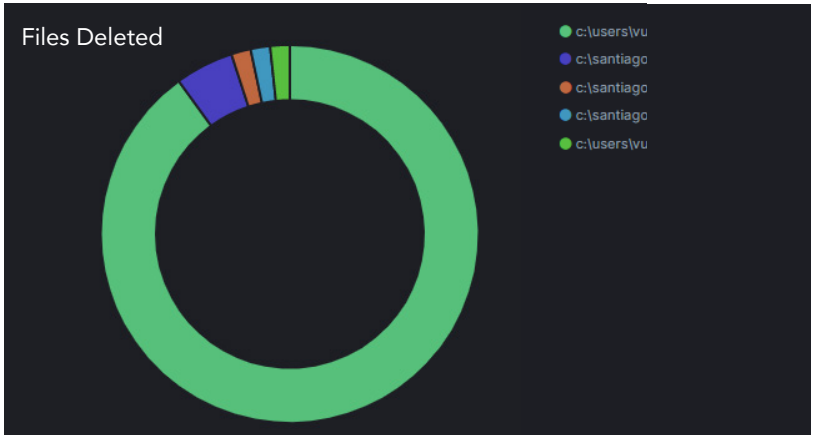
- **Tiered structure.** KnightVision CAM's four-tiered structure allows more businesses access to the latest in cybersecurity protection and regulation compliance. You choose only the services you require and can customize them to fit your network needs, your business goals, and of course, your security budget.
- **Complete support.** No matter which tier you choose, know that you will have access to our team when you need them. Whether you have a question on a Monday afternoon about your Tier 1 compliance reporting dashboard or your Tier 4 MSOC detects an intruder at 2:00 a.m., our cyber professionals are at your service.
- **CAM in the cloud.** As a cloud-based SIEM, KnightVision CAM delivers many benefits. Since it's a single-tenant environment, your data is completely isolated from other users' data, so security is not an issue. Its scalable structure can be designed to match your organization's needs. You'll never have to worry about upgrades, as we take care of them for you. And there's no hardware required, so it's ready to use immediately, less complex, and more affordable.

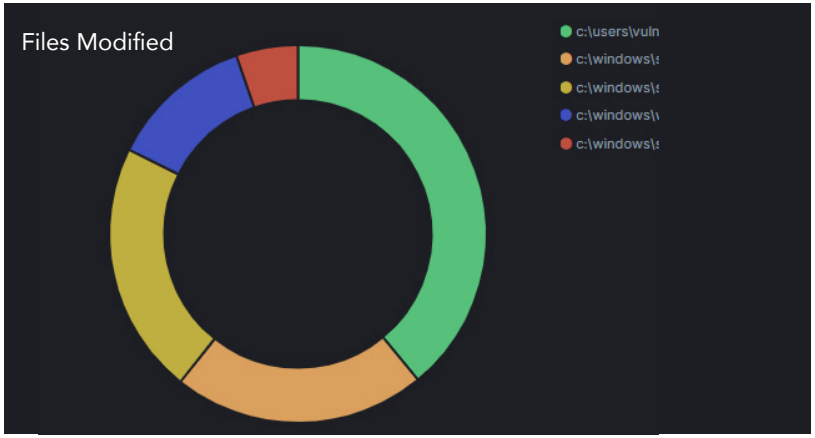
Our Dashboards

Most security teams are overwhelmed by the amount of data and alerts generated by their security tools. For many of them, detecting security incidents doesn't feel so much like looking for a needle in a haystack, as it does looking for a needle in an enormous pile of needles. (Meaning, they don't even know what to look for because there are so many alerts that it's almost impossible to weed out true positives from false positives.) Having a well-designed, user-friendly dashboard can be key in helping them visualize meaningful alerts.

KnightVision CAM's easy-to-read graphics and other visualizations allow your team to review event data and identify patterns and anomalies more proficiently. Users can easily pivot from timelines to log searches to user profiles to gain deeper insight into your environment. And, since all your info is on one glorious dashboard, they can make informed decisions quickly. Finally, dashboards can be engineered to assist with specific regulations, including HIPAA, NIST, GDPR, and PCI, to address your compliance challenges as well.







KnightVision CAM dashboard visualizations of files added, deleted, or modified on a network.

A Closer Look at Tiers 3 & 4: MSOC 8-5 and MSOC 24/7/365

MSOC 8-5 and MSOC 24/7/365 are Avalon Cyber's answer to a Managed Security Operations Center (MSOC) service, but with important differences. MSOC 8-5 offers threat monitoring between 8:00 a.m. and 5:00 p.m., providing SMBs with a more affordable option. But, if you want round-the-clock monitoring, we have you covered there, too, as MSOC 24/7/365 provides "eyes on glass" monitoring, all day, every day, for the ultimate in data information protection.

No matter which option is best for your business, you can rely on MSOC 8-5 and MSOC 24/7/365 to provide the following services/functions:

Security Analytics

Lightweight agents (computer programs that perform tasks continuously and autonomously) collect, aggregate, index, and analyze security data in real time to help your company detect intrusions, threats, and behavioral anomalies.

