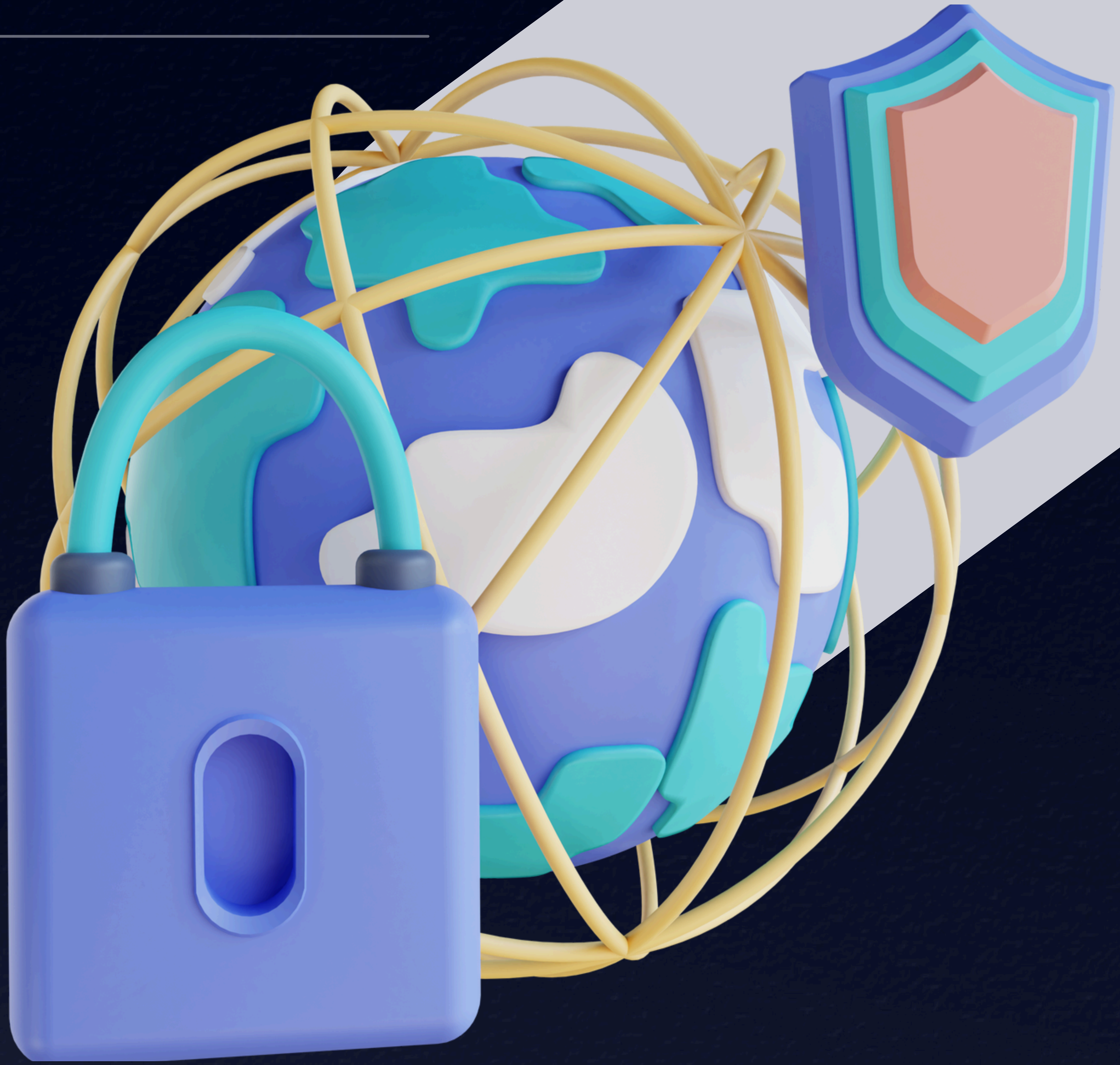
CYBERGUARDX

جامعة الإسكندرية
ALEXANDRIA UNIVERSITY
كلية الحاسبات وعلوم البيانات

Next Generation Secirty Operation Center

Empowering Security, Automating Defense



Graduation Project

02-24-01404 Project I

22-January-2025

Like pieces of a puzzle, our team combines unique skills to create CyberGuardX.

ABOUT OUR TEAM

Cyber Security Department

Faculty of Computers and Data Science,
Alexandria University

2024–2025

DR.
MOHAMED MOSTAFA ABBASY

SUPERVISOR

Dr. Mohamed Moustafa, Associate Professor of Computer Science and AI at Damanhour University and CIO, specializes in educational technology, instructional design, and digital transformation.
With a PhD in IT from Helwan University and 20+ years of experience, he is certified in Predictive Modeling and SAS Visual Analytics. Renowned for his research and teaching, he is a respected leader in IT and AI education.

OUR TEAM MEMBERS

Together, we innovate, secure, and protect.

Abdelrahman Usama Raslan

- Project Team Leader
- Security Operation Center (SOC) Manager

Ahmed Yasser Batour

- Penetration tester
- Network Security Manager

Ahmed Mahmoud ELSayed

- Network Engineer
- Web Developer

Rewan Salah Mahmoud

- Cyber Security Engineer
- Early Detection System Manager

Aya Mohamed Abdelrahman

- Designing and graph Specialist
- Data Loss prevention Manager

Youssef George Abdou

- System and Cloud Engineer
- Threat Intelligence Manager

Why is a Next-Generation SOC necessary now?

Contents

- Problem definition
- Our project : Cyberguardx
- Cyberguardx Component
- Problem Solving
- Research
- Future Work
- Practical Implementation

WHAT

PROBLEM DEFINITION

WE FACS

A WORLD UNDER ATTACK

Defining Cyber Security

Seattle Airport Cyber-Attack (August 2024): Ransomware disrupted travel systems ahead of Labor Day. Caused chaos in critical infrastructure at a major transportation hub.

LoanDepot Ransomware Attack (January 2024): Affected 16.6 million customers and disrupted mortgage payments. Resulted in $26.9 million in recovery costs.

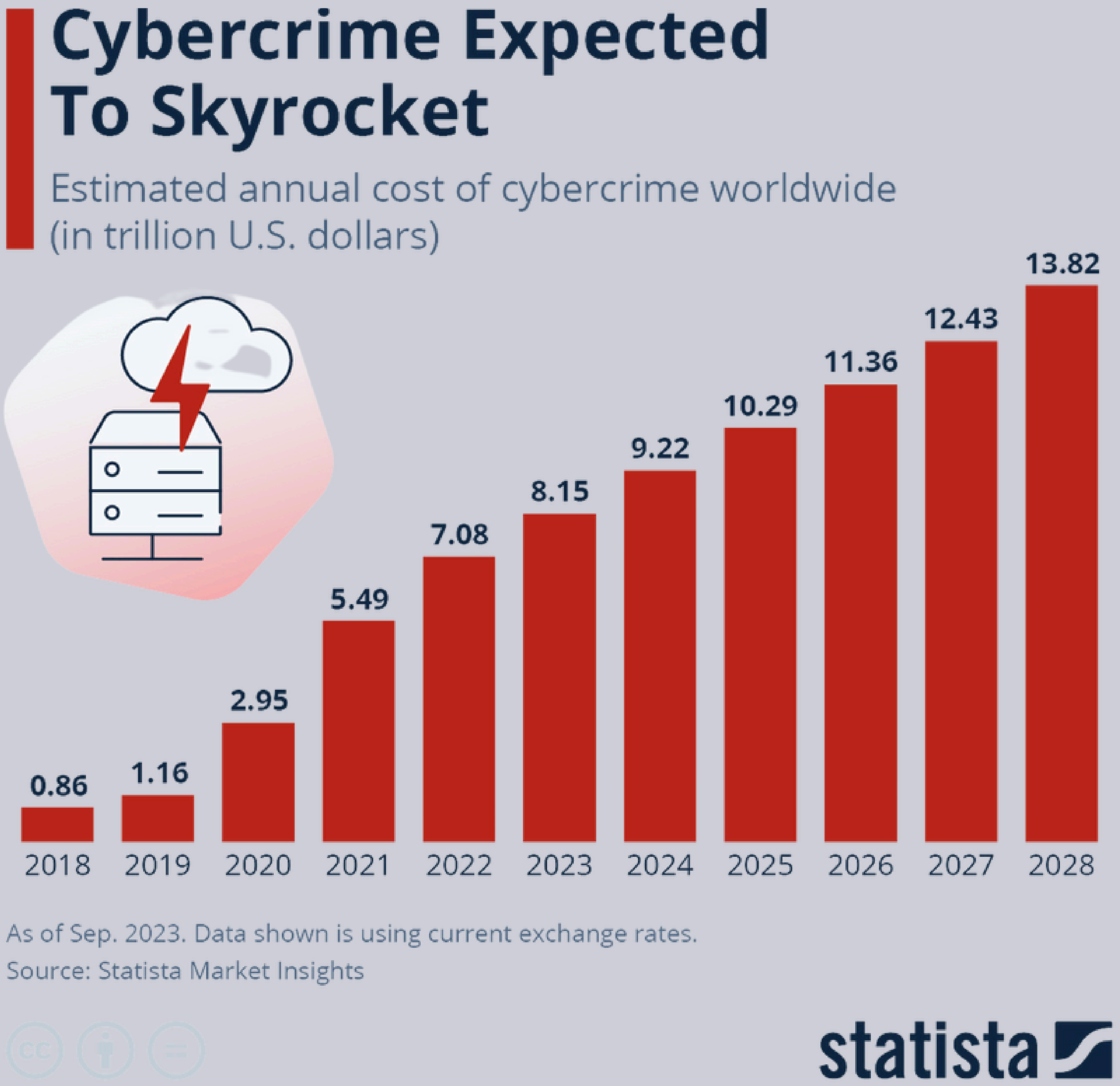
Volt Typhoon Espionage Campaign (2024): Infiltrated U.S. critical infrastructure (energy, transportation). Highlighted geopolitical threats from state-sponsored actors.

Change Healthcare Ransomware Attack (2024): Largest known healthcare data breach, exposing 100 million patient records. Showed healthcare is no longer "off-limits" for cybercriminals.

Colonial Pipeline Ransomware Attack (2021): Shut down fuel supply to the U.S. East Coast. Highlighted risks to critical infrastructure.

WHY IS CYBER SECURITY IMPORTANT?

The Growing Need for Cyber Security



Cybercrime Expected To Skyrocket

Estimated annual cost of cybercrime worldwide (in trillion U.S. dollars)

As of Sep. 2023. Data shown is using current exchange rates.
Source: Statista Market Insights

Global cybercrime costs are projected to reach $13.82 trillion by 2028, reflecting the exponential growth of cyber threats

Data Breaches : Unauthorized access to sensitive information causing severe financial and legal repercussions

Financial Loss: Direct costs from cyber incidents, including ransom payments and recovery expenses

Reputational Damage: Long-term erosion of customer trust and brand value.

National Security & Interdependence: Risks to critical infrastructure and the interconnected digital economy

SECURITY OPEARTION CENTER (SOC)

The SOC is a dedicated team responsible for real-time monitoring and analysis of an organization's security posture. They defend against cyber threats, respond to incidents, and ensure continuous protection of digital assets.

T1 : Analyst & Alert

are the frontline defenders, continuously monitoring systems and detecting threats in real-time.

T2 : Incidence Responder

step in to investigate alerts and resolve incidents, ensuring minimal impact.

T3 : Expert & Threat Hunter

handle complex and escalated incidents, using advanced techniques to address sophisticated threats.

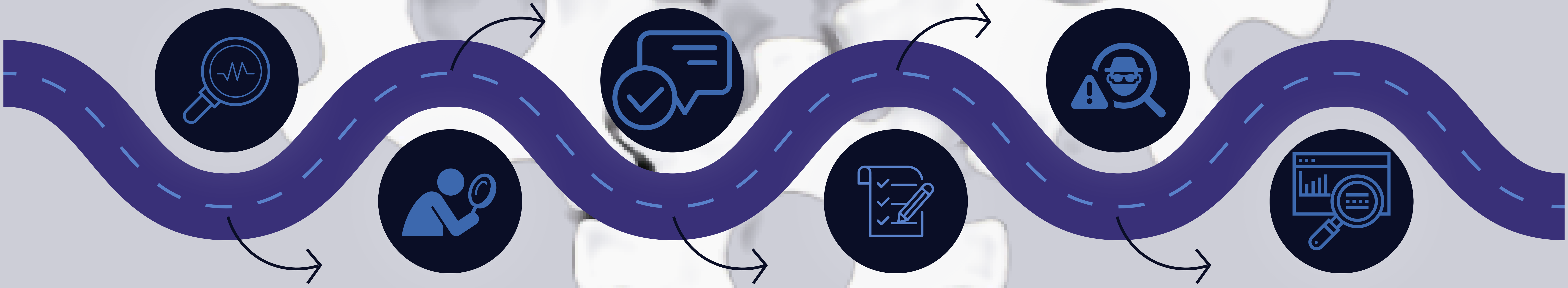
SOC Manager

oversee the team, develop strategies, and ensure that the SOC operates efficiently.

SOC Administrators

ensure that all tools and systems function seamlessly to support the SOC's operations.

SECURITY OPERATION CENTER TOOLS



Security Information and Event Management (SIEM)

Centralized log aggregation, correlation, and real-time threat detection

Threat Intelligence Platforms (TIPs)

Collects and shares threat intelligence to predict and mitigate attacks

Endpoint Detection and Response (EDR)

Detects and responds to endpoint-level threats in real-time

Vulnerability Management

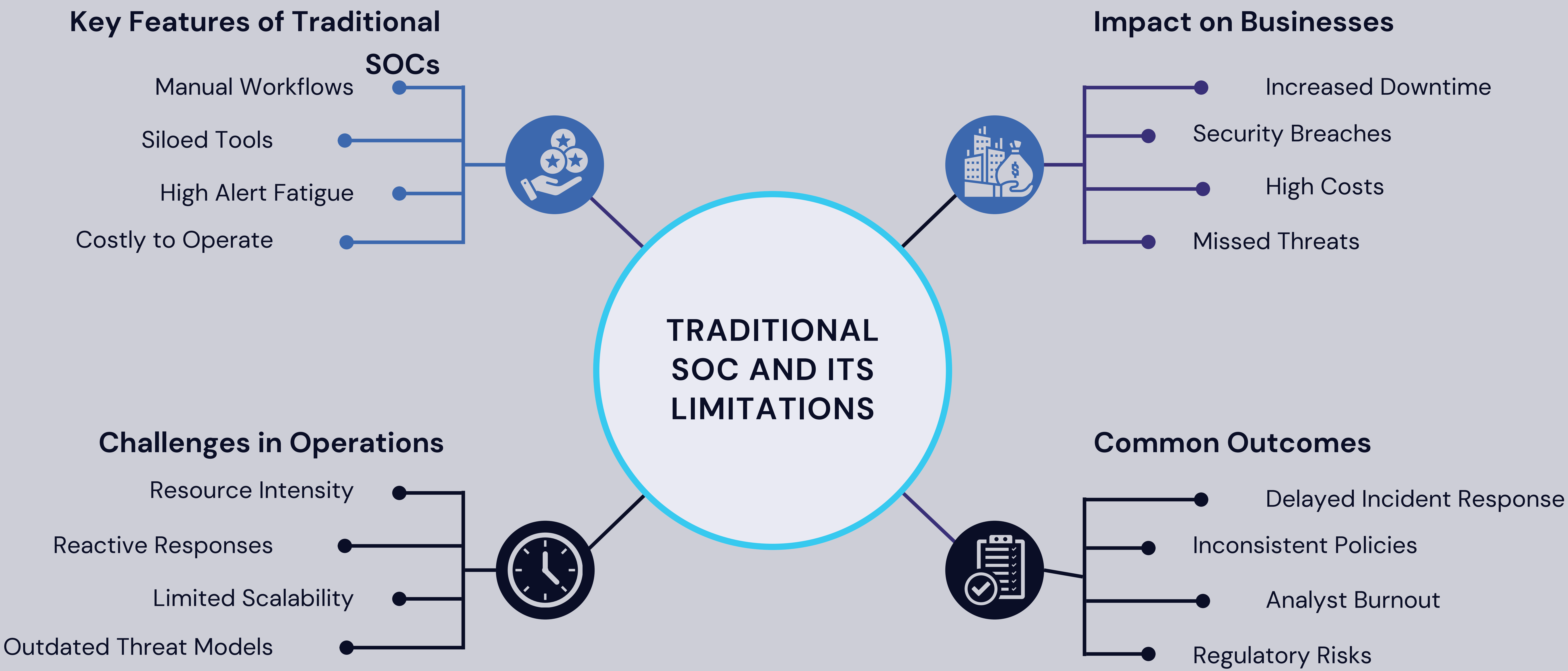
Scans for system vulnerabilities and offers remediation insights

