CONNECTWISE

Banking on Security: Real Time Threat Detection and Vulnerability Response in Finance

CONNECTWISE®

Matthew Kholos

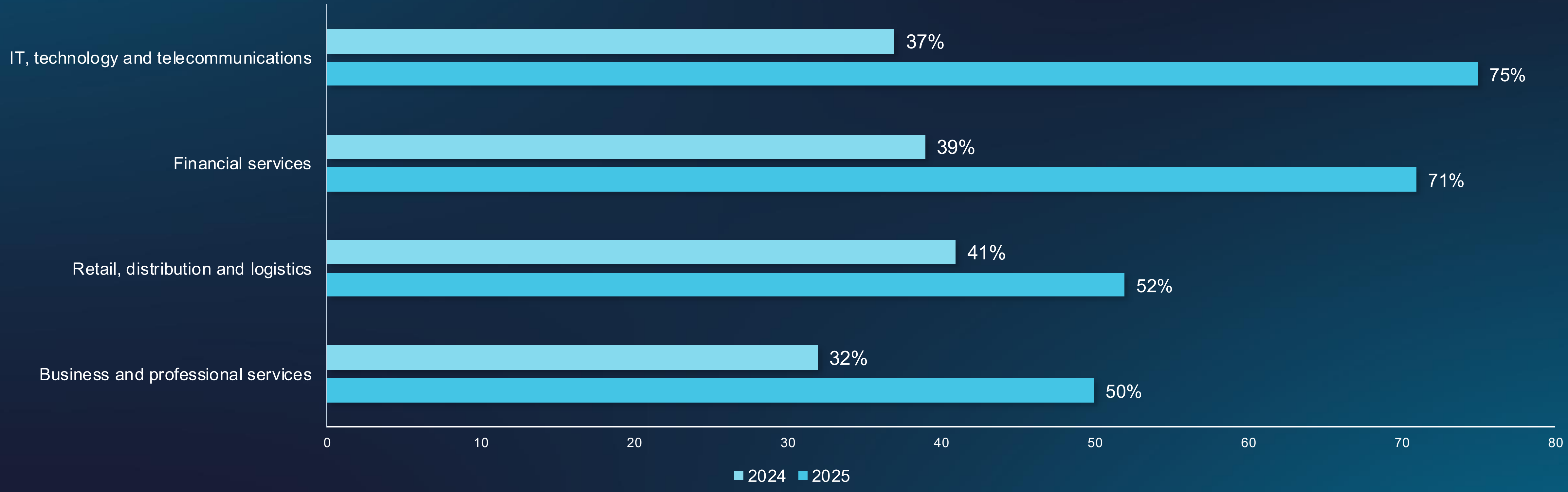
Senior Sales Engineer, Security

Introduction

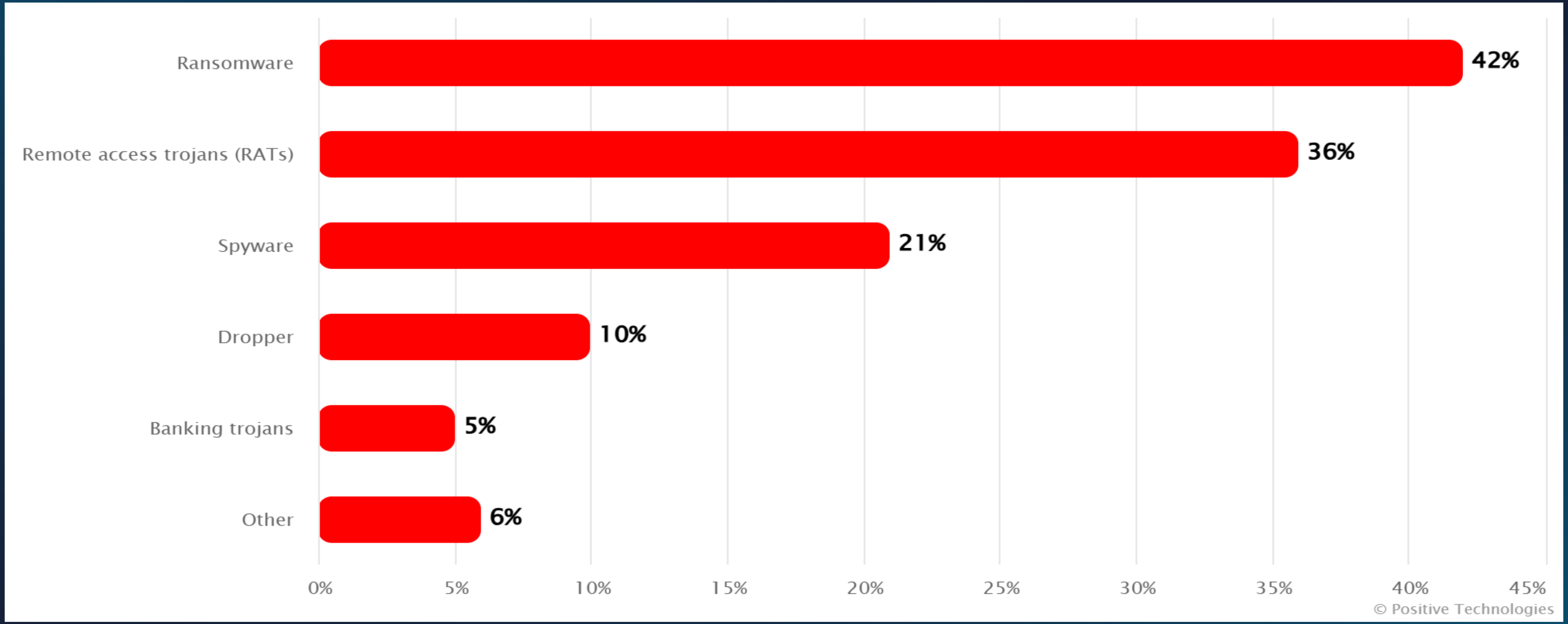
- Overview of Financial Industry Security Challenges
- Importance of Real-Time Threat Detection
- Increasing Cyber Threats

The threat level is increasing across industry sectors – resulting in a growing focus on cybersecurity

Cybersecurity is critical to our business – it’s a top priority



