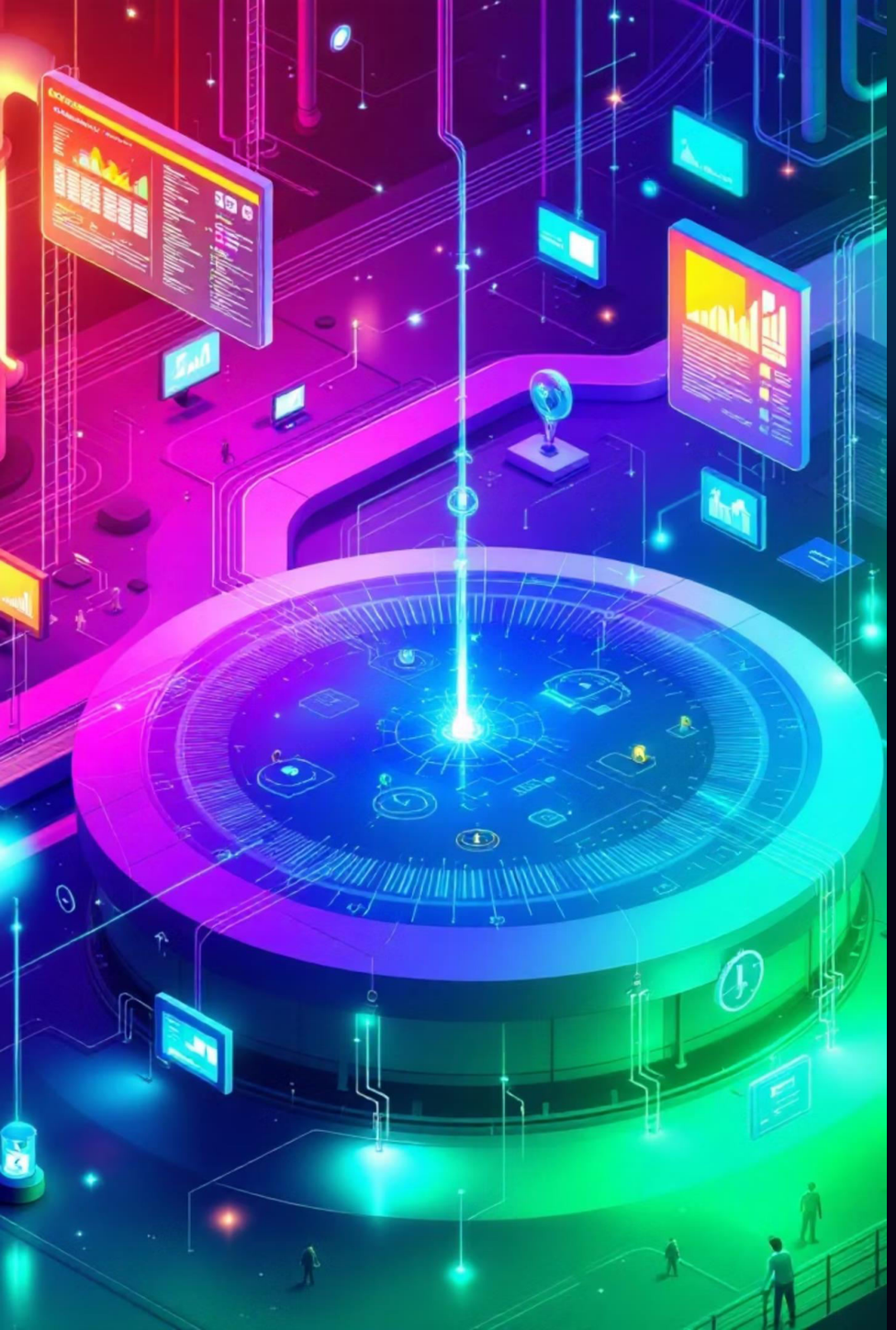


WATER ISAC CHAMPION

Threat STOP

Securing Water Sectors – Actionable Network Defense with ThreatSTOP + Special Guest!

A 60-minute webinar presented by WaterISAC and ThreatSTOP on protecting critical water infrastructure through network security and active defense strategies.

Threat STOP

Agenda

- Setting the Stage: The Evolving Threat Landscape presented by Dr. Paul Mockapetris
- Bridging the Gap: Policy to Practice presented by Tom Brynes
- On the Ground: How SCWD Secures Its Network presented by Bryon Black and Vil Acuna
- Closing Thoughts & Key Takeaways
- Q&A
- Wrap-Up + Closing Slides

Meet Our Expert Speakers

Dr. Paul Mockapetris

ThreatSTOP's Chief Scientist & Creator of the Domain Name System (DNS), providing historical context on cyber threats and DNS security.

Tom Byrnes

ThreatSTOP's CEO & Security expert focusing on compliance requirements and practical implementation of protective measures.

Special Guests:

Bryon Black (IT Manager) & Vil Acuna (Senior Systems Engineer) from South Coast Water District

Q: Why can't we just disconnect from the Internet?

Bad News:

- Remote access
- Cloud interaction
- Laptops
- TV in break room…

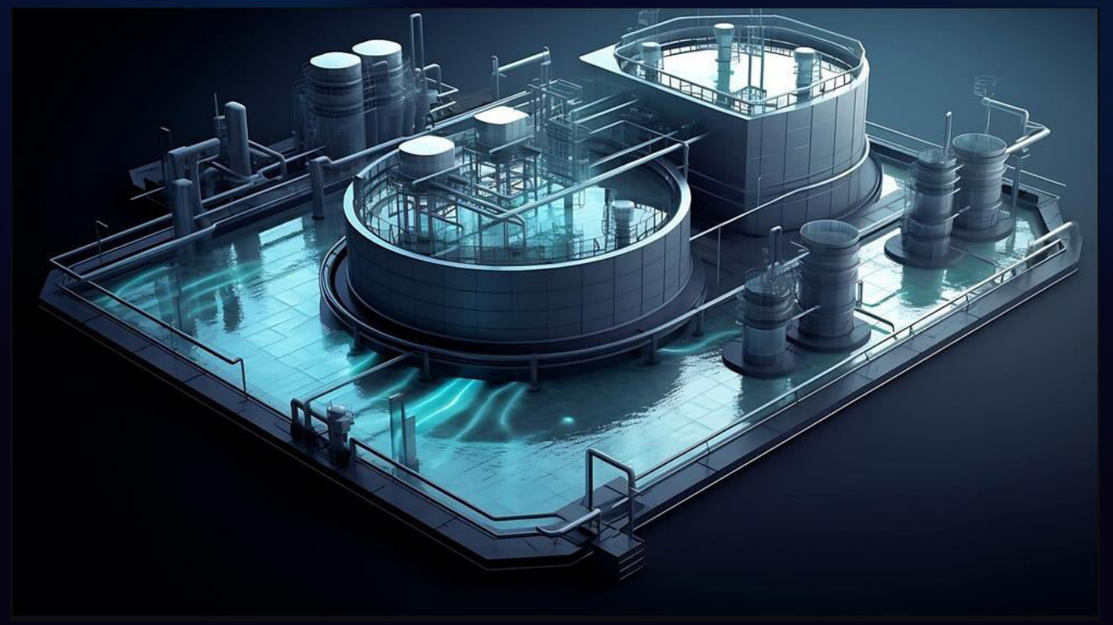
Are all problematic

Good News:

- You can tailor access at every router, firewall, DNS server
- Get close to the ideal

Q: Do I have to listen to / obey / coordinate with CISA if I follow EPA follow EPA guidelines / threat info, etc?

(and what about state, city, county … help)



The goal is to automate the combination of TI once, and have it just happen like clockwork in the background

More sources means better protection, with no additional effort

Q: Why do I need DNS and IP protection?