Incident Response Platform

Streamlines incident response workflows and automates processes

Network Monitoring

Analyzes network traffic for anomalies and potential threats



TRADITIONAL SOC AND ITS LIMITATIONS

Key Features of Traditional SOCs

- Manual Workflows
- Siloed Tools
- High Alert Fatigue
- Costly to Operate

Impact on Businesses

- Increased Downtime
- Security Breaches
- High Costs
- Missed Threats

Challenges in Operations

- Resource Intensity
- Reactive Responses
- Limited Scalability
- Outdated Threat Models

Common Outcomes

- Delayed Incident Response
- Inconsistent Policies
- Analyst Burnout
- Regulatory Risks

IDEA OF

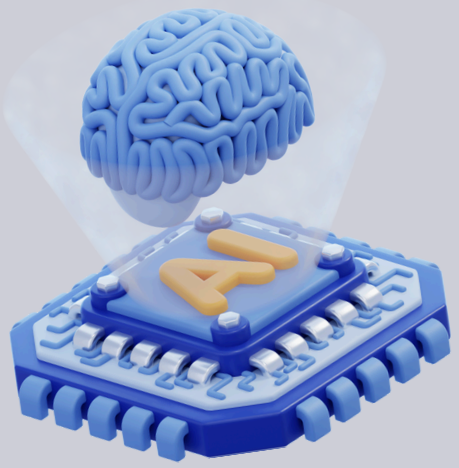
CYBERGUARDX PLATFORM

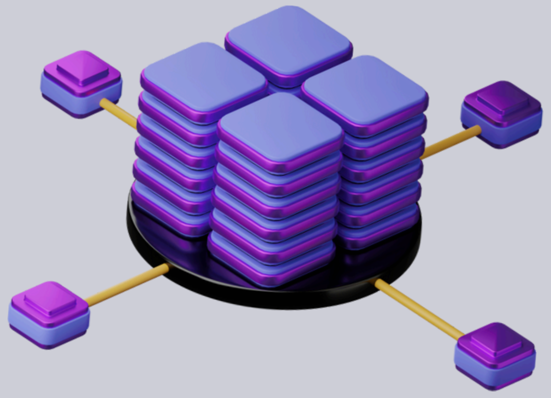
OUR PROJECT

Redefining Cyber Security & Security Operation Centers : CyberGuardX

OUR PROJECT

Next Generation SOC Platform





CyberGuardX represents the future of cybersecurity, integrating cutting-edge technologies like SIEM, SOAR, and UBA to create a secure, scalable, and efficient SOC platform. With collaboration and innovation as our core values, we aim to address evolving cyber threats and redefine defense strategies for the digital age.

HOW CYBERSECURITY WORKS

Protecting Your Digital Assets

Prevent

Tools like firewalls, antivirus software, and secure configurations to block threats.

Detect

Systems like SIEM, IDS, and continuous monitoring to identify suspicious activities.

Respond

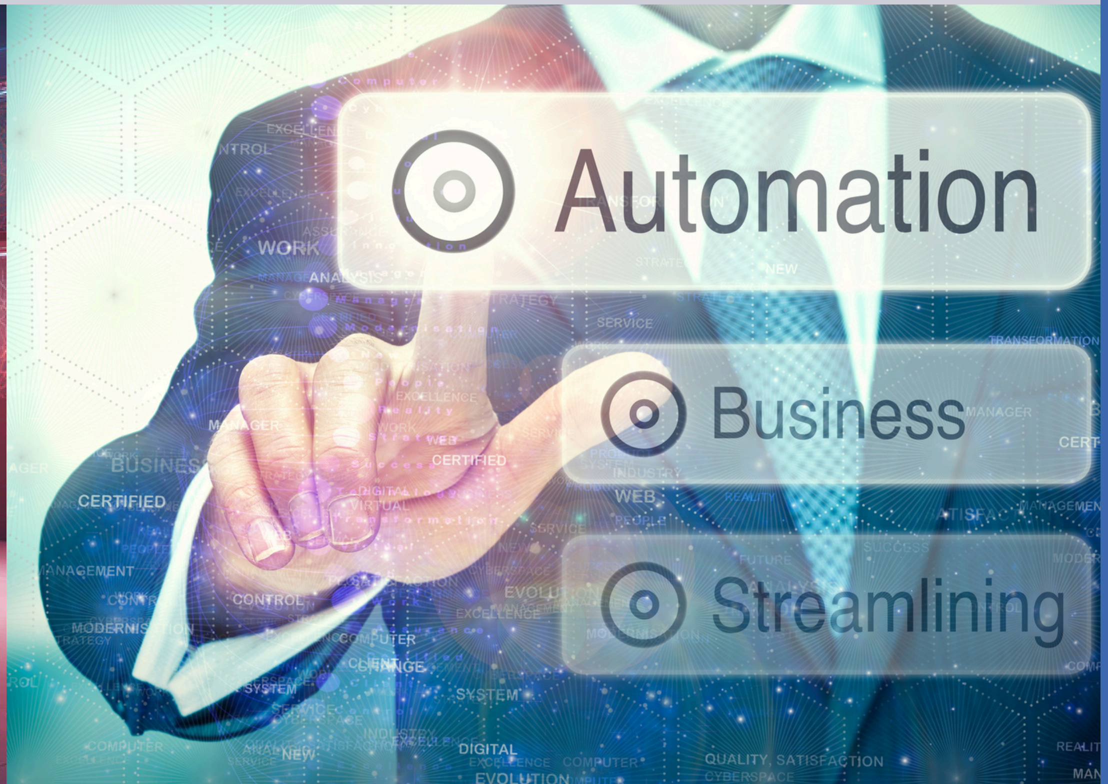
Incident response plans and recovery strategies to mitigate impacts.

NEXT-GENERATION SECURITY OPERATION CENTER (NGSOC)

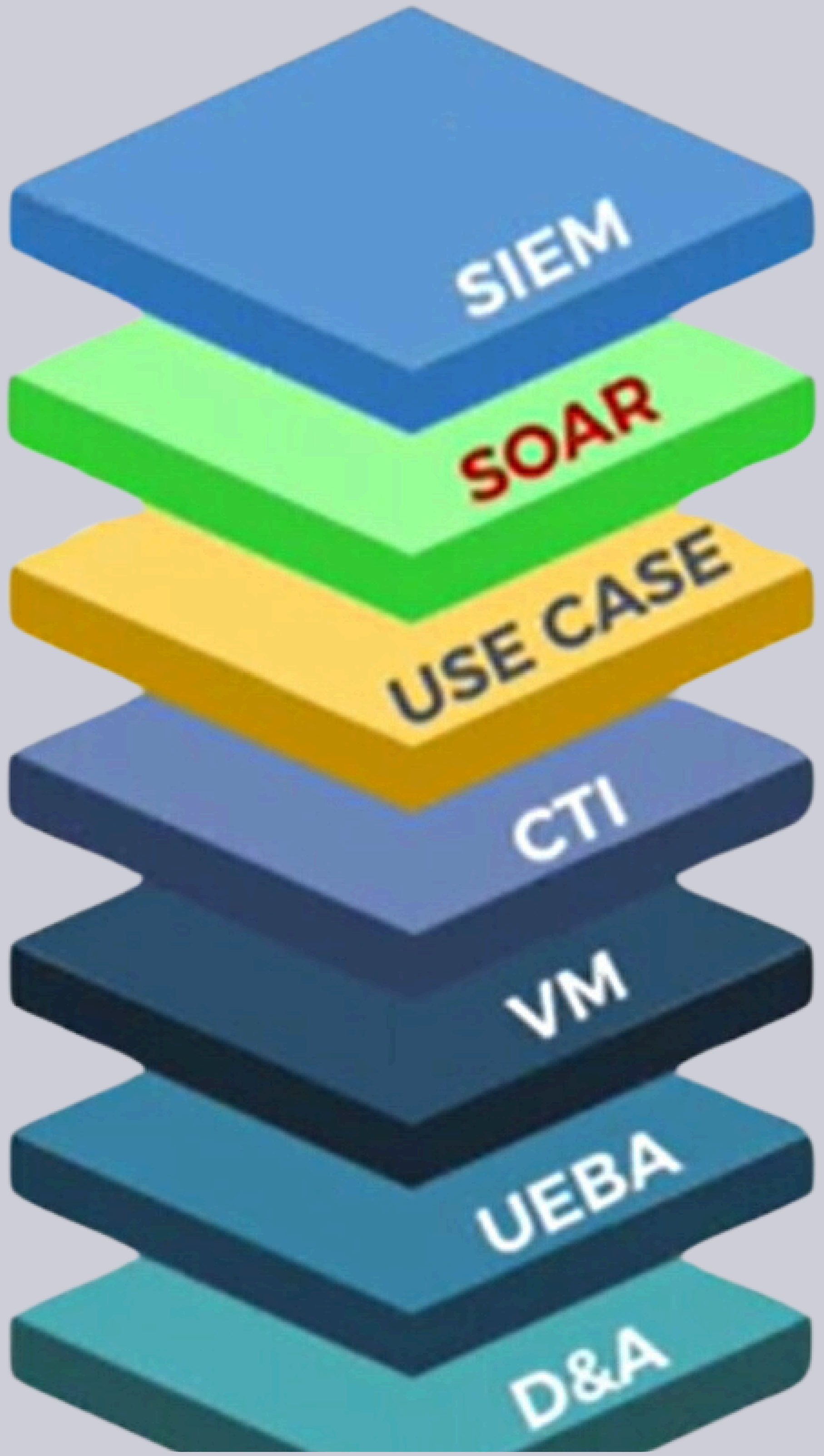
Transforming Cyber Security with Automation and Acritical Inelegance

A Next-Generation SOC leverages advanced technologies like AI, machine learning, automation, and integrated platforms to enhance threat detection, response, and prevention.

AI-Driven Threat Detection	Real-time detection with machine learning models to identify unknown threats
SOAR Integration	Security Orchestration, Automation, and Response (SOAR) for automated workflows
Behavioral Analytics	User and Entity Behavior Analytics (UEBA) to detect insider threats and anomalies
Cloud-Native Capabilities	Comprehensive coverage of hybrid and multi-cloud environments.
Threat Intelligence Integration	Real-time integration with global threat intelligence feeds



Next-Generation SOC Components



On-Prem or Cloud Native SIEM

CyberProof Security Orchestration, Automation & Response (SOAR) Platform

Custom Use Cases & Playbooks

Cyber Threat Intelligence

Vulnerability Management & DevSecOps

User & Entity Behavior Analysis

Deception & Anomaly Detection

Traditional SOC VS Next Generation SOC

Comparison between Traditional and Next-Generation SOC

	INTEGRATION	AUTOMATION	SCALABILITY	COLLABORATION	EFFICIENCY
Traditional SOC	✗ Manual integration of separate tools	✗ Reactive responses requiring manual intervention	✗ Limited scalability; requires more personnel as threats grow	✗ NOC and SOC operate in silos with minimal information sharing	✗ High resource consumption and longer resolution times
Next Generation SOC	✓ Seamless tool integration through unified platforms	✓ Automated workflows for faster incident response	✓ Scales efficiently with technology and infrastructure	✓ Teams collaborate seamlessly with integrated processes	✓ Optimized operations reducing cost and response time

Why Innovation is Essential for Modern SOC Capabilities

1. The Evolving Cyber-Threat Landscape
2. Advanced Persistent Threats (APTs)
3. Automation and Orchestration
4. Big Data Analytics
5. Integration and Collaboration
6. Cloud and Hybrid Environments
7. User Behavior Analytics (UBA)

What challenges do you think are most critical for SOC innovation?

CYBERGUARDX

Meet our website

SCAN ME

PALTFORM COMPONENT

These tools, when combined, form the foundation of CyberGuardX's robust defense system, ensuring comprehensive coverage against evolving cyber threats.