File Integrity Monitoring

Agents monitor your file system, identifying changes in content, permissions, ownership, and attributes of files, as well as users and applications used to create/modify files that you need to keep an eye on. File integrity monitoring capabilities can help identify threats or compromised hosts, and several regulatory compliance standards, such as PCI DSS, require it.

Intrusion Detection

Our agents scan the monitored systems looking for

KnightVision CAM dashboard visualization of commonly affected packages.

KnightVision CAM dashboard visualization of most common CVEs.

KnightVision CAM dashboard visualization of severity distribution.

malware, rootkits, and suspicious anomalies. They can detect hidden files, cloaked processes, or unregistered network listeners, as well as inconsistencies in system call responses. The server component detects intrusions by analyzing collected log data and looking for indicators of compromise (IOCs).

Log Data Analysis

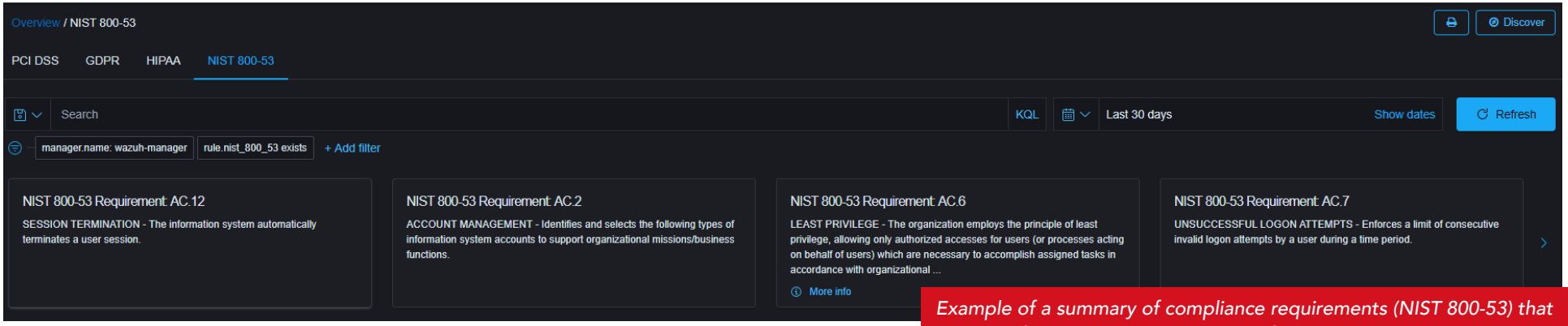
Operation and application logs are read via computing agents and securely forwarded to a central manager for rule-based analysis and storage. Rules help make you aware of application and system errors, misconfigurations, attempted and/or successful malicious activities, policy violations, and a variety of other security and operational issues.

Vulnerability Detection

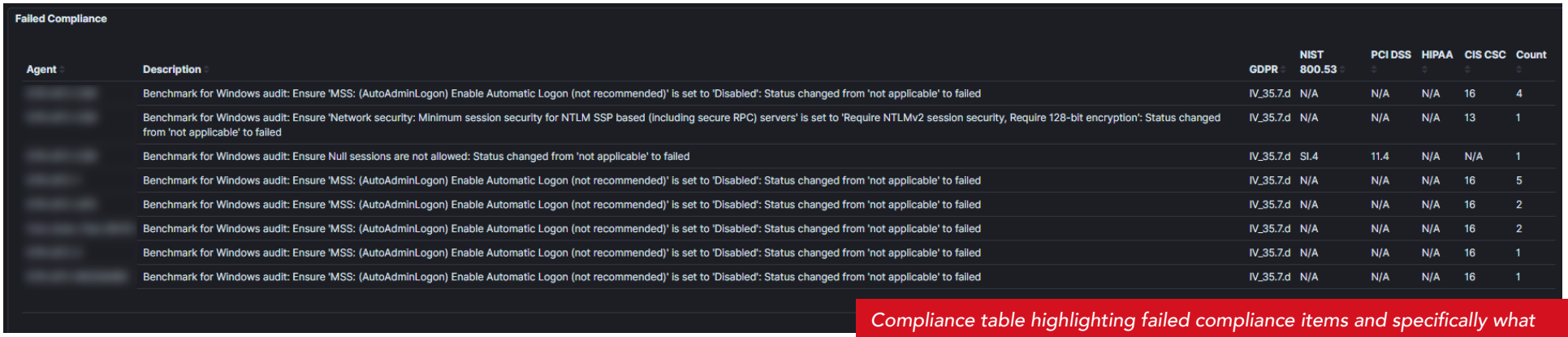
Software inventory data is pulled and sent to your server via agents, where it's correlated with continuously updated CVE (Common Vulnerabilities and Exposure) databases, in order to identify vulnerable software. Automated vulnerability assessments help you find weak spots in your critical assets, so you can take action before attackers exploit them and steal confidential data.

Configuration Assessment

To ensure that your system and application configuration settings are compliant with your security policies, standards, and/or hardening guides, our agents perform periodic scans to detect applications that are known to be vulnerable, unpatched, or insecurely configured. Alerts include recommendations for better configuration, references, and mapping with regulatory compliance.