Either is somewhat effective, but the combination has synergy

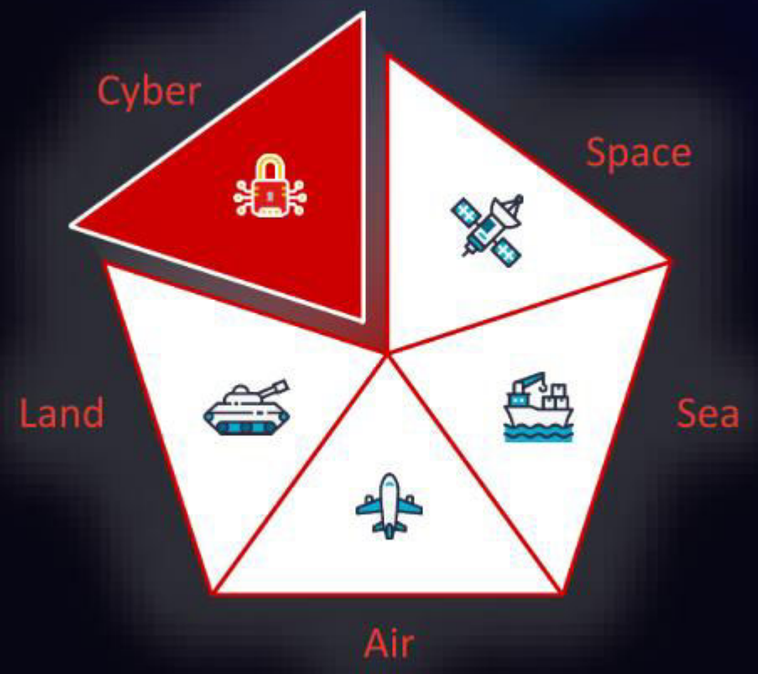
IP protection can prevent your DNS from accessing known bad DNS servers

Setting the Stage: The Evolving Threat Landscape presented

by Dr. Paul Mockapetris

The 5th Domain of Warfare: Cyber

The fifth domain is a continuing state of hot/cold conflict between nations



What’s Different in the 5th Domain?

TIME is of the essence

- If you look at logs all it tells you is what happened.
- Actors beyond reach of Law

You have to catch the preparation preparation

- Constant monitoring and baseline

Hard work and requires a lot of of data crunching

- Automate
- HOT
  - Support of active conquest
  - Influence over population / allies
  - Disruption of infrastructure
  - Sabotage
- COLD
  - Long term penetration and quiet "preparation of the battlefield"
  - Data exfiltration
- Sometimes, plain COMMERCIAL
  - North Korean ransomware

The 5th Domain — Cyber War & Utilities

Strategic Targets

Utilities represent high-value targets for nation-state actors seeking to destabilize critical infrastructure

- Water, power, and gas systems increasingly interconnected
- Physical-digital convergence creates new attack surfaces

Global Impact

Documented attacks on utilities across multiple continents demonstrate the global nature of this threat

- 2021: Florida water treatment facility hack
- 2022: Eastern European power grid compromises

Defense Posture

Moving from reactive to proactive defense models is essential for utility resilience

- Intelligence-driven security becoming standard
- Cross-sector cooperation intensifying

Cyber Risk IS Business Risk

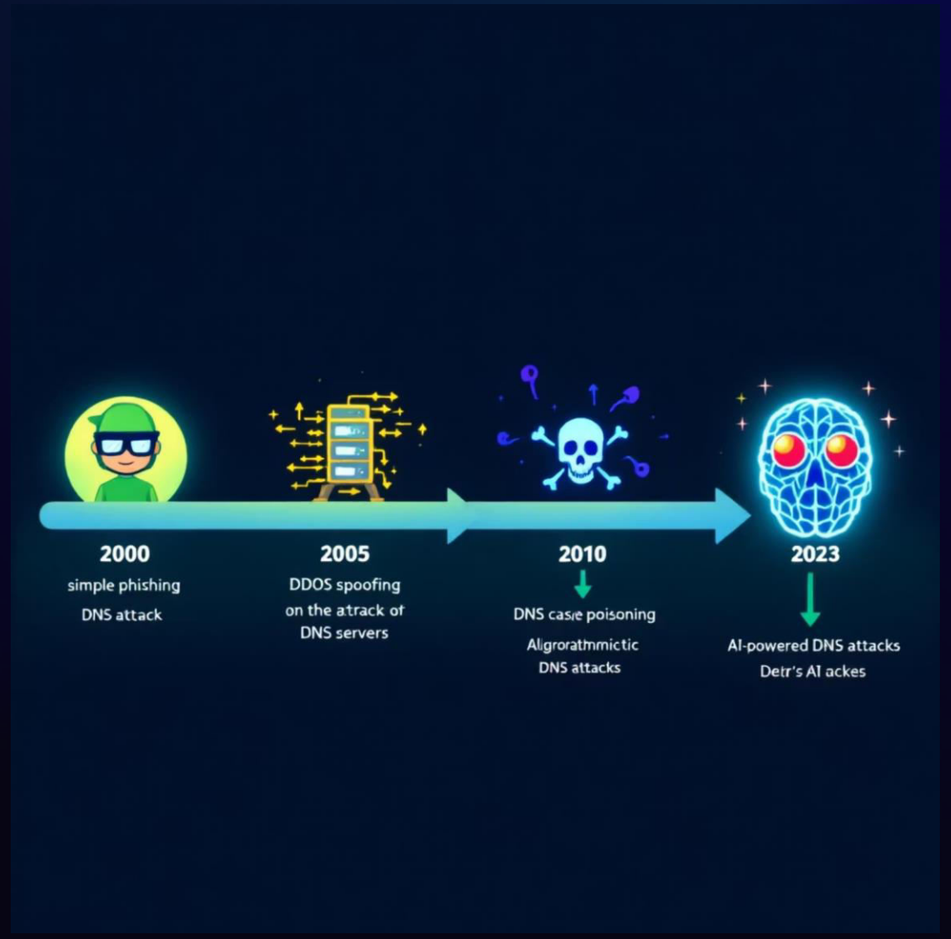
- Issues Right Now
  - Who controls what where changes daily
  - Regulations change weekly
  - Trading systems and alliances shifting
  - Enemy of your enemy is also your enemy
- Risks
  - Heightened risk of cyberattack
    - Nation State actors untouchable
  - Violation of Sanctions
    - Fines
    - Denial of access to SWIFT/US & Euro Banks
    - Jail
- Users can't keep up and subsidiaries/branch offices do their own thing
  - Unintentional does not matter
    - Unless you can show you had measures in place to try to comply and an enforcement and review regime
    - And you're still pwned

Cyber Threats & DNS: Historical Context

Historical Progression

- DNS attacks evolved from simple cache poisoning to sophisticated APTs
- Critical infrastructure targeting increased 300% since 2019 (DHS 2024)
- Water utilities face unique vulnerabilities due to legacy systems
- Outdated SCADA systems prone to exploitation
- Lack of pDNS adoption amplifies risks
- Water utilities saw a 150% rise in DNS-related incidents (WaterISAC, 2023)
- Early 2000s saw first water sector breaches via DNS manipulation
- 2015: Ukraine power grid attack exploited DNS weaknesses (80% outage)
- 2021: Ransomware surge targeted water systems, leveraging DNS flaws
- Over 60% of utility breaches now involve DNS as an entry point (NIST 2024)

Projected: 400% increase in AI-driven attacks by 2025 (est. 07/22/2025)



The Internet's DNA: Why DNS Matters

DNS remains the backbone of internet communications, serving as both:

The foundation for all network connections
-DNS acts as the internet's address book, translating domain names (e.g., www.threatstop.com) into IP addresses, enabling seamless access to websites, email, and online services.

A critical security control point
-DNS is vital for securing traffic, supporting protocols like DNSSEC to prevent spoofing and cache poisoning, and is used to block malicious domains and monitor activity.

A potential vulnerability if left unprotected
-An unsecured DNS can be a weak link, vulnerable to DDoS attacks, redirections, or data theft. Robust protection, like DNS over HTTPS (DoH), is essential.