SIEM

SOAR

IPS/IDS

Firewall

Threat Intlegance

DLP

UBA

GRC

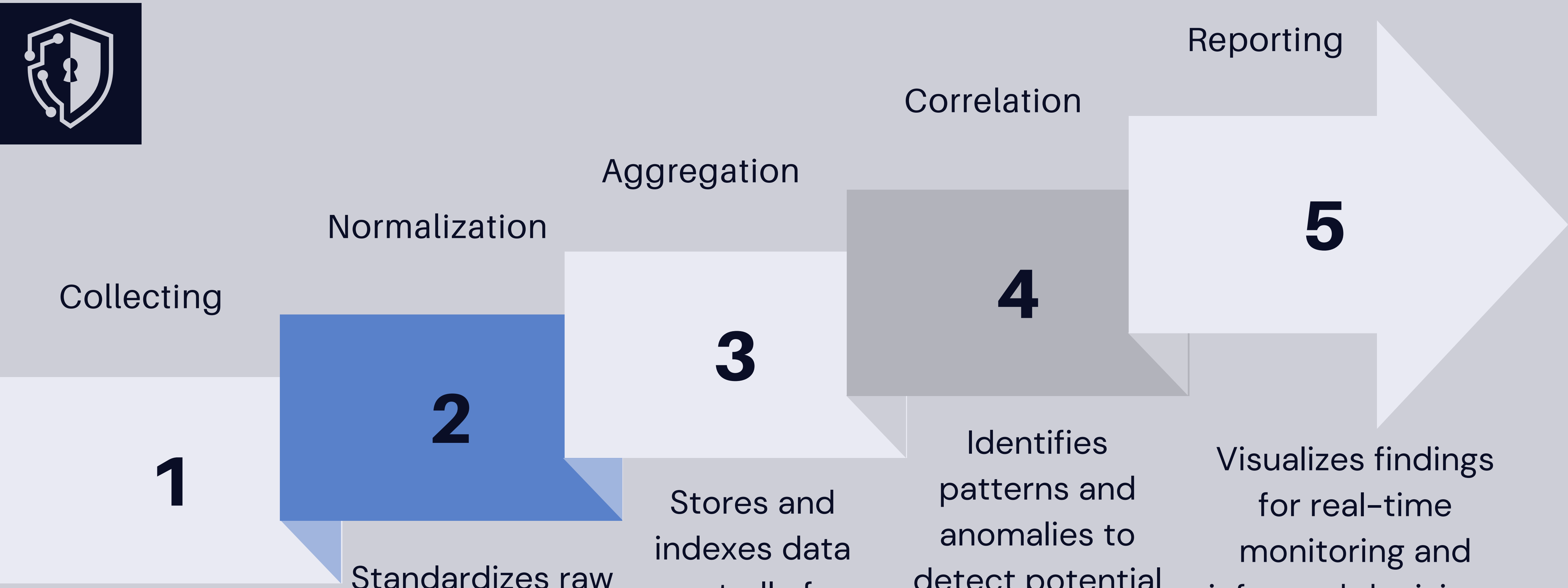
Honeypot

WHAT

CYBERGUARDX COMPONENT

OUR PROJECT

SIEM: EMPOWERING THREAT DETECTION WITH ELK STACK



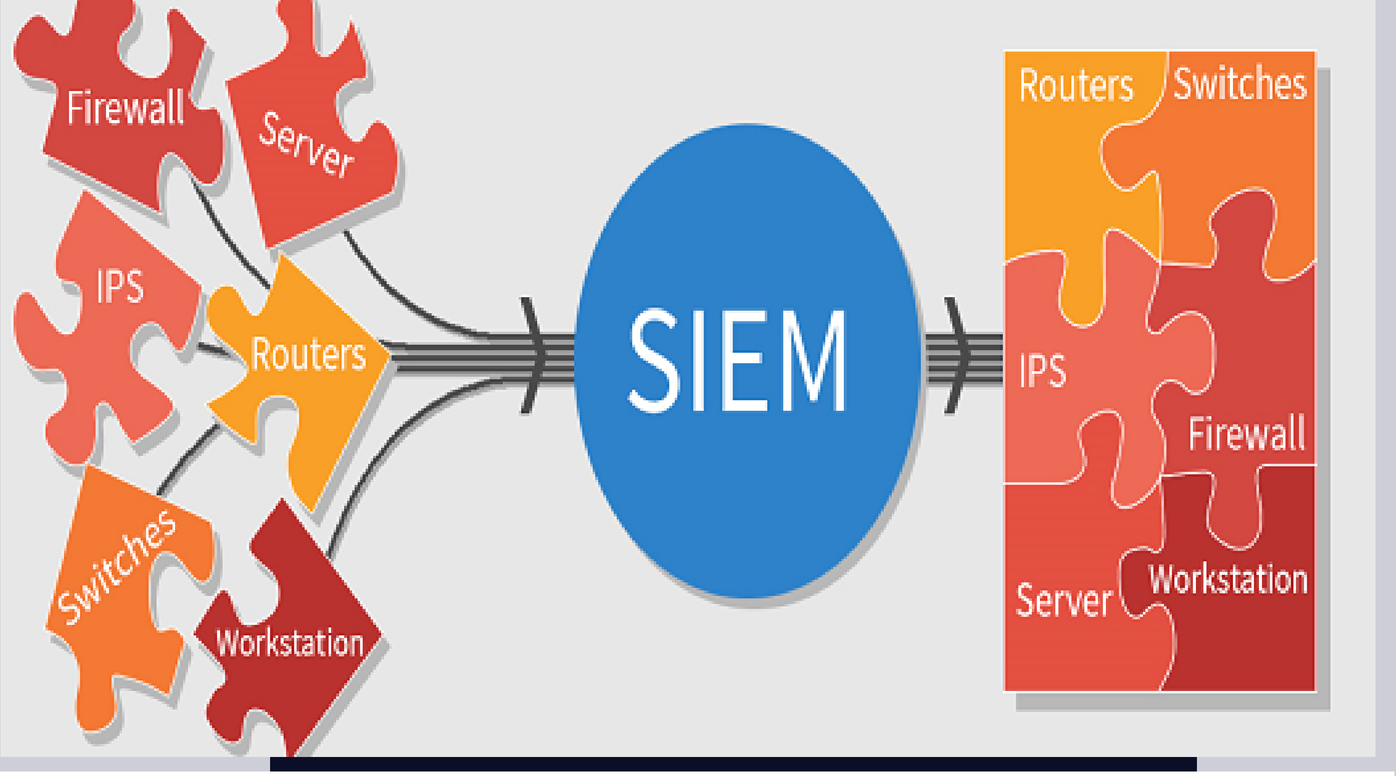
1. Gathers logs from diverse sources to capture all relevant data.

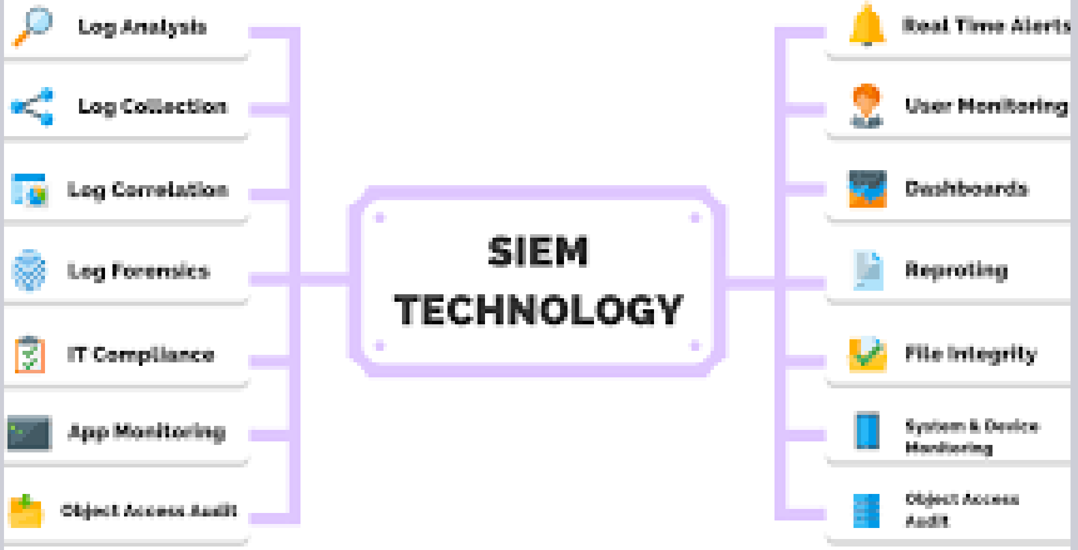
2. Standardizes raw logs into a unified format for easier analysis.

3. Stores and indexes data centrally for quick access and searchability.

4. Identifies patterns and anomalies to detect potential threats.

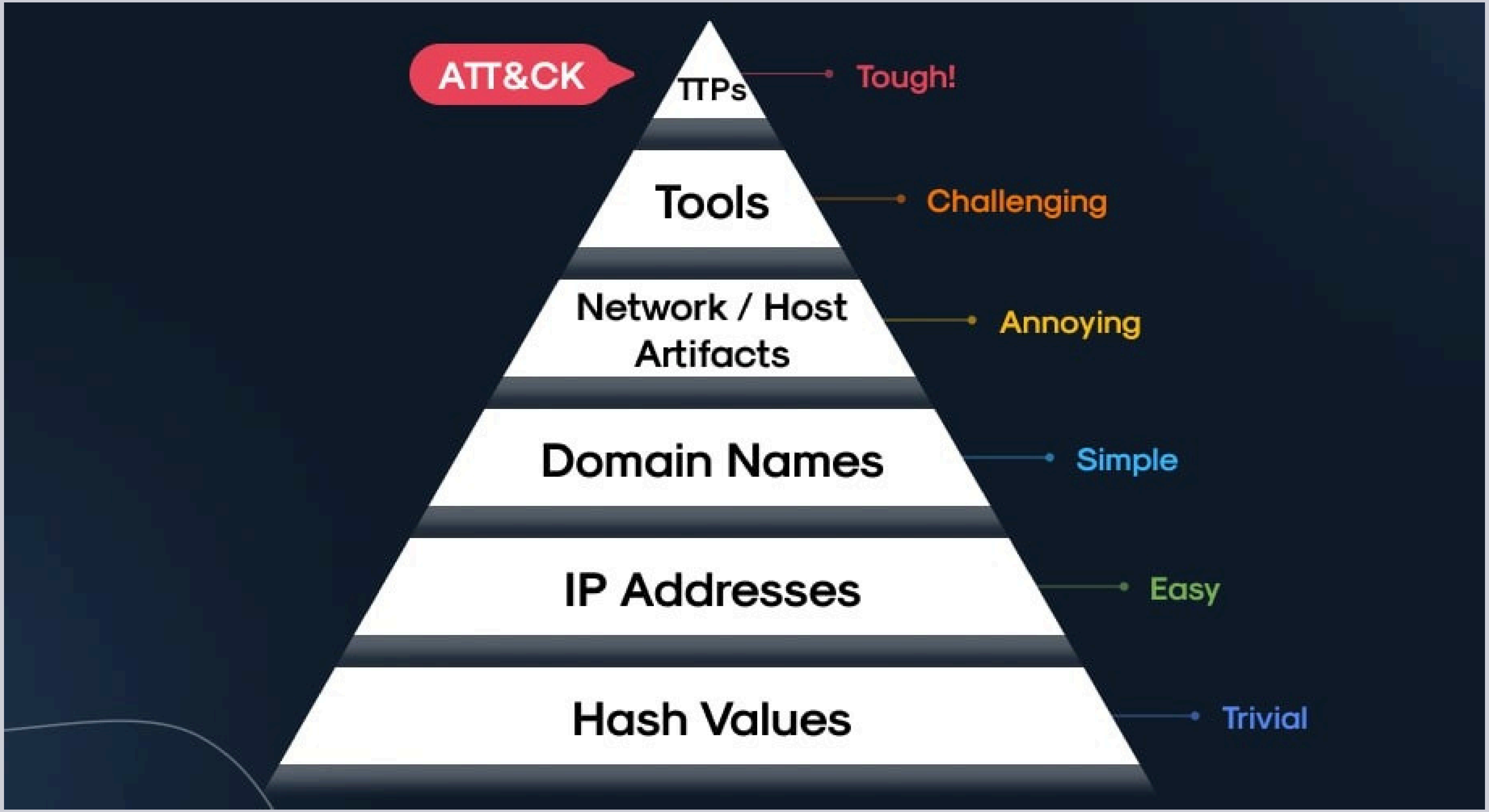
5. Visualizes findings for real-time monitoring and informed decision-making.





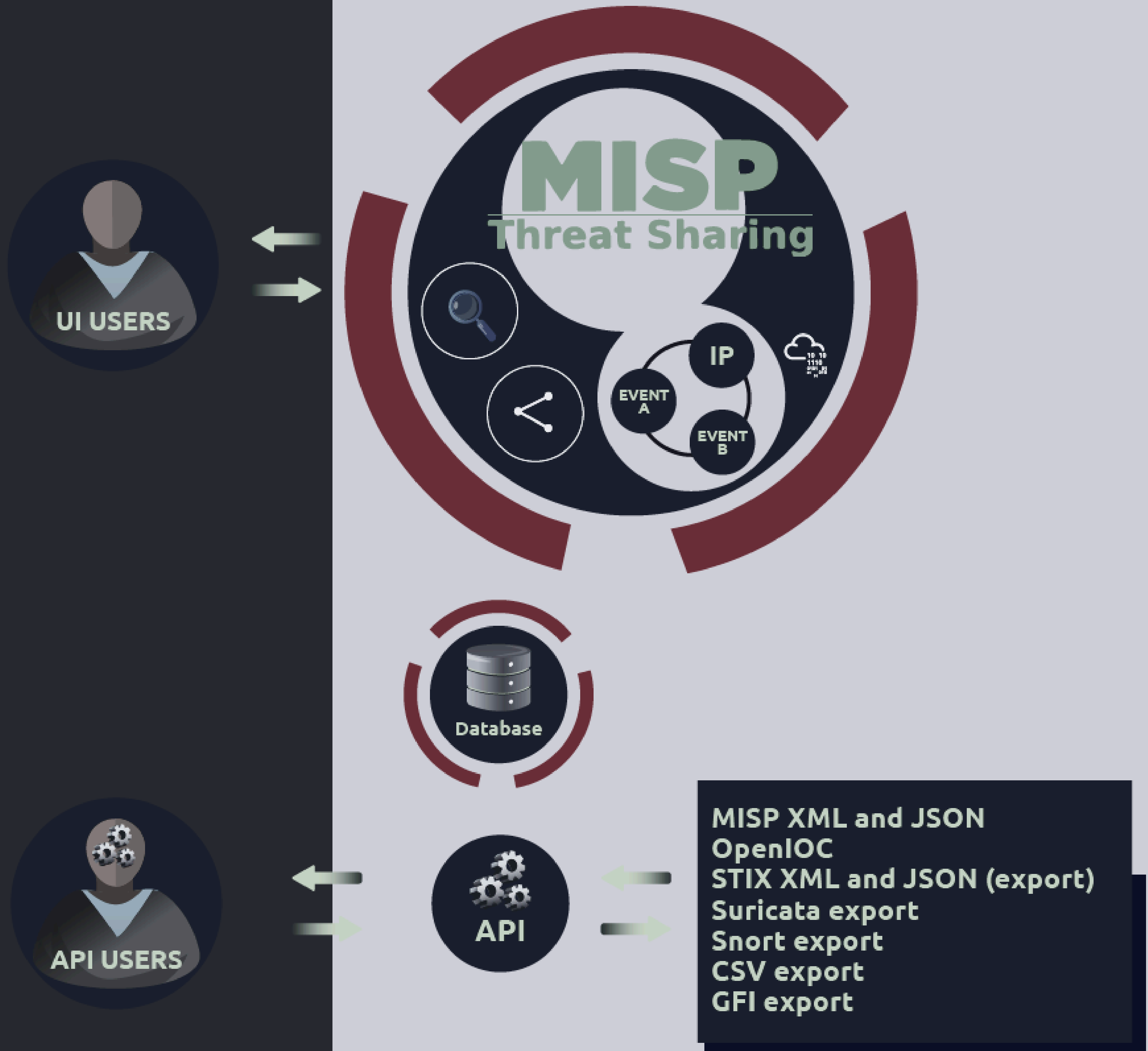
THREAT INTELLIGENCE & THREAT INTELLIGENCE PLATFORMS (TIP)

MITRE ATT&CK™



MALWARE INFORMATION SHARING PALTFORM

Centralizing Threat Data for Effective Incident Response



MISP XML and JSON
OpenIOC
STIX XML and JSON (export)
Suricata export
Snort export
CSV export
GFI export