Types of malware used in attacks on financial organizations, percentage of attacksQ1-2025)



© Positive Technologies

High Value Targets

- High Value of Data and Assets
- Direct Access to Funds
- Service Disruption
- Regulatory and Reputational Pressure

What is a SIEM?

- Full Visibility of Everything Happening Within the Network
- Decreases the Time it Takes to Identify Threats
- Detailed Forensic Analysis in the Event of Major Security Breaches

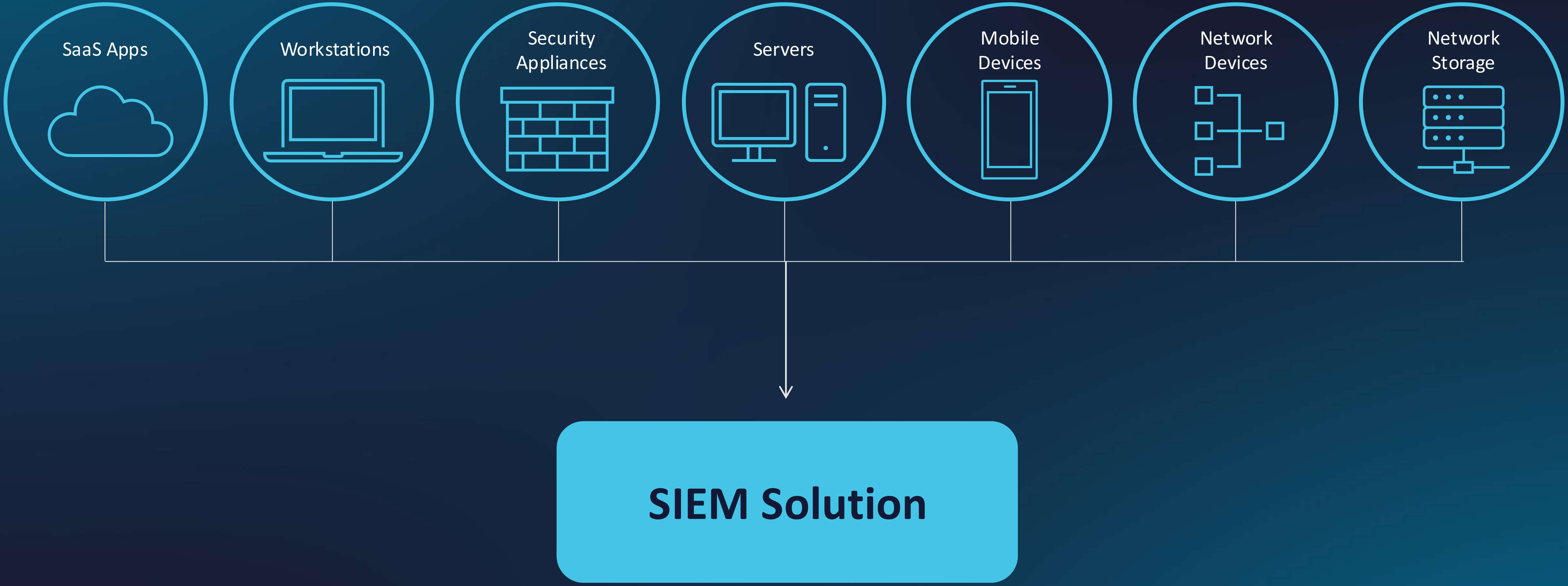
Why do I need it?