Water Utilities: Prime Targets in the Crosshairs

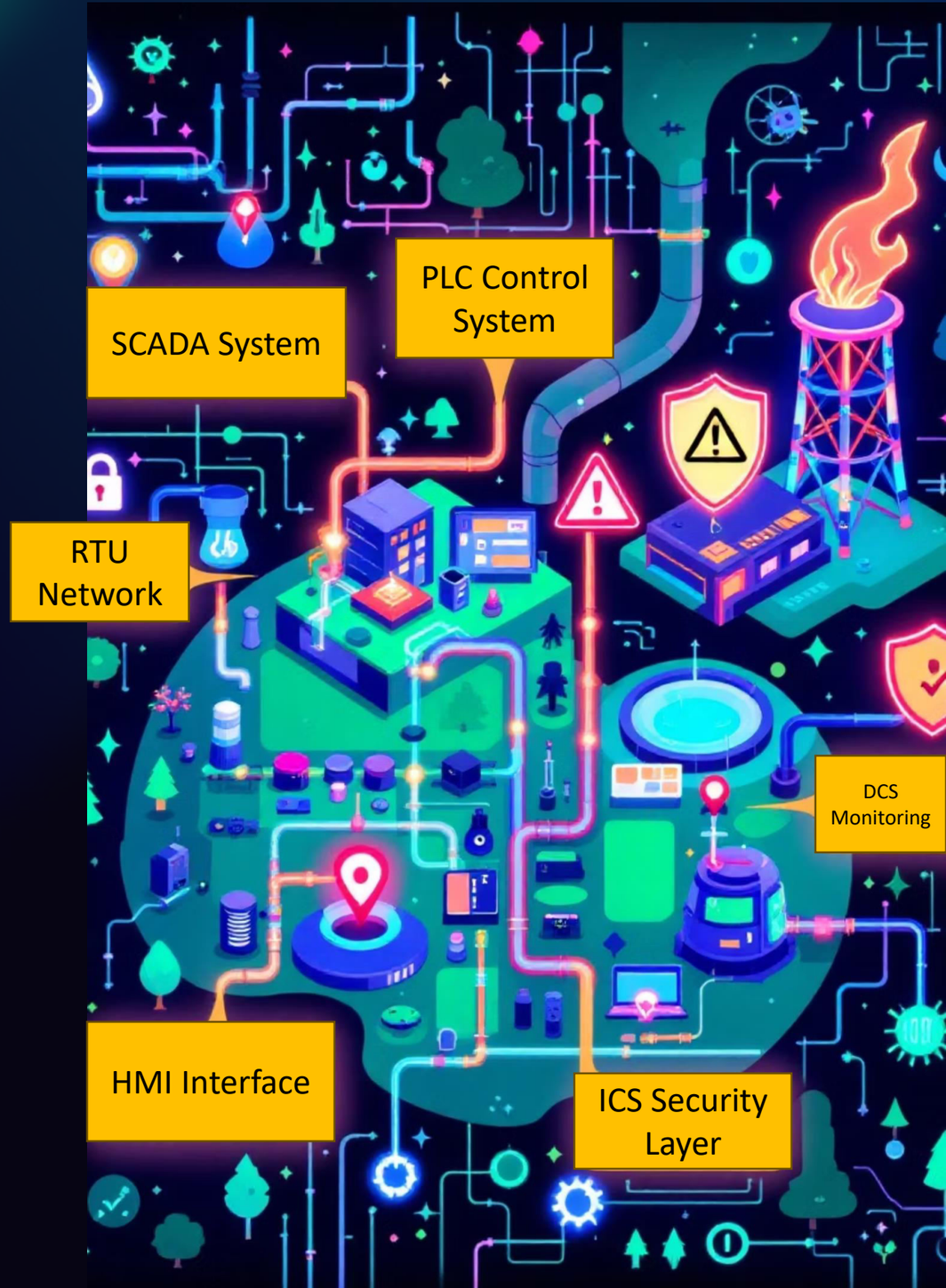
DHS/CISA Alerts on Water Infrastructure

Recent alerts highlight specific threats to water treatment systems:

- AA22-103A: APT actors targeting ICS/SCADA devices
- AA23-045A: Exploitation of OT systems in water facilities
- Malicious actors seeking to alter chemical dosing systems

Why Water is a Tier 1 Target

- Direct impact on public health and safety
- Aging infrastructure with minimal security controls
- Limited cybersecurity resources and expertise
- Widespread distribution systems with remote access points



Why Water is a Tier 1 Target

DHS/CISA Alerts Highlight:

- **Increased targeting of water treatment facilities**

Recent intelligence from DHS and CISA indicates a growing number of cyber and physical attacks aimed at water treatment plants, reflecting their critical role in infrastructure.

- **Public health implications of successful attacks**

A successful breach could contaminate water supplies, leading to widespread health crises, including the spread of diseases or chemical exposure, affecting millions.

- **Limited security resources at many utilities**

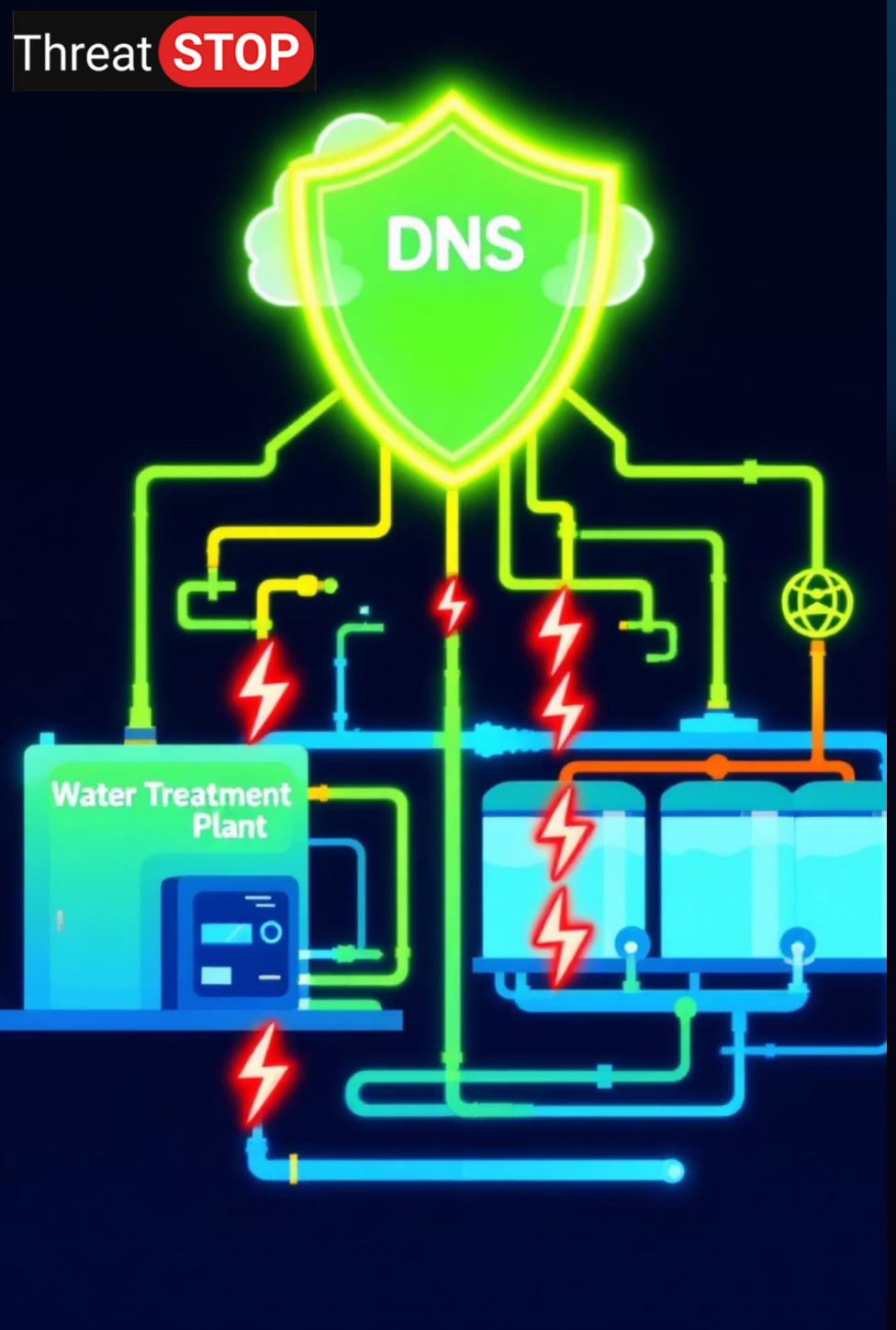
Many water utilities operate with outdated systems and insufficient cybersecurity budgets, leaving them vulnerable to exploitation by well-resourced attackers.

- **High-value target for both criminal and nation-state actors**

The potential to disrupt entire communities or leverage water as a geopolitical tool makes these facilities attractive to hackers seeking ransom and nation-states pursuing strategic advantages.

- **Historical underinvestment in cybersecurity protection**

Water has historically been underinvested in cyber security protection, exacerbating vulnerabilities.