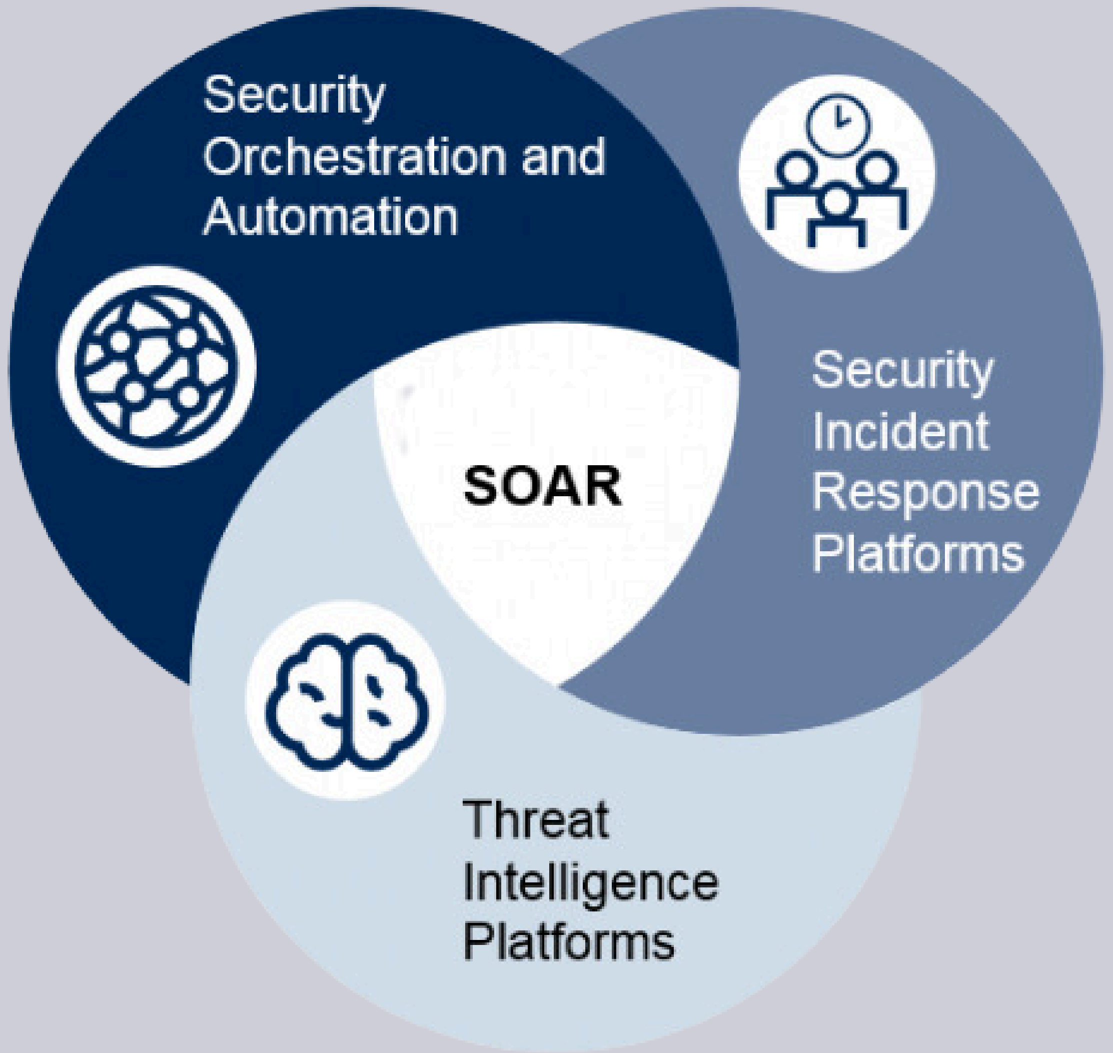
WHY USE MISP IN SOC?

Using MISP within a Security Operations Center (SOC) significantly enhances threat detection, investigation, and response by providing centralized access to actionable threat intelligence. MISP facilitates the sharing of malware and threat indicators, ensuring SOC teams can collaborate effectively and stay proactive against emerging cyber threats. It integrates with user interfaces (UI) for analysts, databases for storing threat intelligence, and APIs for automation, supporting various formats like STIX, JSON, and OpenIOC. By turning raw threat data into meaningful insights, MISP empowers organizations to reduce risks, improve their security posture, and respond efficiently to incidents.

SOAR

Streamlining Security Operations with Automation and Orchestration

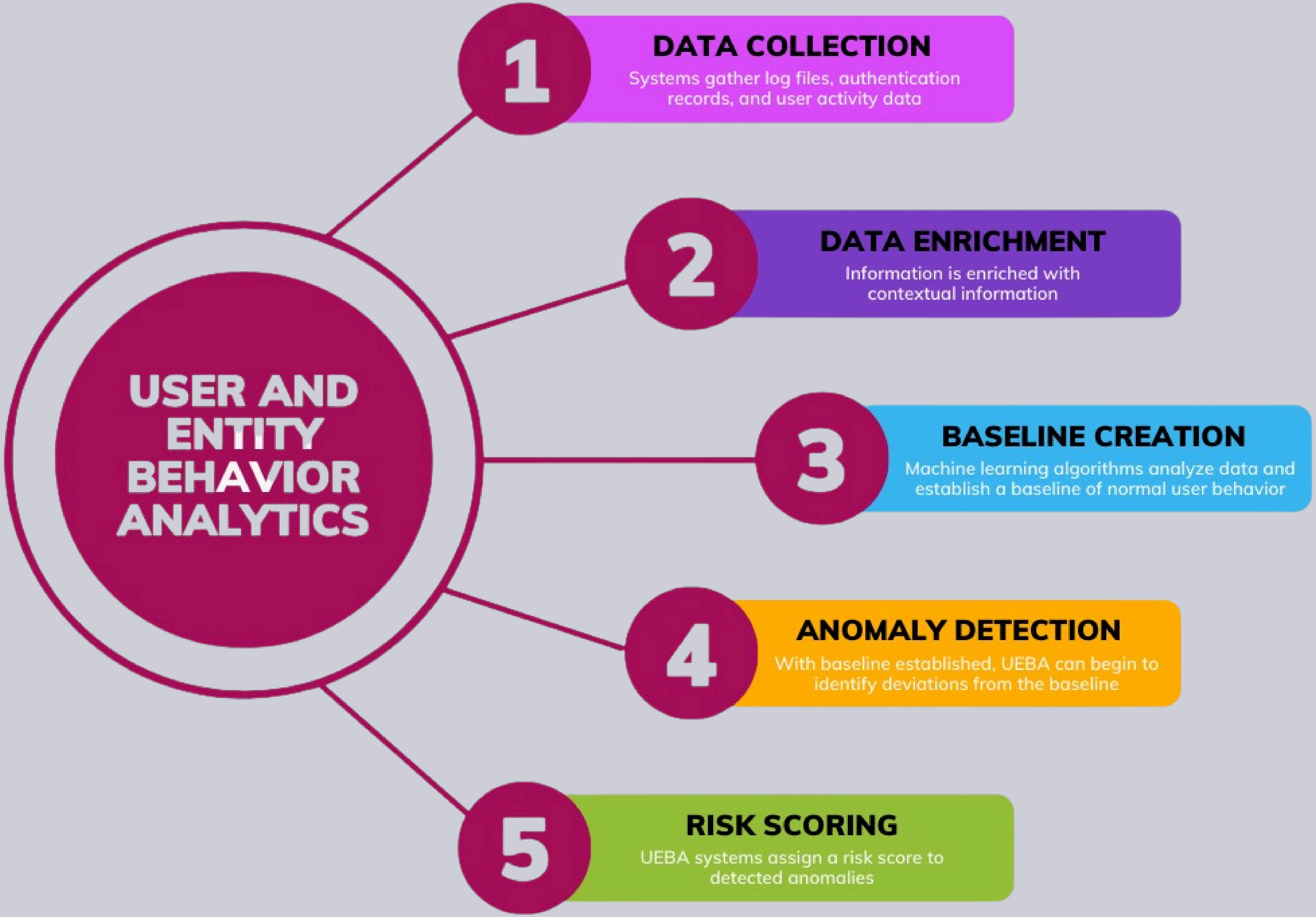
Threat Detection → Alert Prioritization → Automated Response


Security Orchestration and Automation
Security Incident Response Platforms
SOAR
Threat Intelligence Platforms

SOAR = SOA + SIR + TIP

SIEM	SOAR
✓ Aggregates logs	✓ Aggregates security alerts and threat intelligence
✓ Generates alerts	✓ Ingests alerts from SIEM and other tools
✓ Analyzes data to identify potential threats	✓ Enriches and correlates alerts to determine risk
✓ Limited response workflows	✓ End-to-end, automation-powered response workflows
✓ Notifies users and analysts of suspicious activity	✓ Orchestrates actions across integrated tools

User Behavior Analysis (UBA)



USER AND ENTITY BEHAVIOR ANALYTICS

1 **DATA COLLECTION**
Systems gather log files, authentication records, and user activity data

2 **DATA ENRICHMENT**
Information is enriched with contextual information

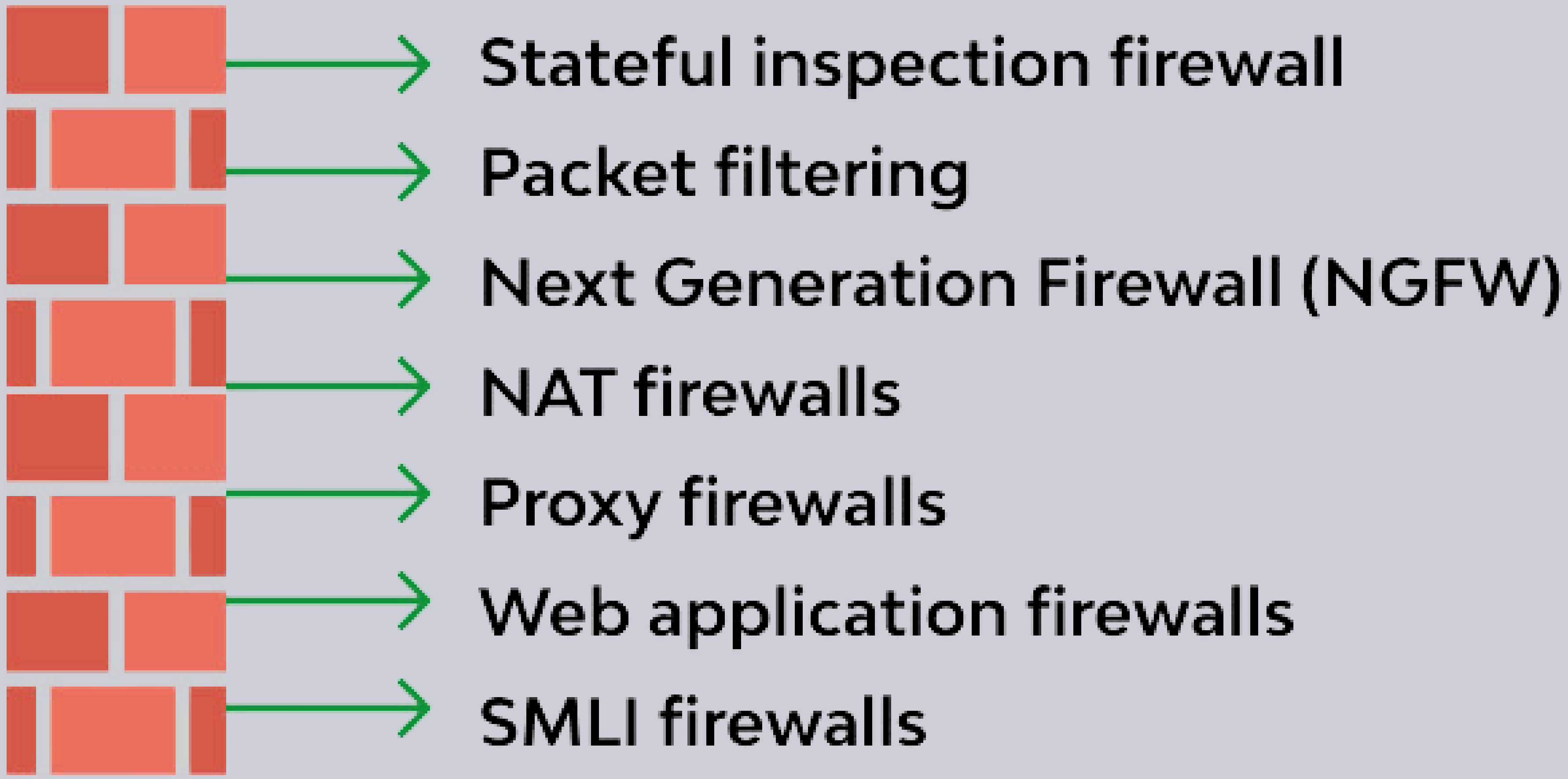
3 **BASELINE CREATION**
Machine learning algorithms analyze data and establish a baseline of normal user behavior

4 **ANOMALY DETECTION**
With baseline established, UEBA can begin to identify deviations from the baseline

5 **RISK SCORING**
UEBA systems assign a risk score to detected anomalies

Firewall

First Line of Defense in Network Security



- Stateful inspection firewall
- Packet filtering
- Next Generation Firewall (NGFW)
- NAT firewalls
- Proxy firewalls
- Web application firewalls
- SMLI firewalls

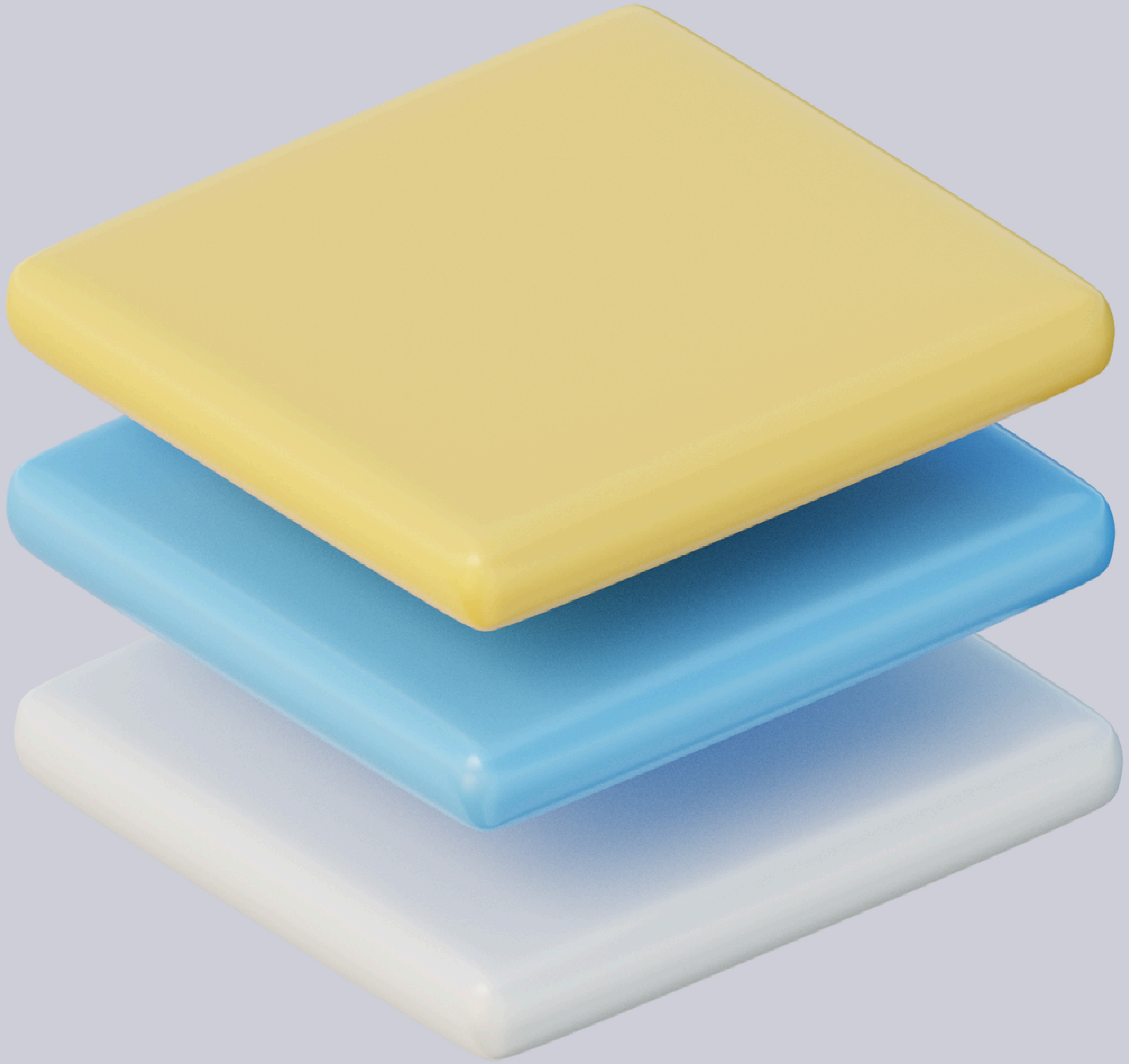
FORTINET

Intrusion Prevention System (IPS)