Example of a summary of compliance requirements (NIST 800-53) that are identifiable through the SIEM platform.



Failed Compliance

Agent	Description	GDPR	NIST 800.53	PCI DSS	HIPAA	CIS CSC	Count
	Benchmark for Windows audit: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled': Status changed from 'not applicable' to failed	IV_35.7.d	N/A	N/A	N/A	16	4
	Benchmark for Windows audit: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption': Status changed from 'not applicable' to failed	IV_35.7.d	N/A	N/A	N/A	13	1
	Benchmark for Windows audit: Ensure Null sessions are not allowed: Status changed from 'not applicable' to failed	IV_35.7.d	SI.4	11.4	N/A	N/A	1
	Benchmark for Windows audit: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled': Status changed from 'not applicable' to failed	IV_35.7.d	N/A	N/A	N/A	16	5
	Benchmark for Windows audit: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled': Status changed from 'not applicable' to failed	IV_35.7.d	N/A	N/A	N/A	16	2
	Benchmark for Windows audit: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled': Status changed from 'not applicable' to failed	IV_35.7.d	N/A	N/A	N/A	16	2
	Benchmark for Windows audit: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled': Status changed from 'not applicable' to failed	IV_35.7.d	N/A	N/A	N/A	16	1
	Benchmark for Windows audit: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled': Status changed from 'not applicable' to failed	IV_35.7.d	N/A	N/A	N/A	16	1

Compliance table highlighting failed compliance items and specifically what framework each ties back to (GDPR, NIST 800-53, PCI DSS, HIPAA, CIS CSC).

Regulatory Compliance

Software agents provide many of the necessary security controls to become compliant with industry standards and regulations. These features, combined with its scalability and multi-platform support, help organizations meet technical compliance requirements. Our technology platform is used by payment processing companies and financial institutions to meet PCI DSS requirements. Its web user interface provides reports and dashboards that can help with this and other regulations (e.g. GPG13 or GDPR).

Incident Response

Various countermeasures are performed by our agents to address active threats, such as blocking access to a system from the threat source when certain criteria are met. Agents can also be used to run commands or system queries remotely, identifying IOCs and helping perform other live forensics or incident response tasks.

KNIGHTVISION CAM BY AVALONCyber

Organizations take up to **197 DAYS** on an average to detect data breaches

Companies that contain a data breach in **less than 30 days** are expected to save **over $1M in finances**[4]

ADVANTAGES OF KNIGHTVISION CAM

- **Cost.** We know we keep repeating it, but it's a fact that cost is a huge factor in the decision-making process. KnightVision CAM is, by design, more affordable, through its use of opensource technology and its tiered structure. This is one instance when a bespoke service actually saves you money.
- **Customizable.** Services. Dashboards. Reports. All of these can be tailored to meet the security and compliance needs of your business.
- **Ease of use.** Our dashboards were created with the end user in mind. Intuitive design allows CIOs and CEOs alike to get an in-depth look at your IT environment. The single pane of glass offered by Tiers 1 and 2 assist your team with compliance obligations and allow them to detect and respond to alerts more quickly and accurately, while Tiers 3 and 4 are completely managed by our team, so you can focus on your business.
- **Long-term storage.** Storing log data for an extended time, for the purposes of compliance, can be extremely expensive. Our infrastructure allows data that no longer needs to be indexed and reported on to transfer automatically to cold storage, like Amazon Glacier, which is significantly more cost effective.
- **Saves time.** By automating everything from compliance reports to long-term storage – or passing off management of the entire KnightVision CAM offering to our cyber experts – your team can focus on other important tasks.

KnightVision CAM was designed to provide your business with peace of mind. While there's an incredible amount of work you'll still need to do to meet compliance regulations and detect and prevent cyberattacks, this new service offering presents you with the tools – and the team – to help you achieve your cybersecurity requirements and goals.

[1] https://blog.netwrix.com/2016/03/15/infographics-common-drawbacks-of-siem-solutions/

[2] https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

[3] https://cybersecurityventures.com/jobs/

[4] https://www.ibm.com/downloads/cas/AEJYBPWA

ABOUT AVALON CYBER

In addition to KnightVision CAM, Avalon Cyber offers a full suite of cyber services, including vulnerability assessments, penetration tests, and managed detection and response (MDR). The men and women who support our managed security services have decades of experience in information security, have or previously have held top secret government clearances, and possess key industry certifications including: CISSP, OSCP, GPEN, CISM, CISA, CRISC, CCNA, CCE, CFCE, EnCE, and ACE.

Avalon Cyber is proud to work with clients in industries that include financial services, legal, healthcare, manufacturing, and telecommunications, who seek a greater level of data security – and we stand ready to assist with your cybersecurity needs too.

If you have questions or would like to speak to someone about implementing our KnightVision CAM services, contact our team today. We will walk you through the entire process, working with you to meet the unique needs of your business.

AVALONCyber

QUESTIONS?

For more information on any of our services, please contact:

Ian Gattie
Director of Marketing
ian.gattie@teamavalon.com