Active Defense: DNS Defense as Your Security Foundation

DNS as Security Control Point

All network communication begins with DNS resolution, creating a natural security checkpoint

- Blocks malicious connections before they establish
- Works even with legacy systems lacking security patches

Passive DNS Monitoring

Analyzing DNS traffic patterns reveals threat activity without disrupting operations

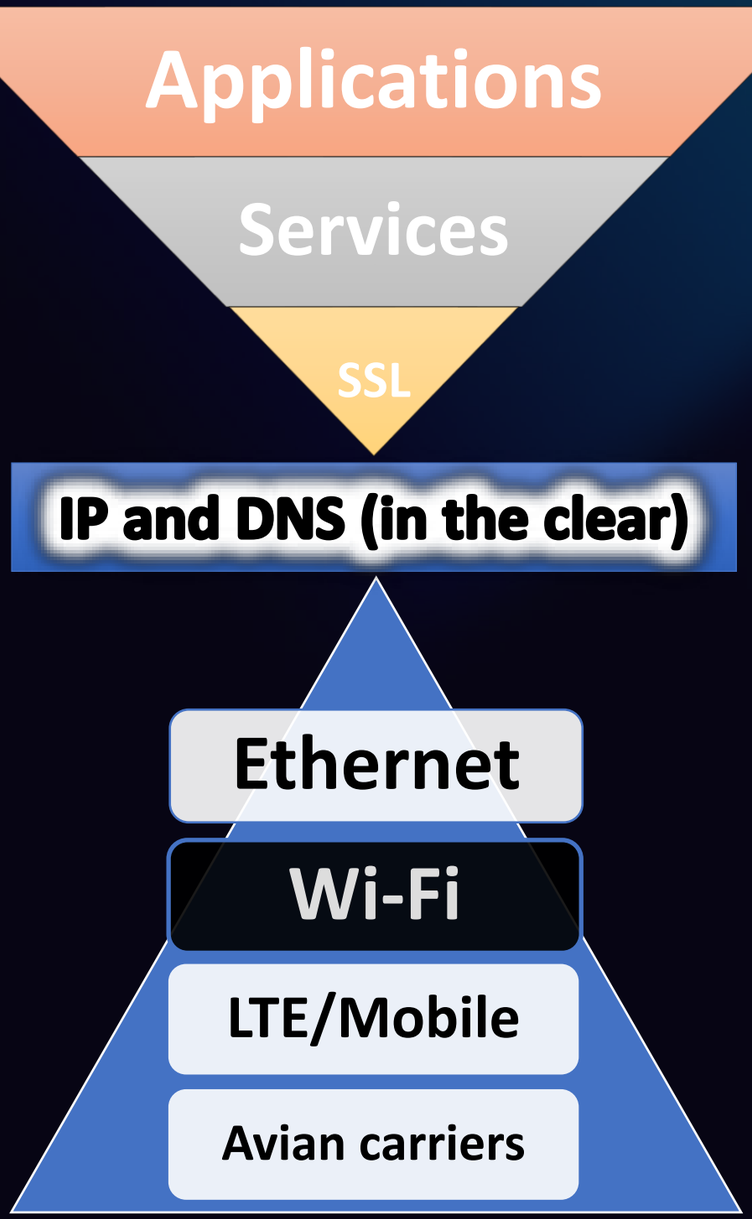
- Identifies command & control communications
- Detects data exfiltration attempts

Threat Intelligence Integration

Continuously updated threat feeds enhance DNS-based protection

- Proactive blocking of emerging threats
- Sector-specific intelligence for water utilities

WATER ISAC CHAMPION



The One to Rule Them All

- Everything converges at IP and DNS
- The only things that CANNOT be encrypted and still have connections complete.
- Used regardless of how the user connects, or what they are doing.
- Ubiquitous, well understood, and supported on all platforms and networks.
- The correct foundation to enforce policy throughout the network

Threat STOP

Bridging the Gap: Policy to Practice

presented by Tom Byrnes

Regulation drives Policy, Policy requires Practice

AWWA Guidelines

Implementation of AIWA driving Industry standards for water utility cybersecurity practices

EPA Guidance

Federal requirements for protecting water infrastructure, includes reporting requirements

NIST CSF

Provides framework for assessments and objectives for controls

EPA Assessment and assistance

Assessment tools

Exercises

Funding

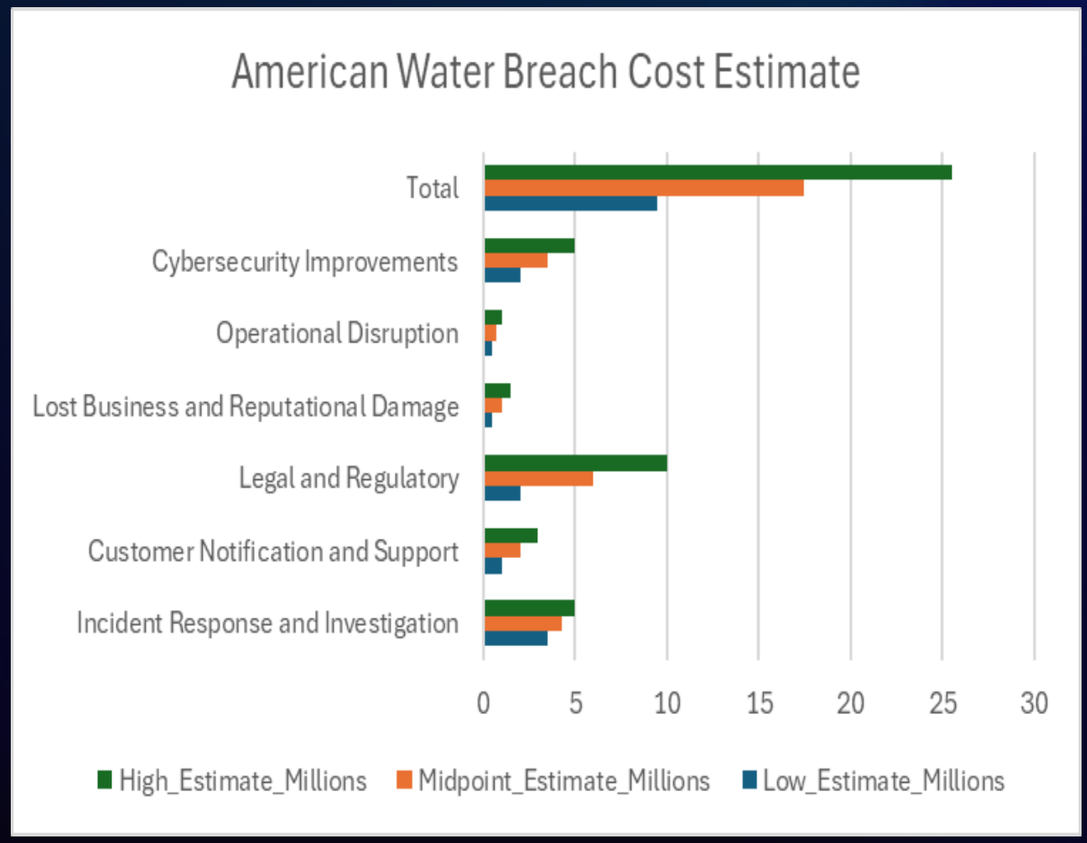
CISA Directives

Specific controls including protective DNS

Cyber Informed Engineering

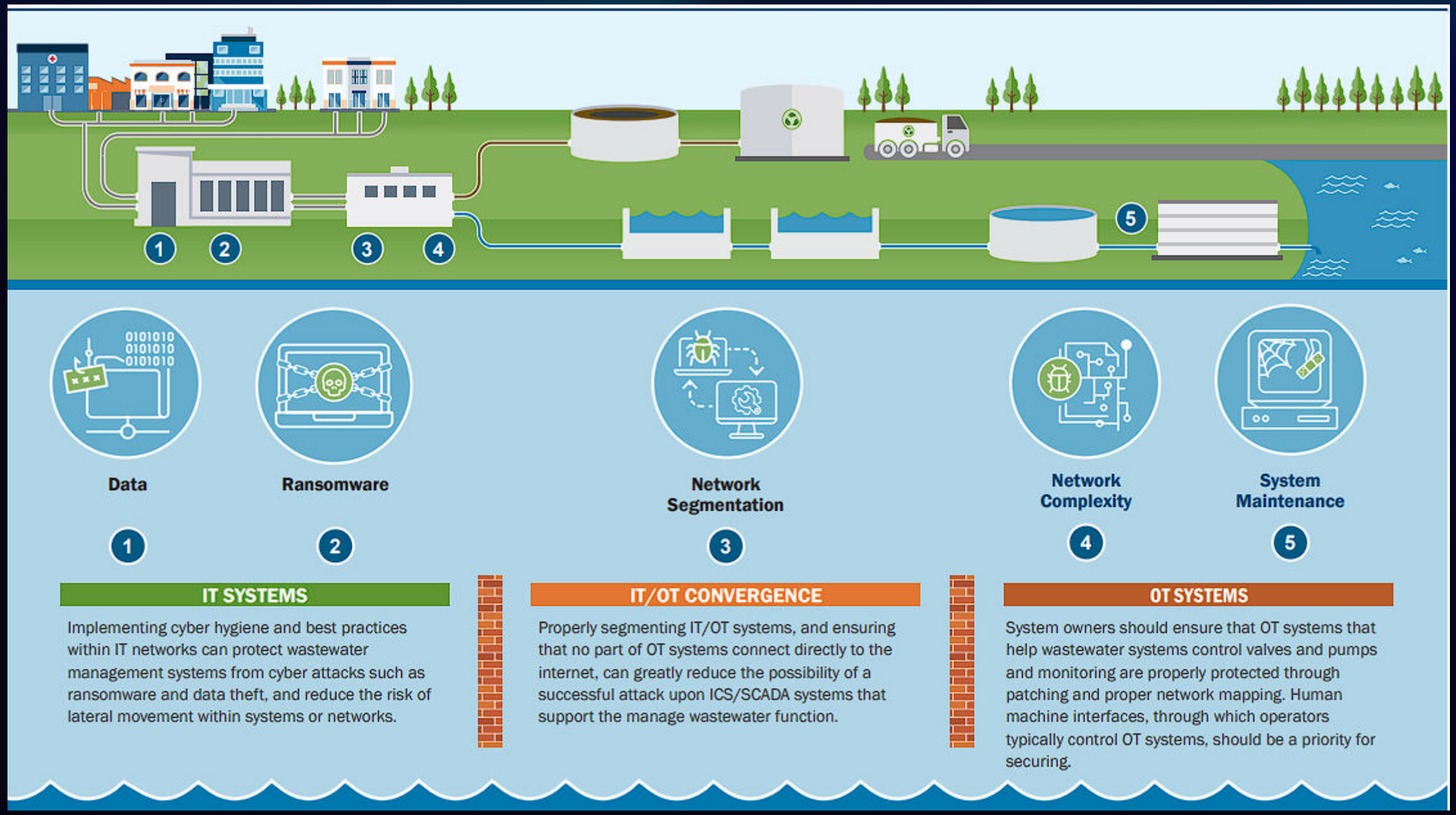
Set of principles to follow at each step of system lifecycle