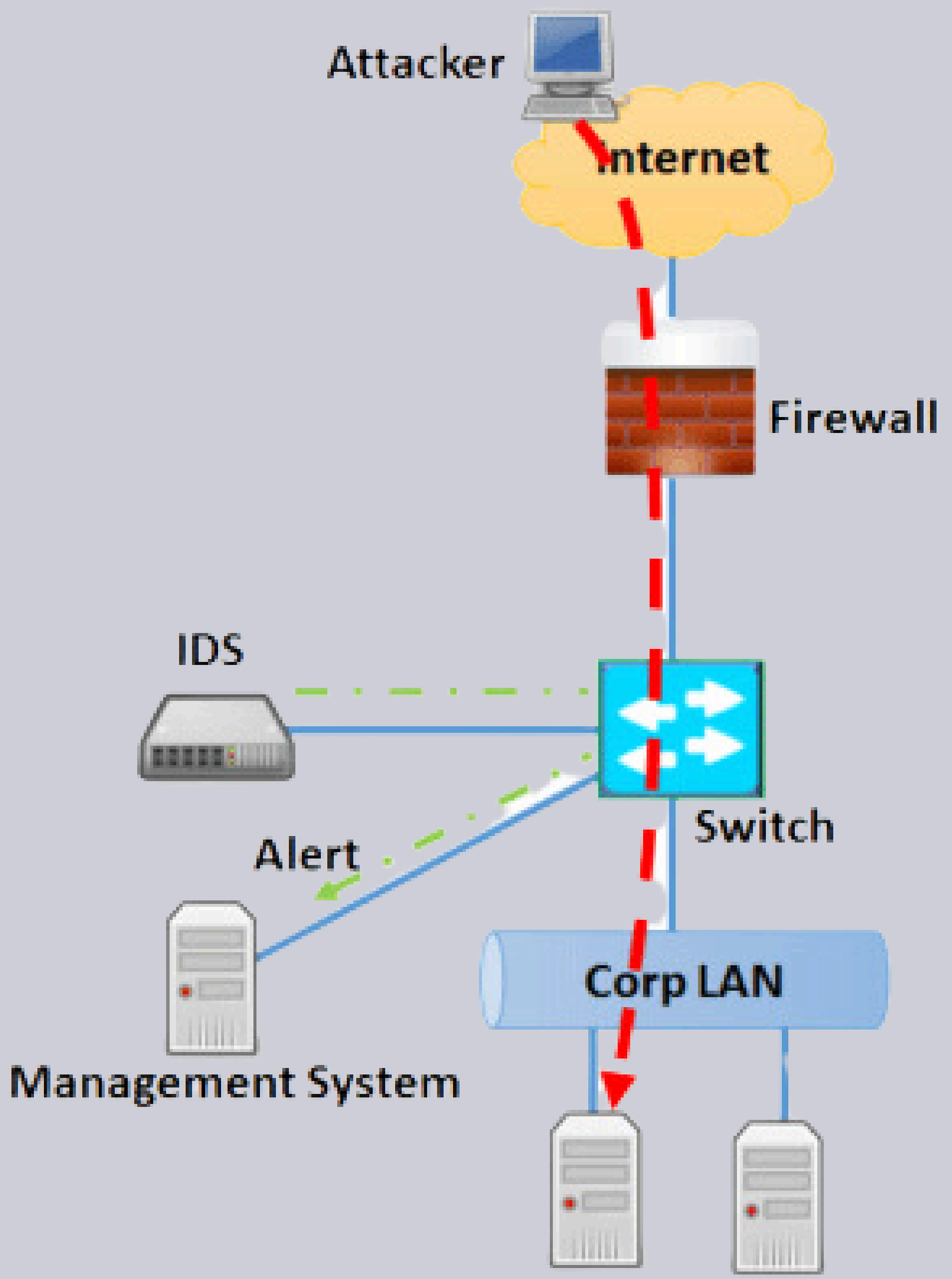
Signature-based
Relies on known threat patterns (signatures) from tools like antivirus software and firewalls to block threats.

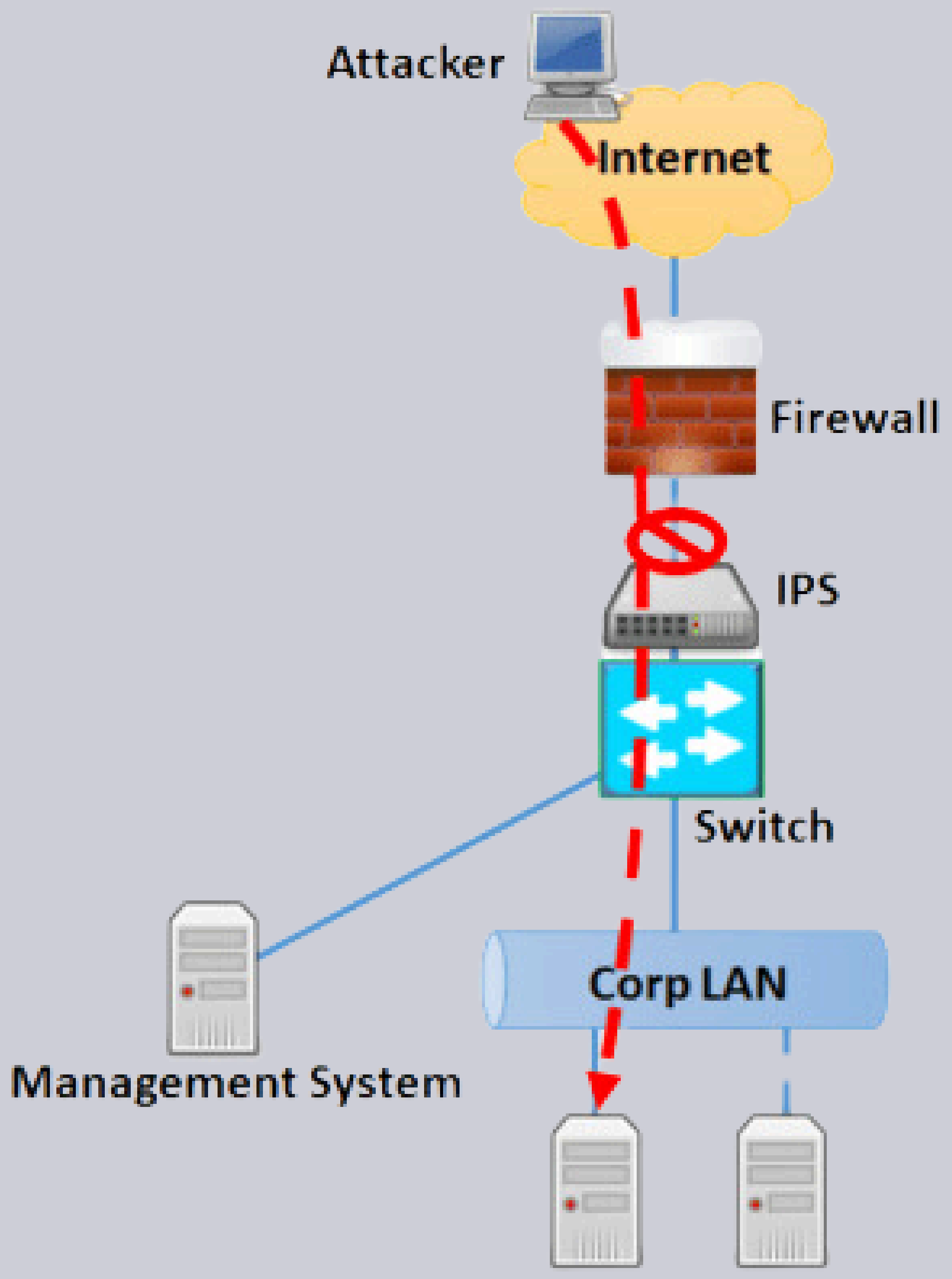
Behavior-based
Analyzes system behavior using tools like SIEM and IDS to detect anomalies and suspicious activities.

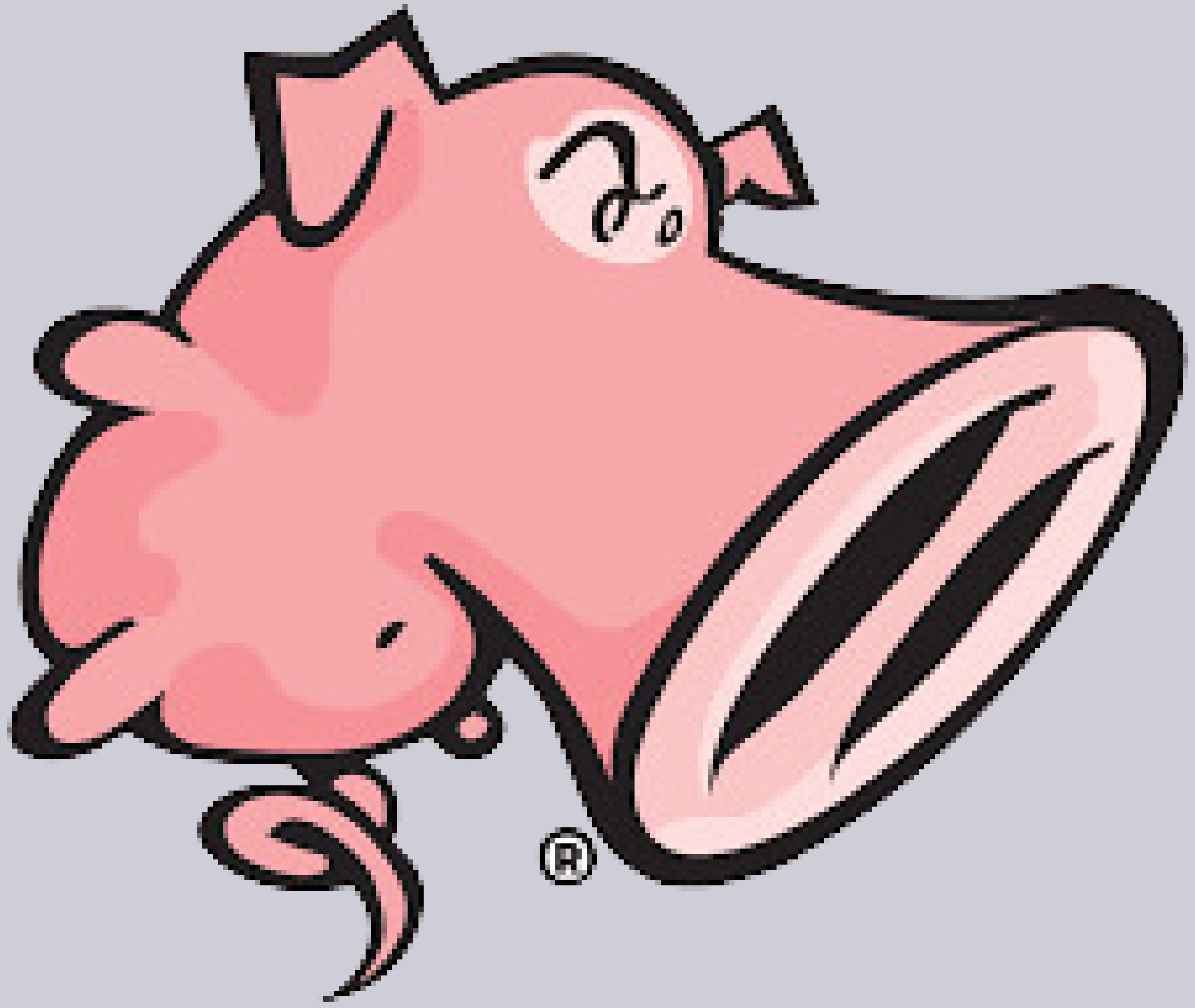
Role-based
Focuses on implementing incident response strategies and recovery plans tailored to specific roles and responsibilities



Intrusion Prevention and Detection System (IPDS) with Snort







Snort is an open-source network intrusion detection and prevention system (IDS/IPS) capable of real-time traffic analysis and packet logging.