Security Information and Event Management

A SIEM works by collecting log and event data generated by an organization’s systems, devices, and applications and brings them into the centralized platform for analysis and reporting.

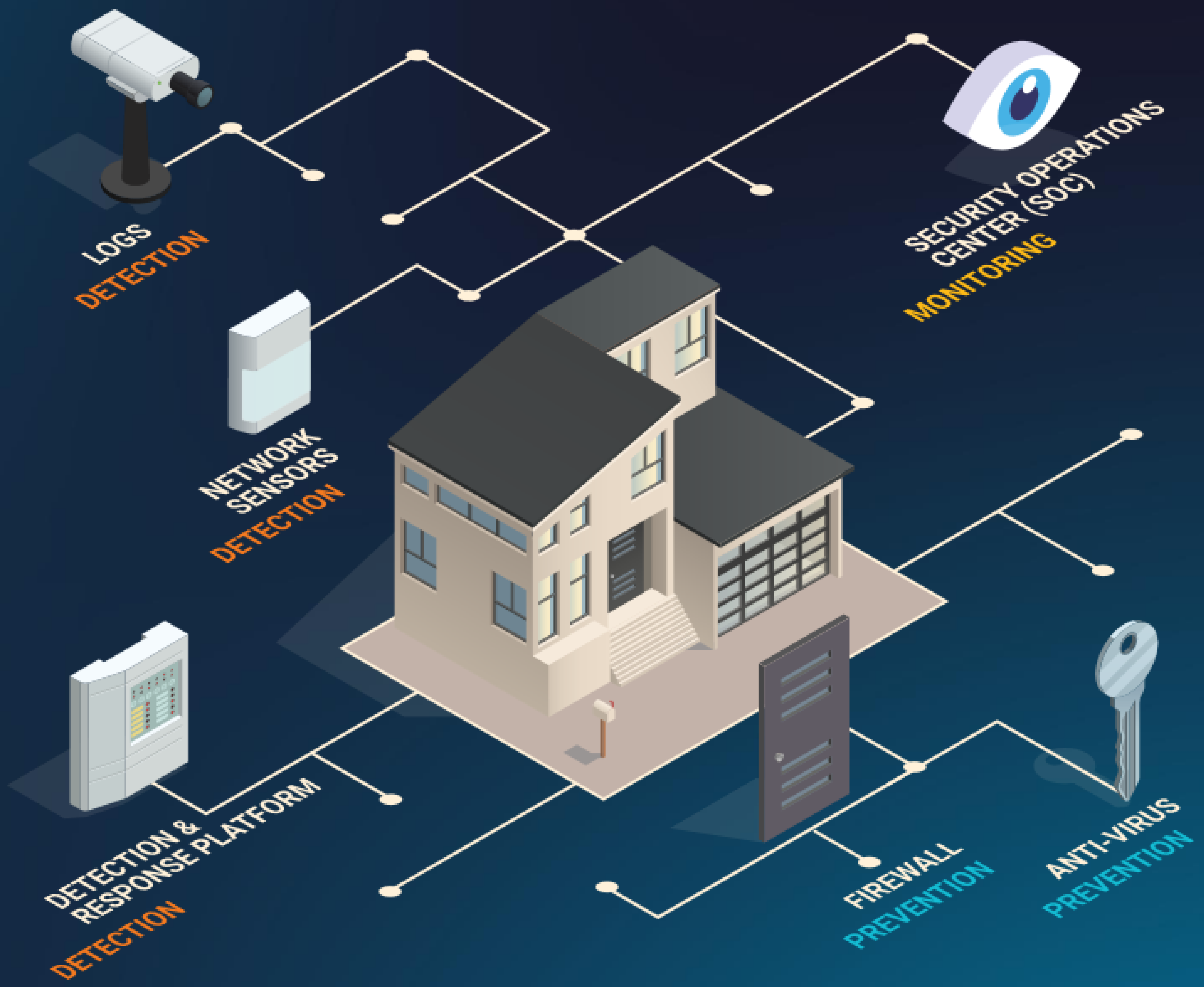
When the SIEM identifies a threat through a set of predetermined rules, an alert is generated for human review.