The Risk is Real



AWWA: Cybersecurity is the top threat facing business and critical infrastructure in the United States, according to reports and testimony from the Director of National Intelligence, the Federal Bureau of Investigation and the Department of Homeland Security. All water systems should act to examine cybersecurity vulnerabilities and develop a cybersecurity risk management program.

Mitigation is a lot of work



Cyber-Informed Engineering: System Design and Lifecycle

PRINCIPLE 1: CONSEQUENCE-FOCUSED DESIGN

PRINCIPLE 2: ENGINEERED CONTROLS

PRINCIPLE 3: SECURE INFORMATION ARCHITECTURE

PRINCIPLE 4: DESIGN SIMPLIFICATION

PRINCIPLE 5: LAYERED DEFENSE

PRINCIPLE 6: ACTIVE DEFENSE

PRINCIPLE 7: INTERDEPENDENCY EVALUATION

PRINCIPLE 8: DIGITAL ASSET AWARENESS

PRINCIPLE 9: CYBER-SECURITY SUPPLY CHAIN CONTROLS

PRINCIPLE 10: PLANNED RESILIENCE

PRINCIPLE 11: ENGINEERING INFORMATION CONTROL

PRINCIPLE 12: ORGANIZATIONAL CULTURE

Water Sector Cybersecurity Maturity Model

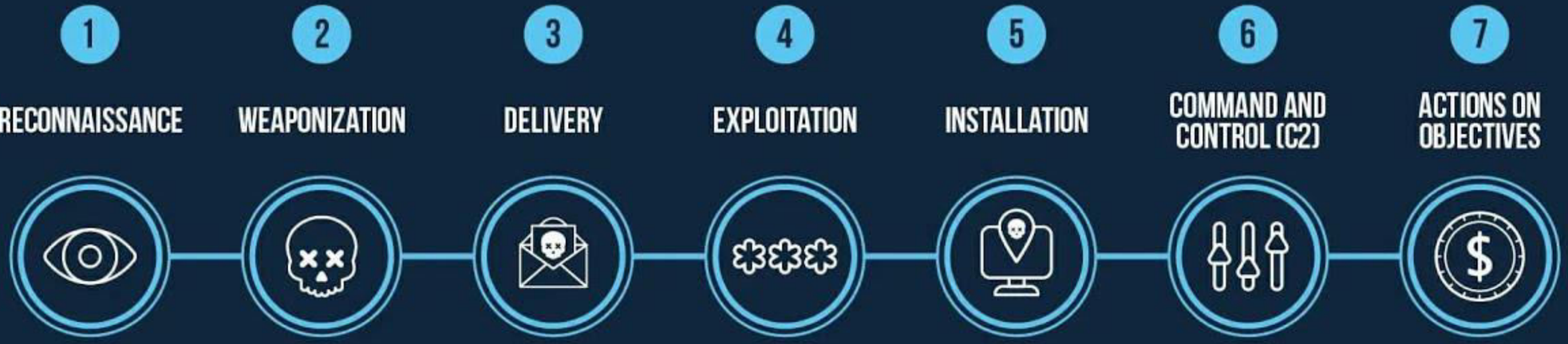
Tier 1 – Partial – There is limited awareness of cybersecurity risks at the organizational level.

Tier 2 – Risk-Informed – There is an awareness of cybersecurity risks at the organizational level, but an organization-wide approach to managing cybersecurity risks has not been established.

Tier 3 – Repeatable – There is an organization-wide approach to managing cybersecurity risks. Cybersecurity information is routinely shared throughout the organization.

Tier 4 – Adaptive – The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement that incorporates advanced cybersecurity technologies and practices, the organization actively adapts to a changing technological landscape and responds in a timely and effective manner to evolving, sophisticated threats.

THE CYBER KILL CHAIN



Implementing the cyber kill chain (Microsoft)

Threat intelligence

Good threat intelligence solutions synthesize data from across an organization's environment and deliver actionable insights that help security professionals detect cyberattacks early.

Identity and access management

Identity and access management solutions help detect anomalous activity that may be an indication that an unauthorized user has gained access. They also offer controls and security measures, such as two-factor authentication, that make it more difficult for someone to use stolen credentials to sign in.

Security information and event management

SIEM solutions aggregate data from across the organization and from third-party sources to surface critical cyberthreats for security teams to triage and address.

Endpoint detection and response

Endpoint detection and response solutions help security teams monitor them for threats and respond quickly when they discover a security issue with a device.

Kill the Supply Chain

CTI Collection

- First Party Intelligence
- Augmented by Third Party Feeds
- Curates millions of indicators of compromise (IOC)

Categorization

- Classifies IOCs into threat categories
- Aggregates blocklists based on IOC attributes

Analysis & Enrichment

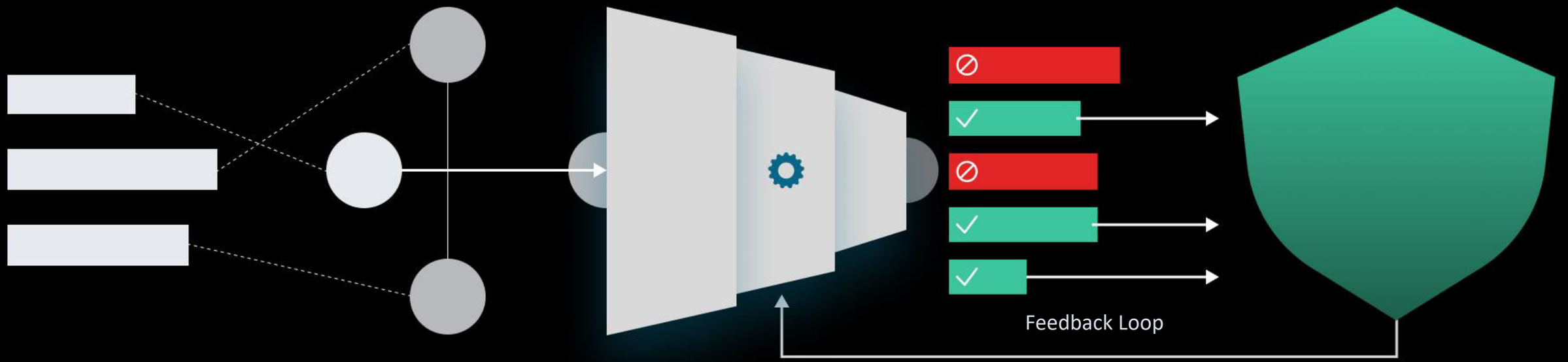
- Human and machine filtering
- IOC validation and False Positive removal
- Scoring for risk, confidence etc.
- IOC and blocklist enrichments

Policy Customization

- Granular policy customization by the user – choose what to block/allow
- Creation of custom, user-defined blocklists
- Seamless incorporation of user-sourced CTI

Enforcement & Reporting

- Instant enforcement in the user network
- Blocks malicious traffic - inbound and outbound
- Integrates with DNS, Firewalls, routers and more
- Advanced web-based reporting



ThreatSTOP Solution

DNS Defense Cloud

Secure your network with our cloud-based DNS solution — in less than 5 minutes

DNS Defense

DNS Defense seamlessly integrates with your existing setup. Our Intelligence, on your device

IP Defense

IP Defense boosts your network's security through a cloud-managed service, supported by nearly any of your IP devices including firewalls, routers, and more.