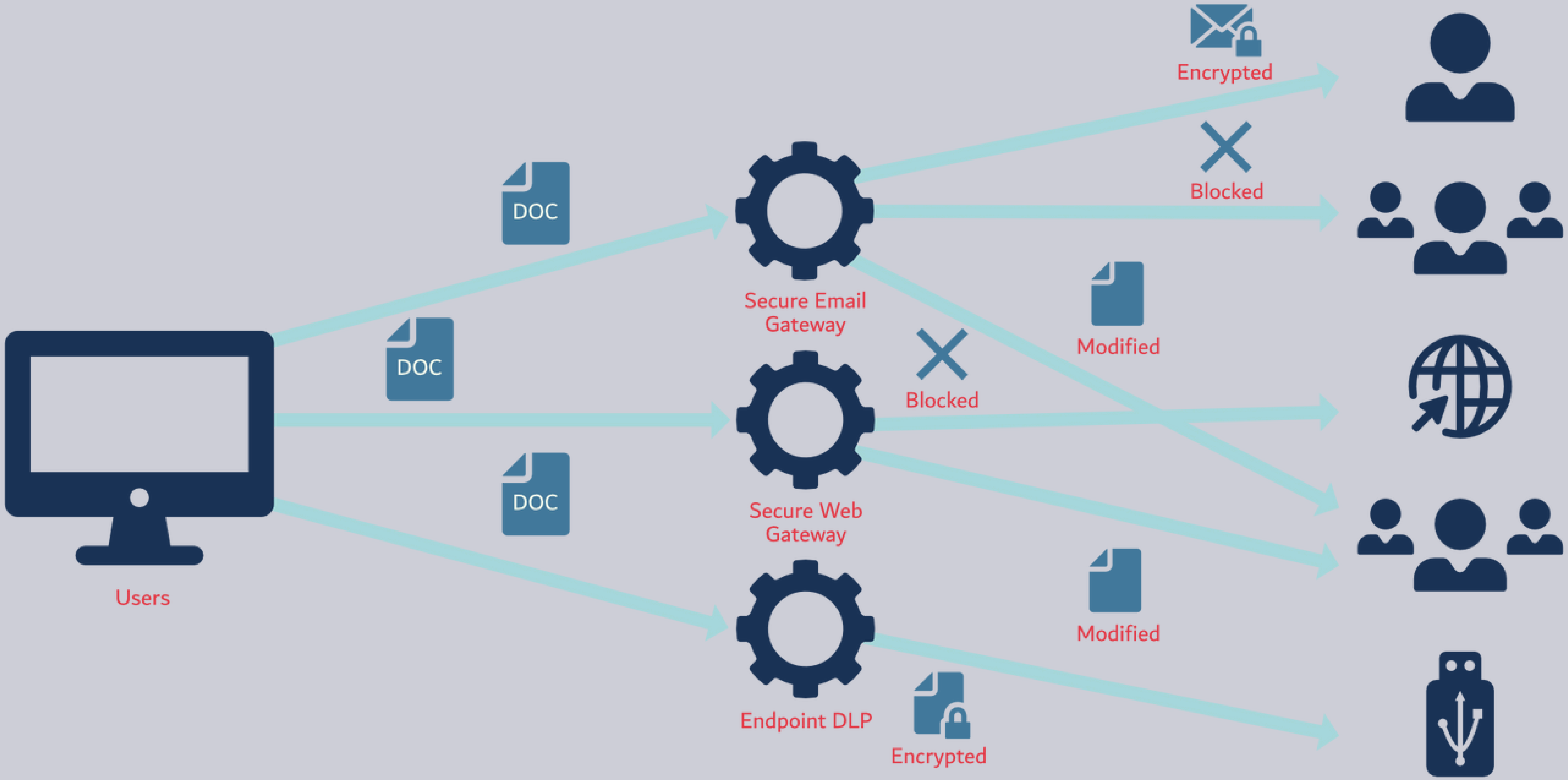
Honeypot and Early Warning System

Honeypot Implementation for Early Threat Detection

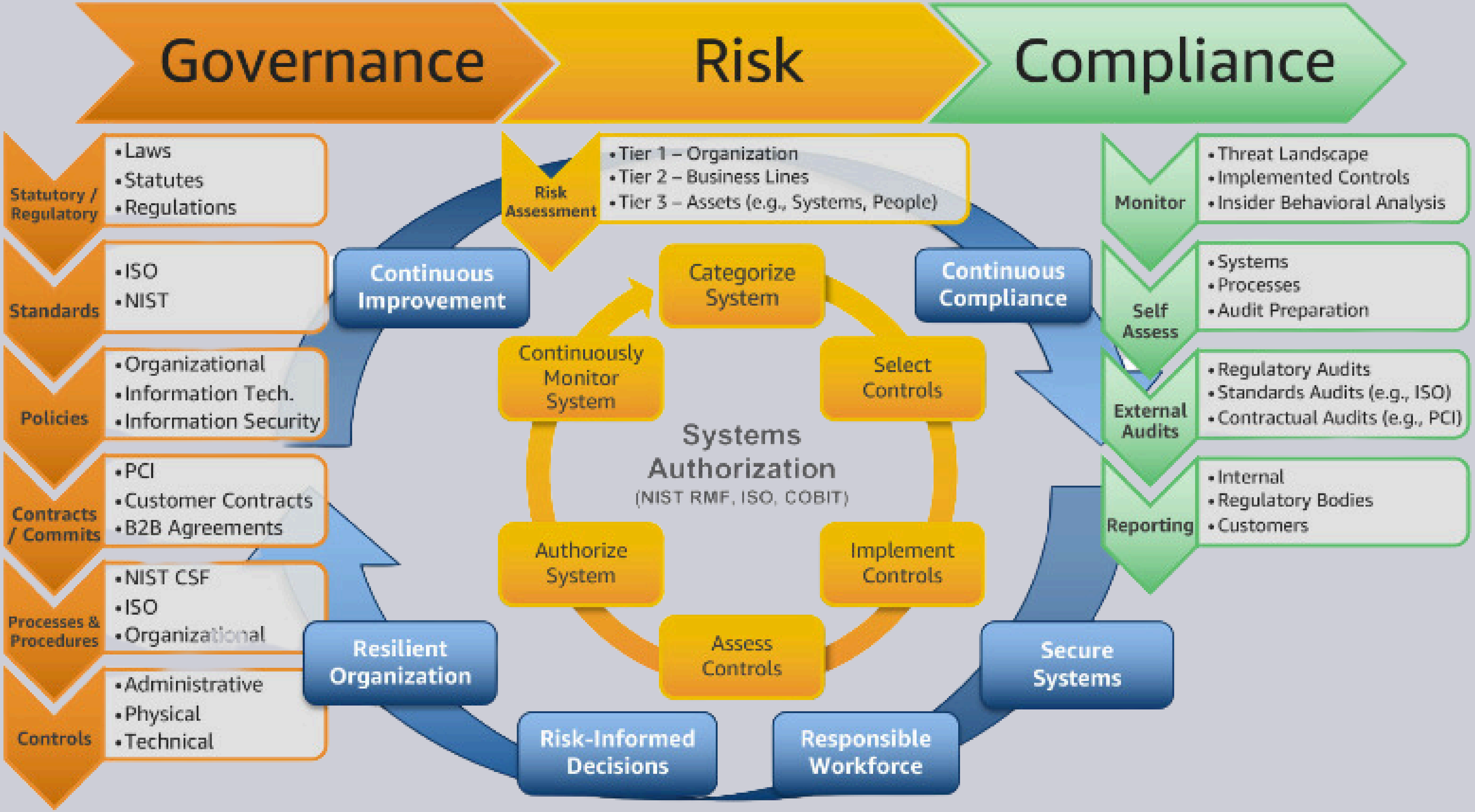
A honeypot is a decoy system designed to attract attackers, study their behavior, and secure the actual network.

By simulating vulnerabilities, honeypots detect malicious activity, providing real-time alerts to SOC teams.

Data Loss Prevision (DLP)



GRC



Governance

Risk

Compliance

Statutory / Regulatory
- Laws
- Statutes
- Regulations

Standards
- ISO
- NIST

Policies
- Organizational
- Information Tech.
- Information Security

Contracts / Commits
- PCI
- Customer Contracts
- B2B Agreements

Processes & Procedures
- NIST CSF
- ISO
- Organizational

Controls
- Administrative
- Physical
- Technical

Risk Assessment
- Tier 1 – Organization
- Tier 2 – Business Lines
- Tier 3 – Assets (e.g., Systems, People)

Continuous Improvement

Continuous Compliance

Categorize System

Select Controls

Implement Controls

Assess Controls

Authorize System

Continuously Monitor System

Systems Authorization

(NIST RMF, ISO, COBIT)

Resilient Organization

Risk-Informed Decisions

Responsible Workforce

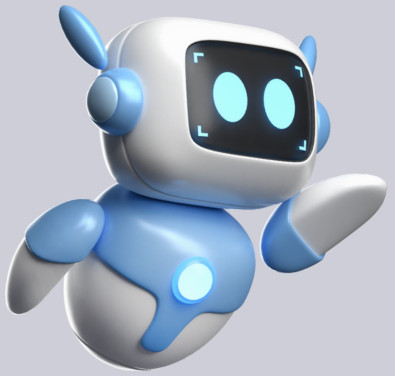
Secure Systems

Monitor
- Threat Landscape
- Implemented Controls
- Insider Behavioral Analysis

Self Assess
- Systems
- Processes
- Audit Preparation

External Audits
- Regulatory Audits
- Standards Audits (e.g., ISO)
- Contractual Audits (e.g., PCI)

Reporting
- Internal
- Regulatory Bodies
- Customers



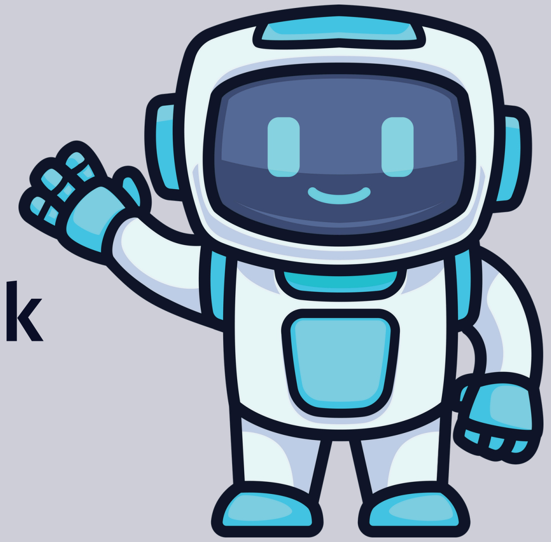
Machine learning and Cyber Security

Artificial intelligence (AI) is expected to play an increasingly important role in cybersecurity in the coming years

Machine learning can mitigate cyber threats and bolster security infrastructure through pattern detection, real-time cyber crime mapping and thorough penetration testing.With its range of applications, machine learning offers many advantages to IT and security personnel.

There are three types of machine learning used in cybersecurity: supervised learning, unsupervised learning and reinforcement learning.

machine learning used in Detecting threats in early stages Uncovering network vulnerabilities Reducing IT workloads and costs



How Machine Learning is Used in SOCs

1. Automating tasks

such as log analysis, threat hunting, and incident response. This frees up SOC analysts to focus on more complex tasks.

2. Improving detection rates

to improve detection rates by identifying patterns in data that are indicative of malicious activity. This can help SOC analysts to identify threats that would otherwise go undetected.

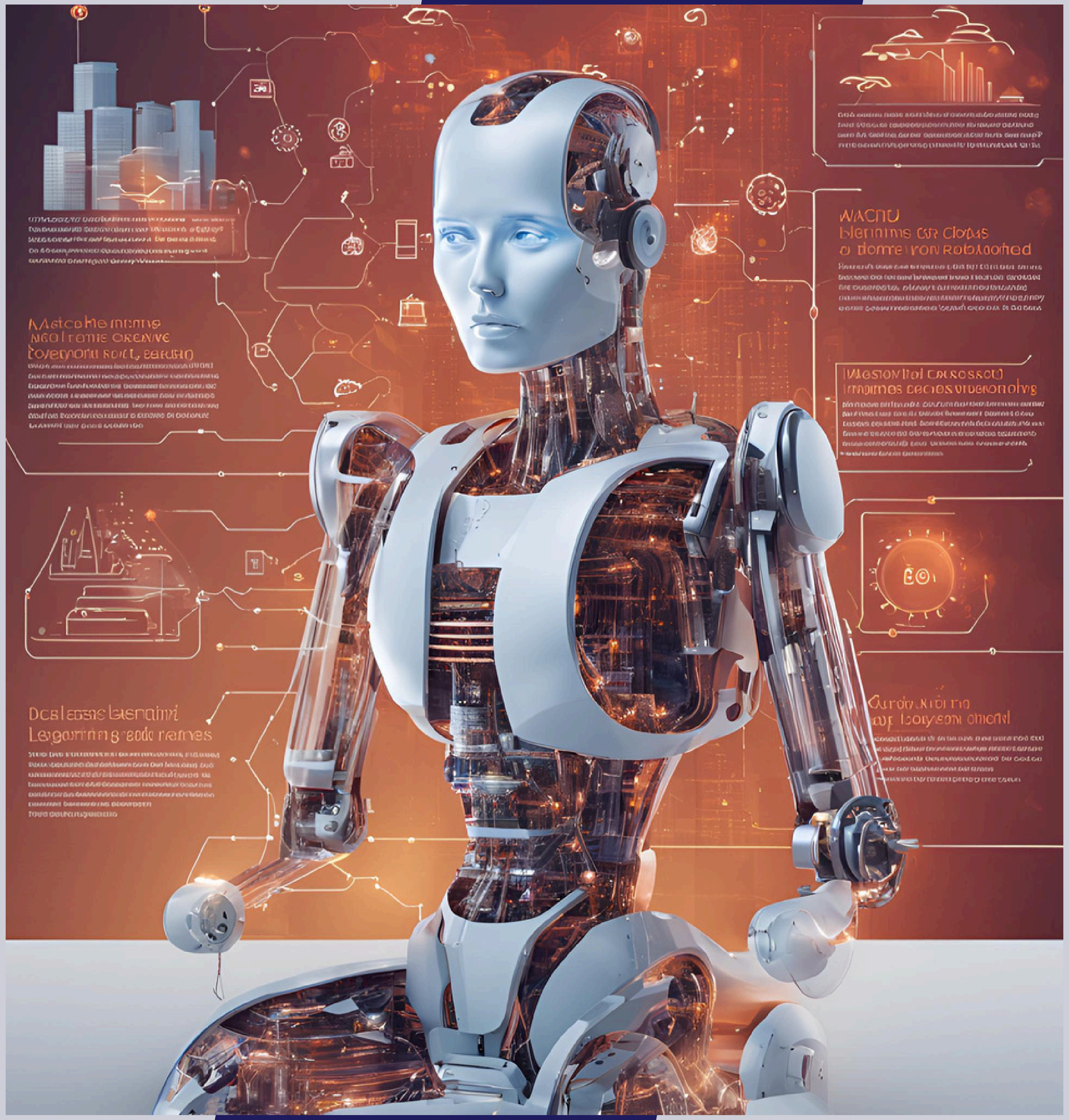
3. Reducing the time to respond to incidents

used to reduce the time it takes to respond to incidents by automating tasks such as triaging alerts and deploying mitigations. This can help organizations to contain incidents more quickly and minimize the damage.

Integration of Machine Learning in Next Generation SOC

SOC are responsible for protecting organizations from cyber threats. They do this by monitoring network traffic, detecting suspicious activity, and responding to incidents.

In recent years, machine learning has become increasingly important in SOCs. Machine learning can be used to automate tasks, improve detection rates, and reduce the time it takes to respond to incidents



User Behavior Analytics

NLP, combined with machine learning, can help in analyzing and understanding user behavior . By processing user activity logs, email communications, and other textual data, NLP models can identify deviations from normal behavior, detect insider threats, and flag suspicious activities.

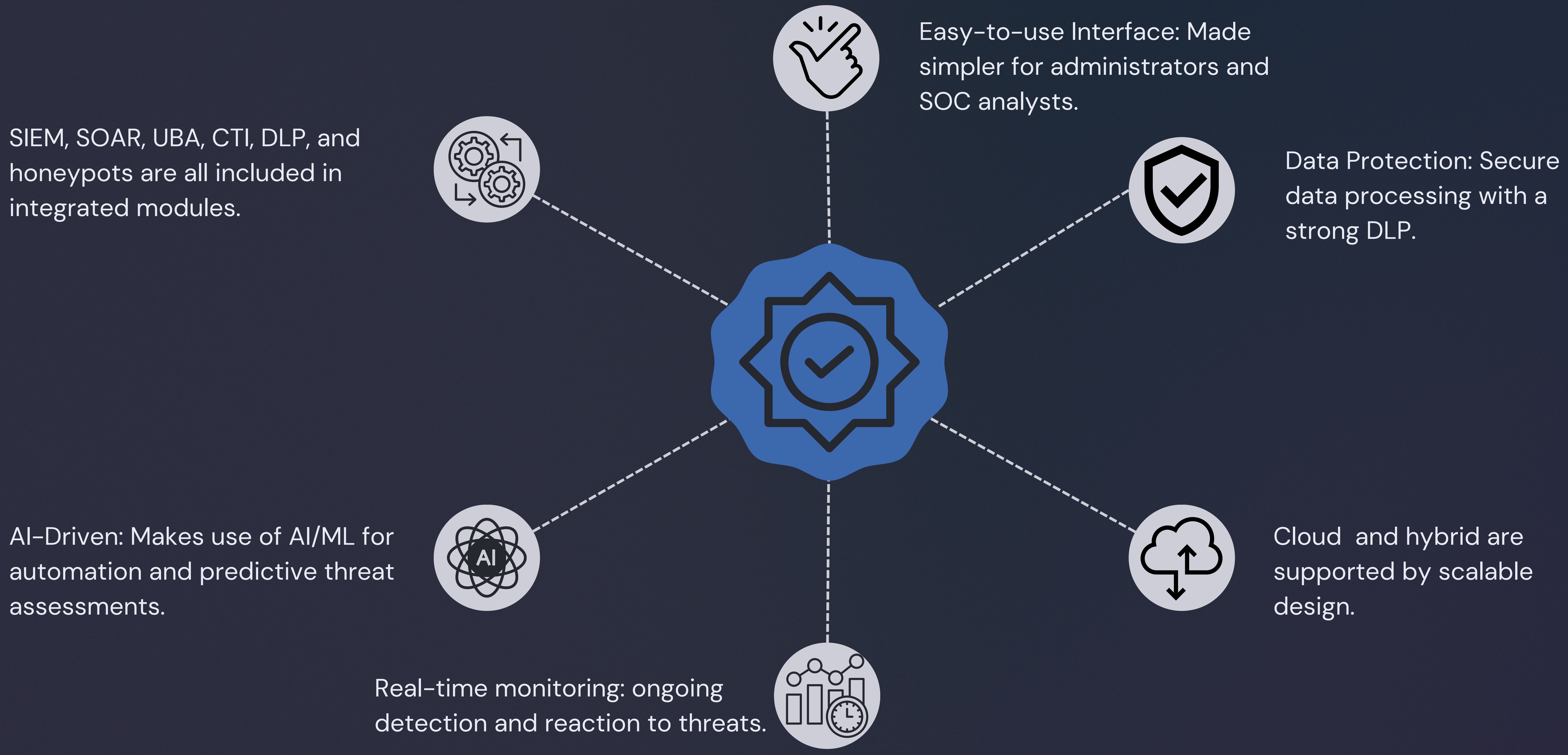
Threat Intelligence Processing

Machine learning models can be trained on this processed data to automatically classify and prioritize threats, providing SOC analysts with actionable information.