Alerting and Logging: SIEM & SOC

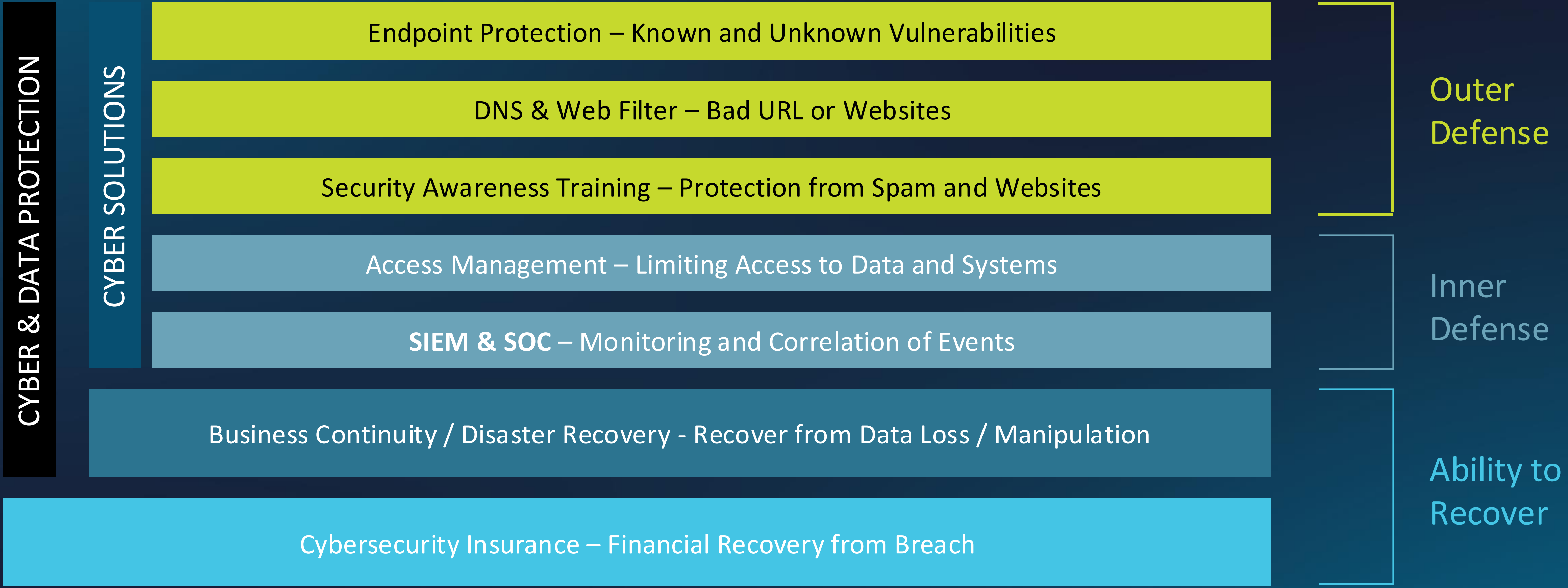


Future Security

PREVENT	Firewall Anti-Virus
DETECT	Detection & Response Platform (SIEM & EDR) Network Sensors Log aggregation (on prem/remote/cloud)
MONITOR	Security Operations Center Threat Hunting Security Research



Technology: Cybersecurity ‘Stack’



CYBER & DATA PROTECTION

CYBER SOLUTIONS

Endpoint Protection – Known and Unknown Vulnerabilities

DNS & Web Filter – Bad URL or Websites

Security Awareness Training – Protection from Spam and Websites

Access Management – Limiting Access to Data and Systems

SIEM & SOC – Monitoring and Correlation of Events

Business Continuity / Disaster Recovery - Recover from Data Loss / Manipulation

Cybersecurity Insurance – Financial Recovery from Breach

Outer Defense

Inner Defense

Ability to Recover

Threat Intelligence

- What is Threat Intelligence?