AWS WAF Defense

ThreatSTOP's AWS WAF Integration swiftly and affordably halts bots, scanners, and malware.

One-Click Sanctions Compliance

Ensure compliance effortlessly with One-Click Sanctions Compliance—our automated platform proactively prevents transactions violating sanctions and export controls.

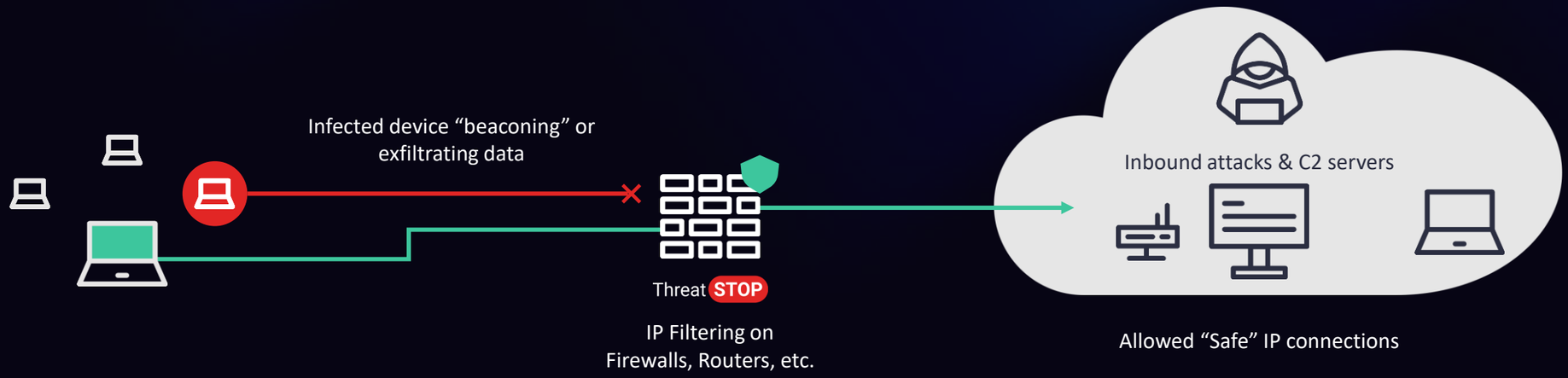
AI Defense

Control AI Usage—using DNS, allow or deny access to Ais, or redirect for inspection by AI Firewalls to control prompts, enforce guardrails, and control costs.

IP Defense

Implementing Perimeter Defenses

- Strengthen network borders with IP Defense, blocking threats and risky connections instantly.
- Secure all vectors universally with our comprehensive protection, no complex tracking needed.
- Enhance security effortlessly; IP Defense integrates seamlessly without changing firewall settings.

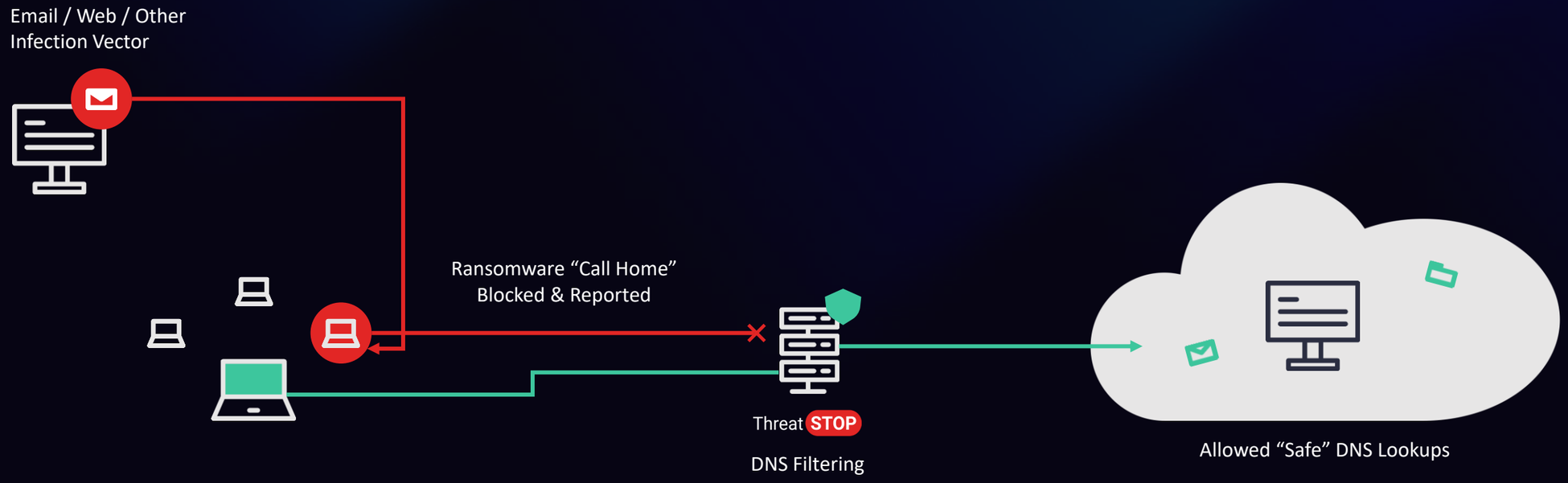


Threat STOP

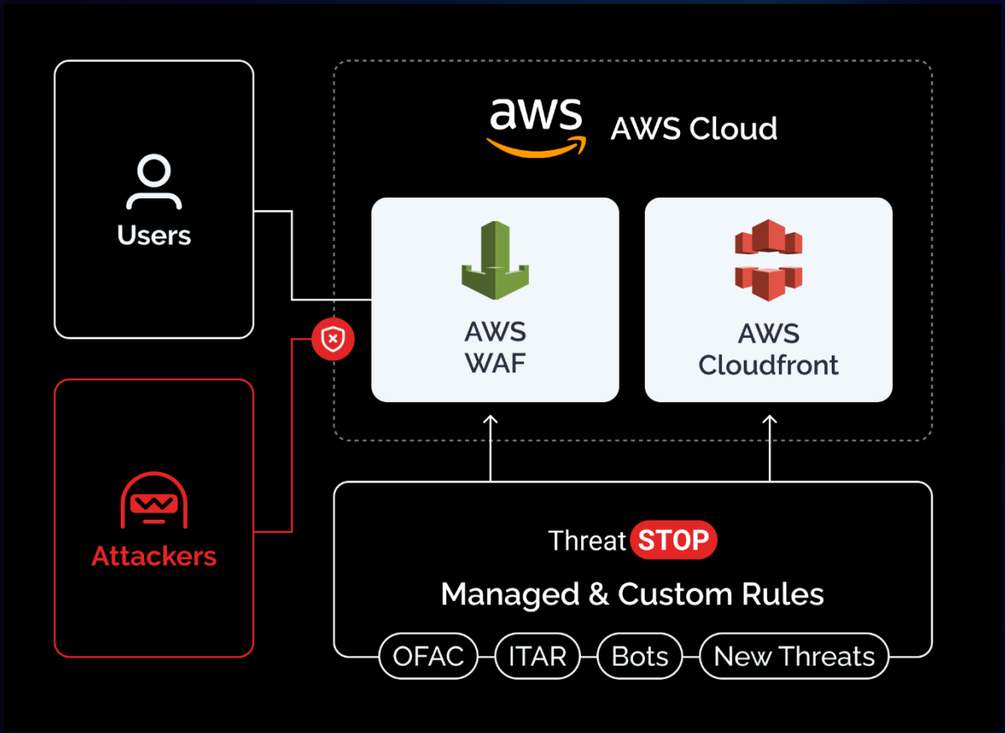
DNS Defense

Proactive, Easy-to-use, and Effective

- Our Intelligence, your device.
- Manage defenses via one cloud-based interface for all devices.
- Streamline security with our easy-to-use, quick-to-deploy DNS protection.