HOW THIS PROBLEM SOLVING

IN CYBERGUARDX

FEATURES OF CYBERGUARDX



Easy-to-use Interface: Made simpler for administrators and SOC analysts.

Data Protection: Secure data processing with a strong DLP.

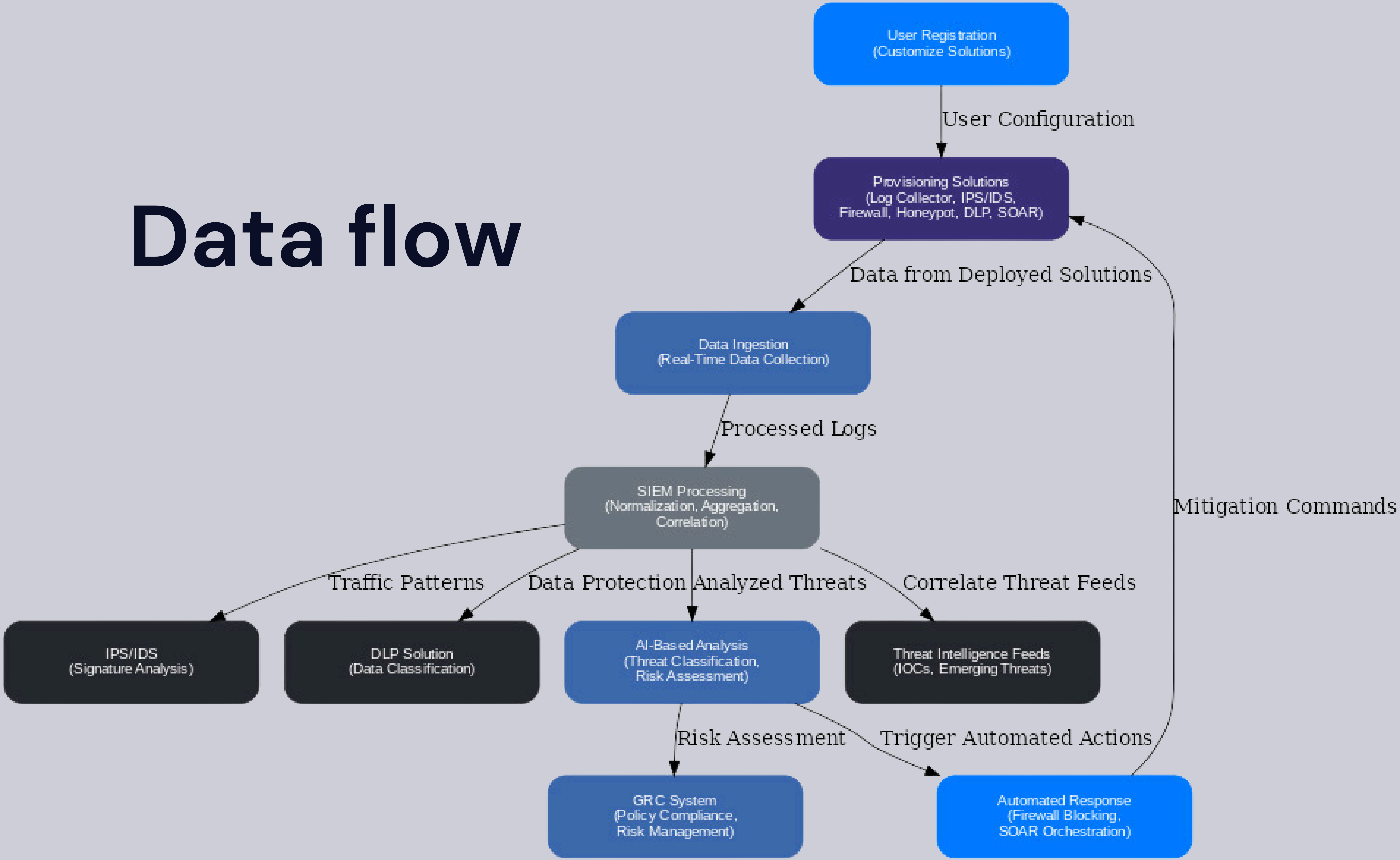
Cloud and hybrid are supported by scalable design.

Real-time monitoring: ongoing detection and reaction to threats.

AI-Driven: Makes use of AI/ML for automation and predictive threat assessments.

SIEM, SOAR, UBA, CTI, DLP, and honeypots are all included in integrated modules.

Data flow

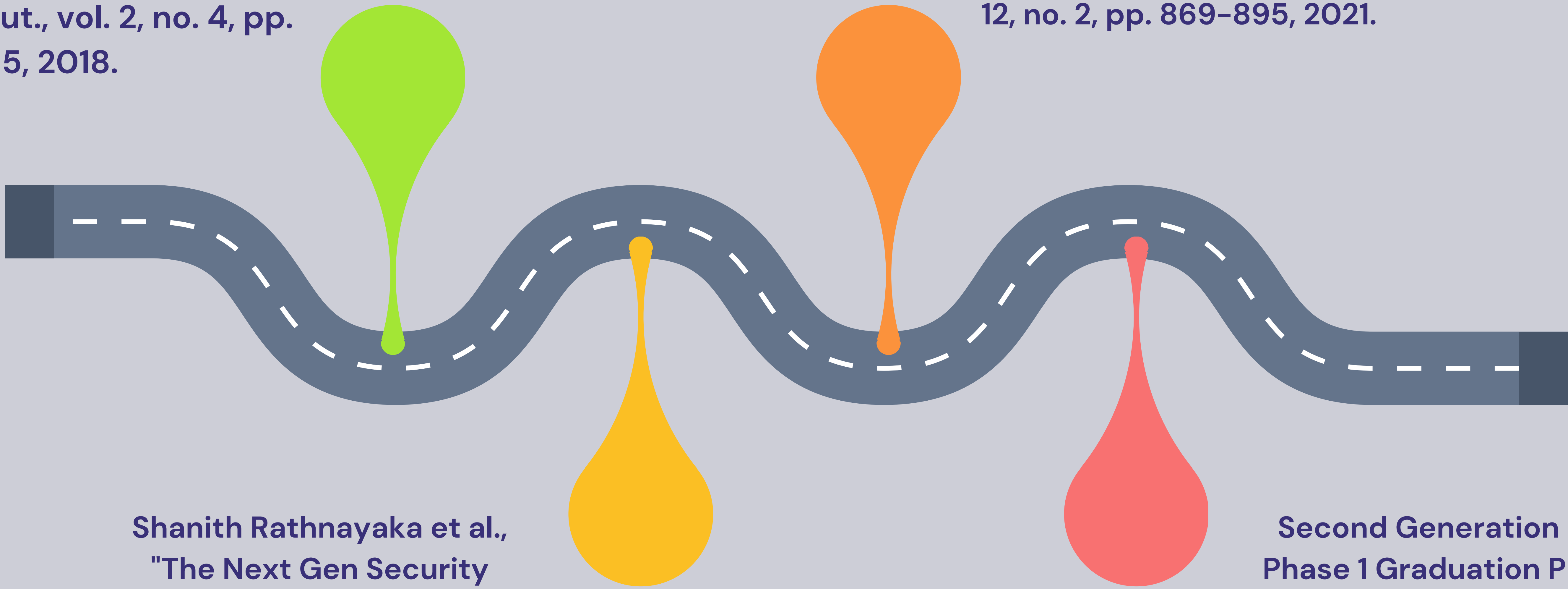

User Registration
(Customize Solutions)
User Configuration
Provisioning Solutions
(Log Collector, IPS/IDS,
Firewall, Honeypot, DLP, SOAR)
Data from Deployed Solutions
Data Ingestion
(Real-Time Data Collection)
Processed Logs
SIEM Processing
(Normalization, Aggregation,
Correlation)
Mitigation Commands
Traffic Patterns
Data Protection
Analyzed Threats
Correlate Threat Feeds
IPS/IDS
(Signature Analysis)
DLP Solution
(Data Classification)
AI-Based Analysis
(Threat Classification,
Risk Assessment)
Threat Intelligence Feeds
(IOCs, Emerging Threats)
Risk Assessment
Trigger Automated Actions
GRC System
(Policy Compliance,
Risk Management)
Automated Response
(Firewall Blocking,
SOAR Orchestration)

THE ACADIMIC & INDUSTRIAL RESEARCHES

Industrial Research

	IBM QRadar SOAR	Elastic Stack (SIEM + SOAR)	MITRE Caldera (SOAR for Simulation)	CyberGuardX
Purpose	Incident response, automation, and integration with enterprise security tools.	SIEM with SOAR for threat detection, monitoring, and automation.	Simulation and automation of adversary behavior for training and testing.	Comprehensive SOC platform with SIEM, SOAR, GRC, DLP, and advanced training.
Integration scope	Over 300 integrations with SIEM, EDR, ITSM, and more.	Integrates with Elastic ecosystem and third-party tools (limited scope).	Focused on simulation and testing; integrations mainly for adversary emulation.	Focused on key integrations (SIEM, SOAR, DLP, GRC) for streamlined deployment.
Ease of use	Requires expertise; steep learning curve.	Moderate learning curve, especially for non-Elastic users.	Designed for security professionals; steep learning curve for new users.	Simplified setup and configuration for new users.
Unique Strengths	Enterprise-grade integrations and incident response.	Unified ecosystem with Elasticsearch, Kibana, and Logstash.	Adversary emulation for red team/blue team testing.	All-in-one SOC platform with GRC, DLP, SIEM, and SOAR.
Unique Limitations	Steep learning curve and high cost.	Requires Elastic expertise and additional tools for full functionality.	Focused on simulation; not suitable as a full-fledged SOC solution.	Limited market presence

ACADEMIC REASEARCH



Konstantinos Demertzis et al., "The Next Generation Cognitive Security Operations Center: Network Flow Forensics," Big Data Cogn. Comput., vol. 2, no. 4, pp. 35, 2018.

Shanith Rathnayaka et al., "The Next Gen Security Operation Center," 6th Int. Conf. for Convergence in Technology (I2CT), 2021.

Yau Ti Dun et al., "Grasp on Next Generation SOC: Comparative Study," Int. J. Nonlinear Anal. Appl., vol. 12, no. 2, pp. 869-895, 2021.

Second Generation SOC: Phase 1 Graduation Project

COMPARISON

	THE NEXT GENERATION COGNITIVE SECURITY OPERATIONS CENTER: NETWORK FLOW FORENSICS	GRASP ON NEXT GENERATION SOC: COMPARATIVE STUDY	THE NEXT GEN SECURITY OPERATION CENTER
Features	- Automates SOC tasks with ML. - Uses MITRE ATT&CK for threat detection.	- Highlights SOC frameworks. - Emphasizes SLAs and KPIs.	- Proposes NF3 for traffic analysis. - Focuses on anomaly detection.
Gaps	- Limited scalability. - Lacks open-source adaptability.	- No real-time analytics. - Relies on static rules.	- High computational needs. - Ignores endpoint security.
CyberGaurdX	- Provides open-source tools and flexible APIs for SMEs.	- Adds real-time analytics and AI-driven detection.	- Uses lightweight AI and includes endpoint security.

THE FUTURE WORK

ON CYBERGUARDX

PROJECT ROADMAP

Teams	Phase 1	Phase 2	Phase 3	Phase 4
Development	SIEM + DLP + IPS/IDS	Firewall + Honeypot	UBA + SOAR + GRC	Intergration
Platform	Design Web as Frontend	Start Create Pages and links	Backend	Publish for users
Research	Find paper of NGSOC and each solution	Academic and industry research	Market Research	Publish a research paper

Future WORK

SOAR Integration

Implement advanced Security Orchestration, Automation, and Response (SOAR) systems to improve incident management and automated responses.

Enable seamless workflow automation between SOC tools for efficiency.

UBA Integration

Integrate enhanced User Behavior Analytics (UBA) for deeper insights into user activities and threat patterns.

Strengthen anomaly detection capabilities using predictive AI/ML algorithms.

GRC Services

Expand Governance, Risk, and Compliance (GRC) offerings to include automated frameworks for regulatory adherence, such as GDPR and ISO 27001.

Build real-time compliance dashboards for efficient monitoring and auditing.

Cloud Integration

Develop robust integrations with cloud-native tools like AWS Security Hub and Azure Sentinel for hybrid and multi-cloud environments.

Optimize scalability and flexibility of the SOC platform for cloud users.

AI Integration

Embed Artificial Intelligence (AI) for advanced threat detection, behavior analysis, and predictive modeling.

Leverage AI-powered insights to automate and enhance decision-making processes.

Training and Simulation

Create immersive training programs for SOC analysts using real-world attack scenarios.

Incorporate gamification techniques to foster skill development and engagement.

Legal License

Obtain certifications and licenses for global market compliance, ensuring credibility and legality in different regions.

Provide compliance-ready services to industries requiring stringent regulatory adherence.