- External vs Internal

- Importance in Finance

Harnessing External Threat Intelligence

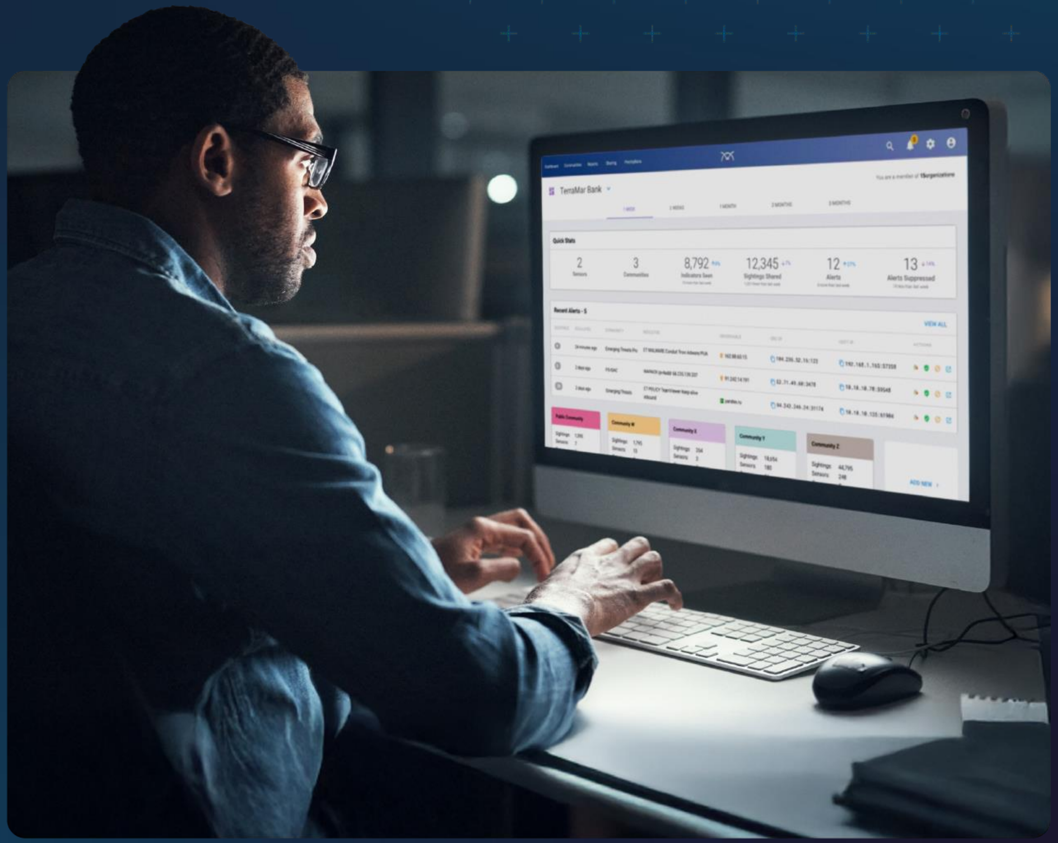
- **FS-ISAC**
- **CRU**
- **Anomali ISAC**
- **Cisco Talos**

Leveraging Internal Threat Intelligence

- Security Event and Audit Logs
- User Activity and Access
- Endpoint Telemetry
- Network Traffic
- SaaS Applications

Real-Time Monitoring

- Faster Threat Detection
- Visibility Across Systems
- Analysis and Correlation



What is Credential Theft and How to Prevent It

Real World Example

- **Strengthening of Blank Bank's Network Perimeter with SIEM**

- **Monitoring the following data sources**:
  - Firewalls
  - VPN
  - Endpoints
  - External Facing Applications

- **Post Incident Analysis**

Conclusion

- SIEM plays a vital role in centralizing monitoring, providing real-time threat detection, and enabling proactive threat hunting
- Threat Intelligence, both external and internal, is crutial for protecting sensitive data and ensuring compliance
- Integrating threat intelligence with SIEM enhances situational awareness and helps identify both external and insider threats
- Real time monitoring and automated responses are essential for early detection