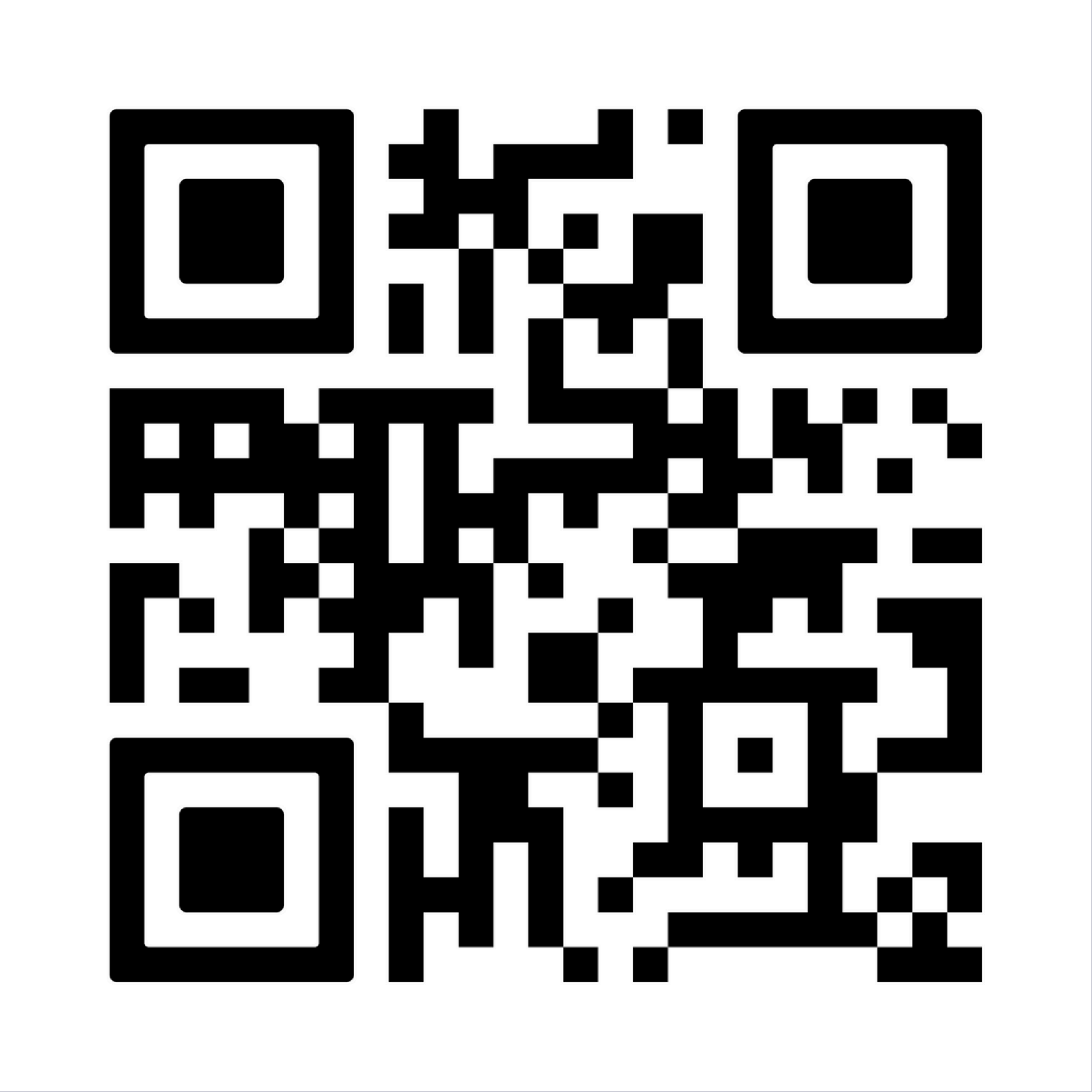
TAKE ACTION

From Concept to Implementation

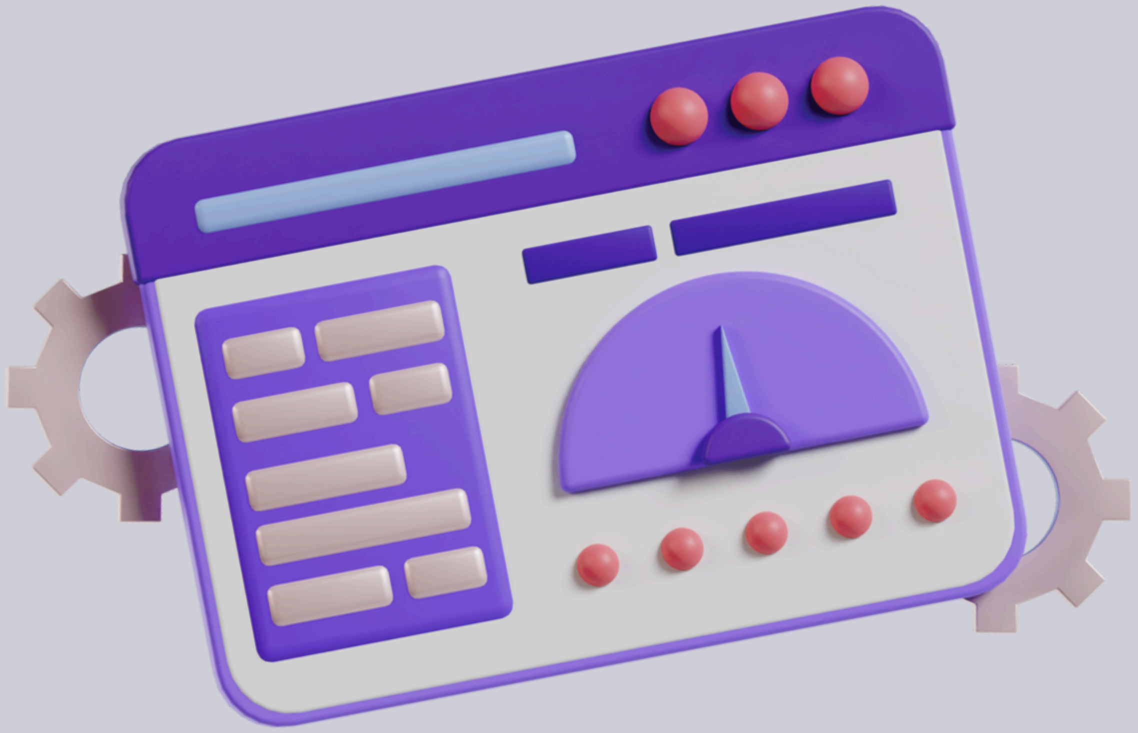
We've navigated through the complexities of cybersecurity, exploring evolving threats and modern defense mechanisms. Now it's time to transition from knowledge to actionable steps. Together, we aim to implement a robust platform that embodies cutting-edge technology and collaboration to strengthen cybersecurity resilience.

- ✓ Design and Build the Platform
- ✓ Integrate Advanced Technologies
- ✓ Regular Updates and Monitoring
- ✓ Collaboration and Knowledge Sharing

Admin Pannal



https://bit.ly/3EePy4n



YOUR QUESTIONS
OUR INSIGHTS

Let's Discuss

We've explored various aspects of cybersecurity today, from assessing the evolving threat landscape to deploying robust defenses and effectively managing incident responses.

جامعة الإسكندرية
ALEXANDRIA UNIVERSITY
كلية الحاسبات وعلوم البيانات

CYBERGUARDX

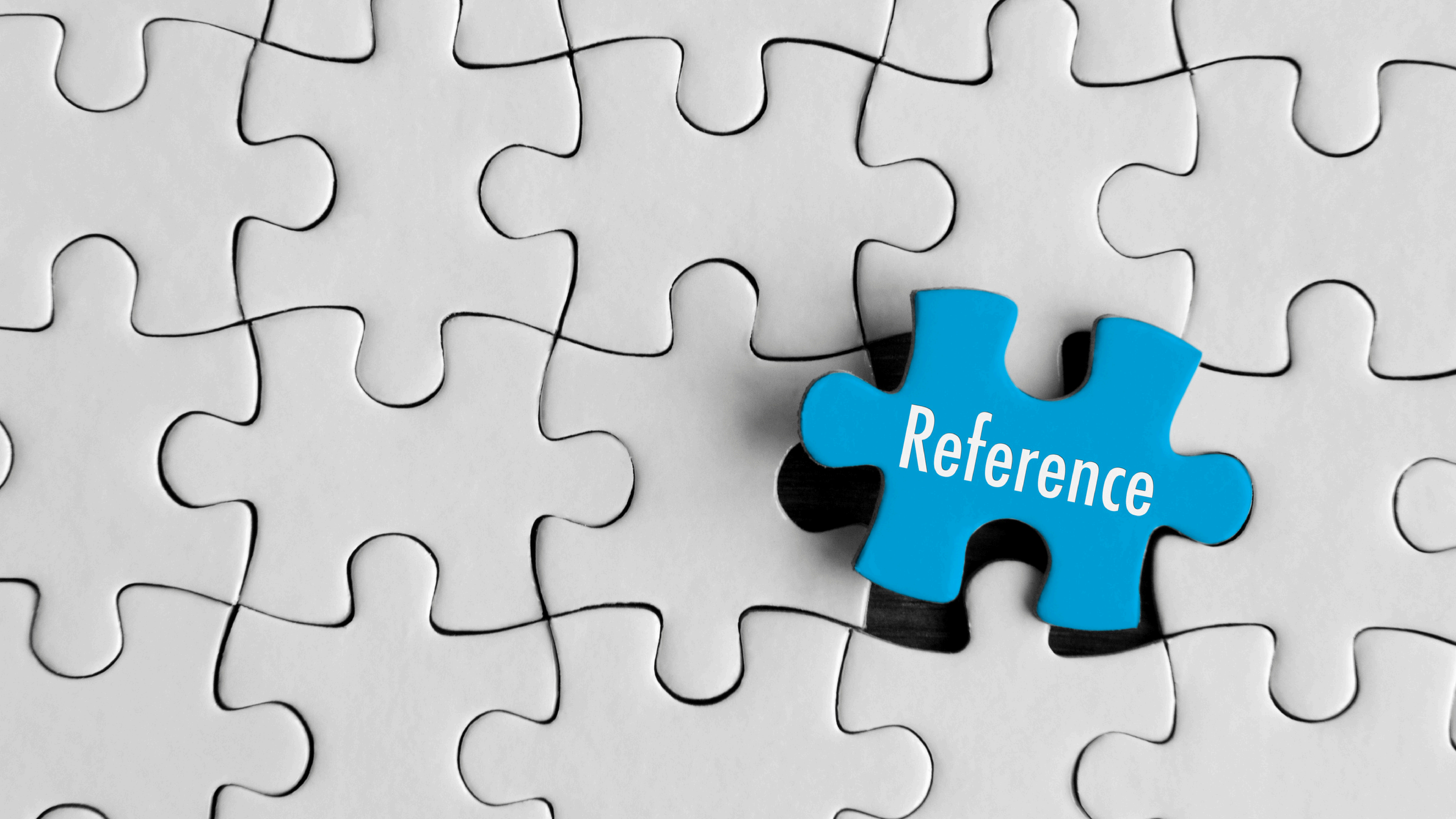
THANK YOU

We appreciate you joining us today

Contact Information:

OUR ROLES

	Responsibilities	Specialties
Abdelrahman Raslan	Team Leader, Overseeing the entire project, ensuring deadlines are met, and managing resources.	SOC (Monitoring and Incident Response), GRC, Networks, Systems
Rewan Salah	Assisting with research, testing tools, and documenting findings and results.	SOC, GRC, Red Teaming (Basic), Cloud
Aya Mohamed	Designing presentations and documentation, coordinating communication among team members.	Networking, Programming, Report Writing, Design
Yousef George	Implementing Linux-based tools, handling server setups, and managing penetration testing activities.	Linux Systems, Cloud, Networks, Penetration Testing
Ahmed Elsayed	Configuring and testing network penetration tools, assisting in secure network setups.	Operating Systems (Windows/Linux), Networking, Network Penetration Testing
Ahmed Yasser	Developing and implementing policies, overseeing compliance testing, and supporting technical configurations.	GRC, DLP, SIEM Integration


Reference

[1]
M. VIELBERTH, "SECURITY OPERATIONS CENTER: A SYSTEMATIC STUDY AND OPEN CHALLENGES," IEEE ACCESS, 2023.

[2]
A. SRIDHARAN, "SIEM INTEGRATION WITH SOAR," IEEE XPLORE, 2023'

[3]
M. ANWARUL, "APPLICATIONS OF AI IN SOAR," CSIAC, 2023.

[4]
A. LISKA, "BUILDING A NETWORK SECURITY INTELLIGENCE MODEL," RESEARCHGATE, 2022.

[5]
N. D. PERERA, "THE NEXT-GEN SECURITY OPERATION CENTER," IEEE ACCESS, 2024.

[6]
J. JOHNSON, "SOAR FOR DISTRIBUTED ENERGY RESOURCES," RESEARCHGATE, 2023

[7]
J. KINYUA, "AI/ML IN SECURITY ORCHESTRATION AND AUTOMATION," TECH SCIENCE PRESS, 2024.

[8]
AALIYAH TASNEEM AND ABHISHEK KUMAR, "INTRUSION DETECTION & PREVENTION SYSTEM USING SNORT," RESEARCHGATE, 2018. [ONLINE]. AVAILABLE: HTTPS://WWW.RESEARCHGATE.NET/PUBLICATION/329716671_INTRUSION_DETECTION_PREVENTION_SYSTEM_USING_SNORT

[9]
SHANITH RATHNAYAKA ET AL., "THE NEXT-GEN SECURITY OPERATION CENTER," IEEE ACCESS, 2024.

[10]
C. ARNDT, "THE NEXT GENERATION COGNITIVE SECURITY OPERATIONS CENTER: NETWORK FLOW FORENSICS USING CYBERSECURITY INTELLIGENCE," BIG DATA AND COGNITIVE COMPUTING, VOL. 3, NO. 6, PP. 1–25, 2018.

[11]
T. ANANTAM, "HONEYPOTS: CONCEPTS, TYPES, AND CHALLENGES," SSRN ELECTRONIC JOURNAL, AUG. 2023. [ONLINE]. AVAILABLE: HTTPS://SSRN.COM/ABSTRACT=4484320.

[12]
DEFENSE.COM, "THE ESSENTIAL GUIDE TO SIEM: NEXT GENERATION SECURITY MONITORING," WHITE PAPER, 2023. AVAILABLE: HTTPS://DEFENSE.COM

[13]
P. WANG, "RESEARCH ON FIREWALL TECHNOLOGY AND ITS APPLICATION IN COMPUTER NETWORK SECURITY STRATEGY," FRONTIERS IN COMPUTING AND INTELLIGENT SYSTEMS

[14]
K. A. MWILA AND J. PHIRI, "DATA LOSS PREVENTION," TECHNICAL REPORT, UNIVERSITY OF ZAMBIA, AUG. 2019

[15]
K. GUPTA AND A. KUSH, "A FORECASTING-BASED DLP APPROACH FOR DATA SECURITY," IN DATA ANALYTICS AND MANAGEMENT, A. KHANNA ET AL., EDS., LECTURE NOTES ON DATA ENGINEERING AND COMMUNICATIONS TECHNOLOGIES

[16]
S. A. ALHARBI, "A QUALITATIVE STUDY ON SECURITY OPERATIONS CENTERS IN SAUDI ARABIA: CHALLENGES AND RESEARCH DIRECTIONS," JOURNAL OF THEORETICAL AND APPLIED INFORMATION TECHNOLOGY

[17]
E. FITZGERALD, A. SMITH, AND J. DOE, "TITLE OF THE ARTICLE," JOURNAL OF ADVANCED STUDIES IN CYBERSECURITY, DEC. 2023. [ONLINE]. AVAILABLE: HTTPS://WWW.MDPI.COM/2624-800X/4/4/36.

[18]
C. WAGNER, A. DULAUNOY, G. WAGENER, AND A. IKLODY, "MISP – THE DESIGN AND IMPLEMENTATION OF A COLLABORATIVE THREAT INTELLIGENCE SHARING PLATFORM," IN PROCEEDINGS OF THE 2016 ACM WORKSHOP ON INFORMATION SHARING AND COLLABORATIVE SECURITY (WISCS), VIENNA, AUSTRIA, OCT. 2016,

[19]
B. A. ALAHMADI, L. AXON, AND I. MARTINOVIC, "99% FALSE POSITIVES: A QUALITATIVE STUDY OF SOC ANALYSTS’ PERSPECTIVES ON SECURITY ALARMS," UNIVERSITY OF OXFORD, 2022.

[20]
B. BOSMA, K. KJIROSKI, P. SMYRLI, S. ANDREOU, AND R. MOOI, "BEST PRACTICES FOR SECURITY OPERATIONS IN RESEARCH AND EDUCATION," GÉANT ASSOCIATION, DELIVERABLE D8.9, DOCUMENT ID GN4-3-22-961B47, JUNE 2022.