AWS WAF Managed Rules



- Effortless Prepackaged Managed Rules
- Flexible policies enabled in native AWS Interface

ALLOWS

- Fully managed or customizable blocklists

STOPS

- Brute-force credential attacks
- Scanners and harassing IPs
- Unwanted scrapers / content theft
- ITAR/OFAC sanctions violations

THE CYBER KILL CHAIN

The Result with ThreatSTOP.

PRINCIPLE 2: ENGINEERED CONTROLS: The controls are designed in

PRINCIPLE 3: SECURE INFORMATION ARCHITECTURE: All network elements become part of security.

PRINCIPLE 4: DESIGN SIMPLIFICATION: System as a service covering Intelligence, enforcement, and reporting.

PRINCIPLE 6: ACTIVE DEFENSE: Continually updated with latest threat infrastructure based on your policy.

PRINCIPLE 5: LAYERED DEFENSE: Inbound and outbound, with multiple customizable policies depending on environment and platform.

PRINCIPLE 8: DIGITAL ASSET AWARENESS: Everything uses the DNS, detects unknown and new devices immediately.

PRINCIPLE 9: CYBER-SECURITY SUPPLY CHAIN CONTROLS: New devices usually beacon to vendor, detect and interdict.

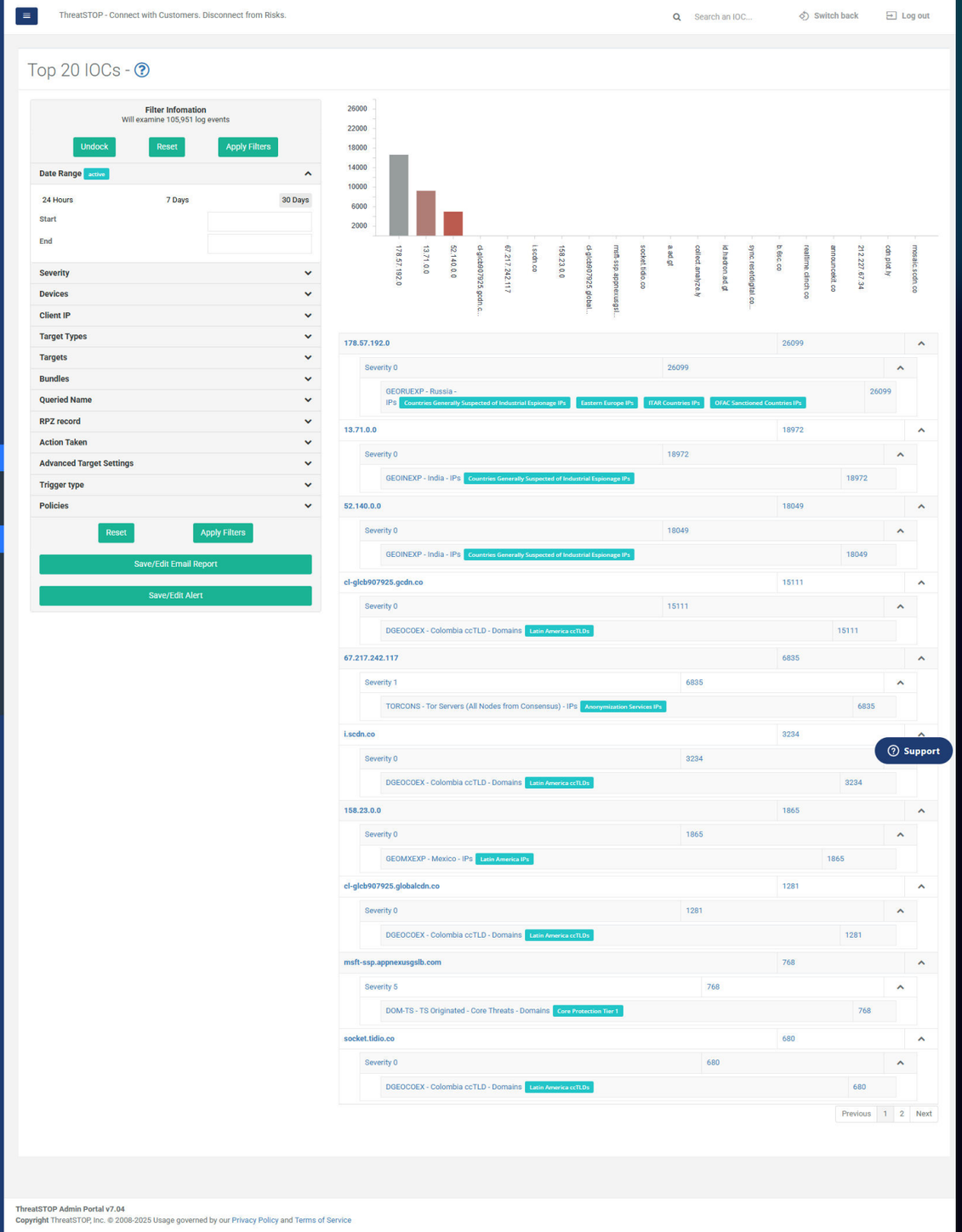
PRINCIPLE 10: PLANNED RESILIENCE: Supports on prem, cloud, DR sites, WFH, Field

PRINCIPLE 11: ENGINEERING INFORMATION CONTROL: Full NIST RBAC for all access with 2FA

PRINCIPLE 12: ORGANIZATIONAL CULTURE: Proactive, easy to use so used

Tier 4 – Adaptive – The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement that incorporates advanced cybersecurity technologies and practices, the organization actively adapts to a changing technological landscape and responds in a timely and effective manner to evolving, sophisticated threats.

The ThreatSTOP system, with its feedback loop, reporting, alerting, and ability to dynamically adjust policy across all elements enables Tier 4 Capability



WATER ISAC CHAMPION

ThreatSTOP: Your Compliance Solution Solution

Regulatory Alignment

Meets requirements across EPA, AWWA, and CISA frameworks

- Pre-configured compliance policies
- Automated documentation generation

Layered Defense

Integrates with existing security infrastructure

- Works with firewalls and IDS/IPS systems
- Enhances SCADA/ICS protection

Visibility & Reporting

Comprehensive dashboards for compliance verification

- Threat intelligence reporting
- Audit-ready documentation

ThreatSTOP

Real-World Protection: Blocking C2 Infrastructure

[Case Study: South Coast Water District]

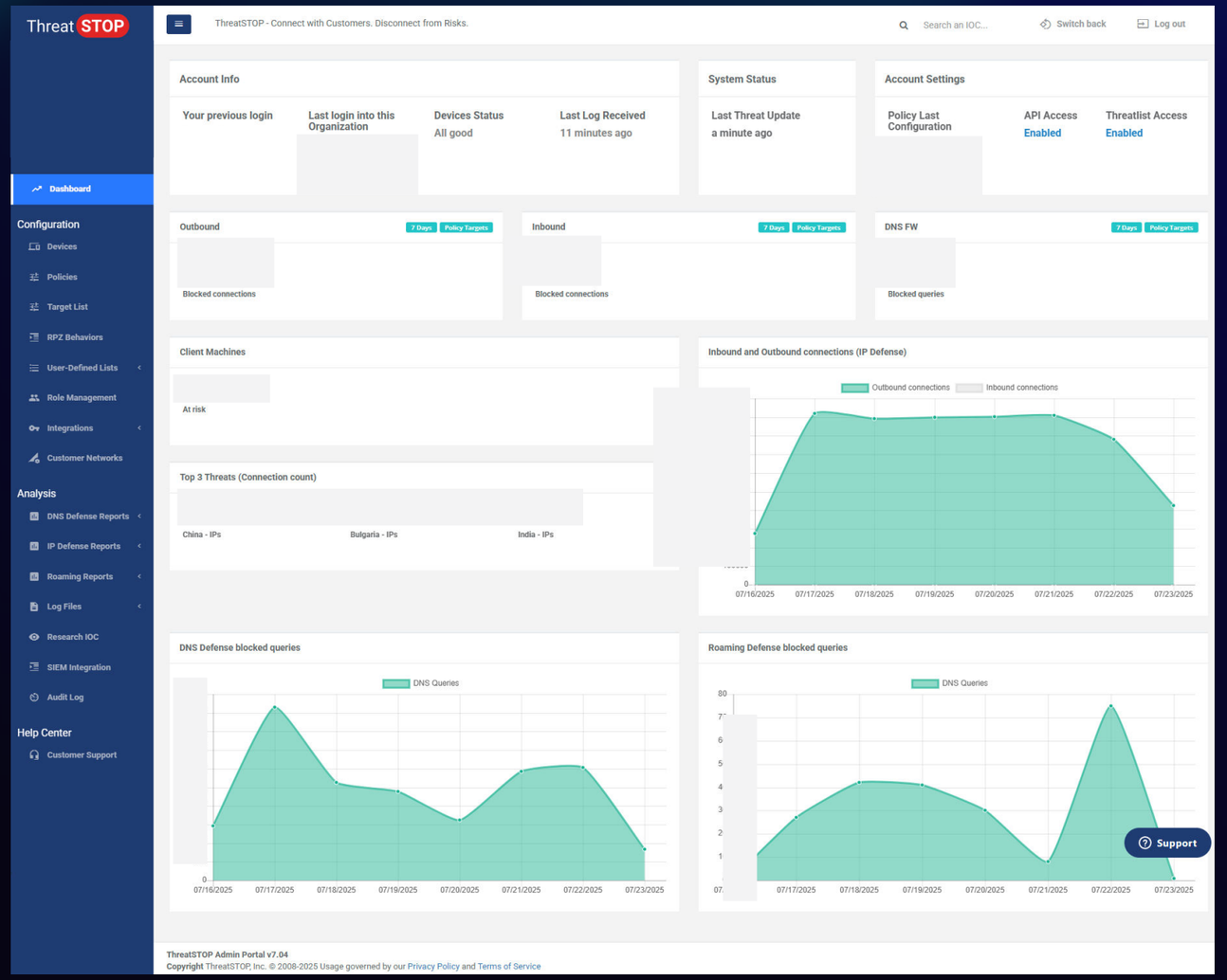
ThreatSTOP provides:

- **Proactive blocking of command & control servers**
ThreatSTOP actively identifies and blocks communication with malicious command and control (C2) servers in real-time, preventing malware from receiving instructions or exfiltrating data.

- **Automated threat intelligence updates**
The system delivers continuous, automated updates based on the latest threat intelligence, ensuring protection against emerging threats without manual intervention.

- **Simplified compliance reporting**
ThreatSTOP generates detailed, easy-to-understand reports that help organizations meet regulatory requirements, such as NIST or GDPR, with minimal effort from security teams.

- **Reduced operational burden on security teams**
By automating threat detection and response, ThreatSTOP minimizes manual tasks, allowing security teams to focus on strategic priorities rather than routine monitoring.



On the Ground: How South Coast Water District Secures Its Network

presented by Bryon Black and Vil Acuna

ThreatSTOP: First and Last Line Line of Defense at SCWD

ThreatSTOP serves as both our first and last line of defense in SCWD's multi-layered protection strategy for enterprise and operational technology systems. By securing inbound network traffic and preventing malicious outbound communications to command and control systems, ThreatSTOP delivers exceptional value with the broadest protection at the lowest cost among our best-of-breed security solutions.

ThreatSTOP Deployment and Tools at SCWD

Continuous Protection Since 2016

SCWD has relied on ThreatSTOP's comprehensive protection for almost a decade, starting with physical hardware and evolving to fully integrated NGFW solutions.

Comprehensive Security Suite Suite

Our implementation includes DNS Defense, IP Defense, and mobile agents on all remote work laptops, creating multiple layers of protection.

Simple, Guided Deployment

Step-by-step instructions enabled quick implementation with two bridge IP Defense protections and pre-built virtual DNS Defense, requiring minimal reconfiguration.

Initial Impact and Ongoing Support with ThreatSTOP

Immediate Security Enhancement

From day one, ThreatSTOP delivered significant protection improvements over our previous static firewall policies, rules, and IP/port blocking mechanisms.

Real-Time Threat Intelligence

ThreatSTOP's threat intelligence consistently identifies zero-day and novel vulnerabilities before official CVE publication, providing critical early warnings.

Continuous Support Structure

- Quarterly policy reviews ensure optimal protection
- Constant monitoring of ThreatSTOP tools
- 24-hour support response for any issues
- Prompt, helpful training during implementation

Upgrading to NGFW with ThreatSTOP Integration

Remote Site NGFW Upgrade

We're currently implementing Next-Generation Firewalls across all remote sites, enhancing our security posture with advanced traffic inspection capabilities.

Seamless ThreatSTOP Integration

ThreatSTOP integrates directly with our NGFW user interface, providing unified management and visibility into security events.

Enhanced Real-Time Protection

The combined solution delivers real-time blocking using ThreatSTOP's DNS/IP-based defenses embedded within our firewall infrastructure.

Threat STOP

ThreatSTOP - Connect with Customers. Disconnect from Risks.

Search an IOC... Switch back Log out

- Dashboard

Configuration
- Devices
- Policies
- Target List
- RPZ Behaviors
- User-Defined Lists
- Role Management
- Integrations
- Customer Networks

Analysis
- DNS Defense Reports
- IP Defense Reports
- Roaming Reports
- Log Files
- Research IOC
- SIEM Integration
- Audit Log

Help Center
- Customer Support

Account Info

Your previous login

Last login into this Organization

Devices Status
All good

Last Log Received
11 minutes ago

System Status

Last Threat Update
a few seconds ago

Account Settings

Policy Last Configuration

API Access
Enabled

Threatlist Access
Enabled

Outbound

7 Days | Policy Targets

Blocked connections

Inbound

7 Days | Policy Targets

Blocked connections

DNS FW

7 Days | Policy Targets

Blocked queries

Client Machines

At risk

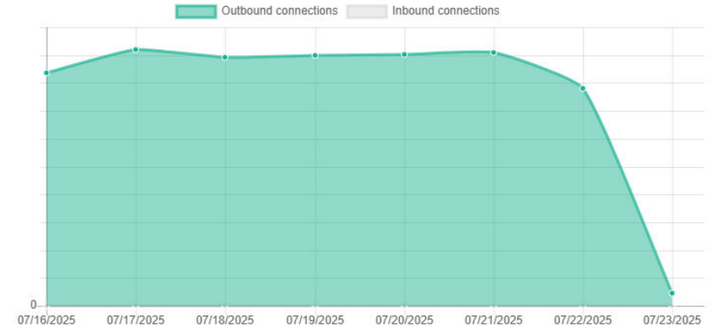
Top 3 Threats (Connection count)

China - IPs

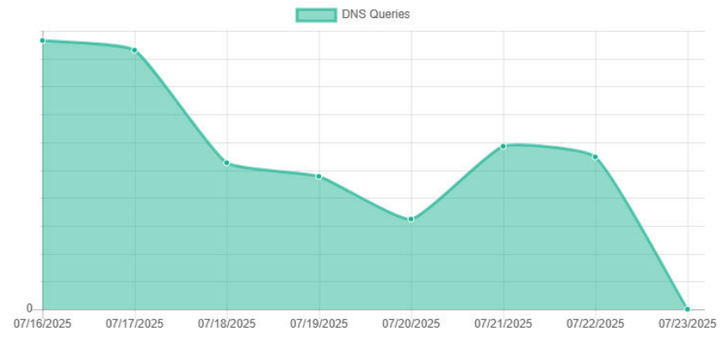
Bulgaria - IPs

India - IPs

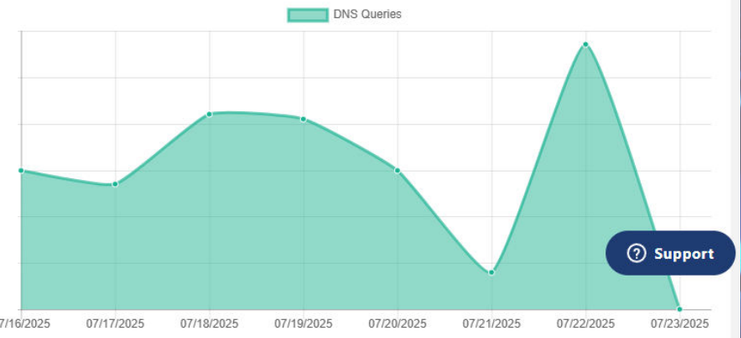
Inbound and Outbound connections (IP Defense)



DNS Defense blocked queries



Roaming Defense blocked queries



Support

Before ThreatSTOP: Vulnerability Assessment

Limited Visibility

No comprehensive view of network traffic or potential intrusion attempts across our SCADA systems

Reactive Posture

Security incidents detected only after damage occurred, with extended remediation timeframes

Resource Constraints

Small IT team managing critical infrastructure with minimal dedicated cybersecurity staff

Our regional threat assessment identified water utilities as high-priority targets for nation-state actors and cybercriminals.

Implementation Strategy & Deployment

What We Implemented

1. **Assessment Phase**

   Comprehensive network audit and vulnerability scan of OT/IT infrastructure

2. **ThreatSTOP Integration**

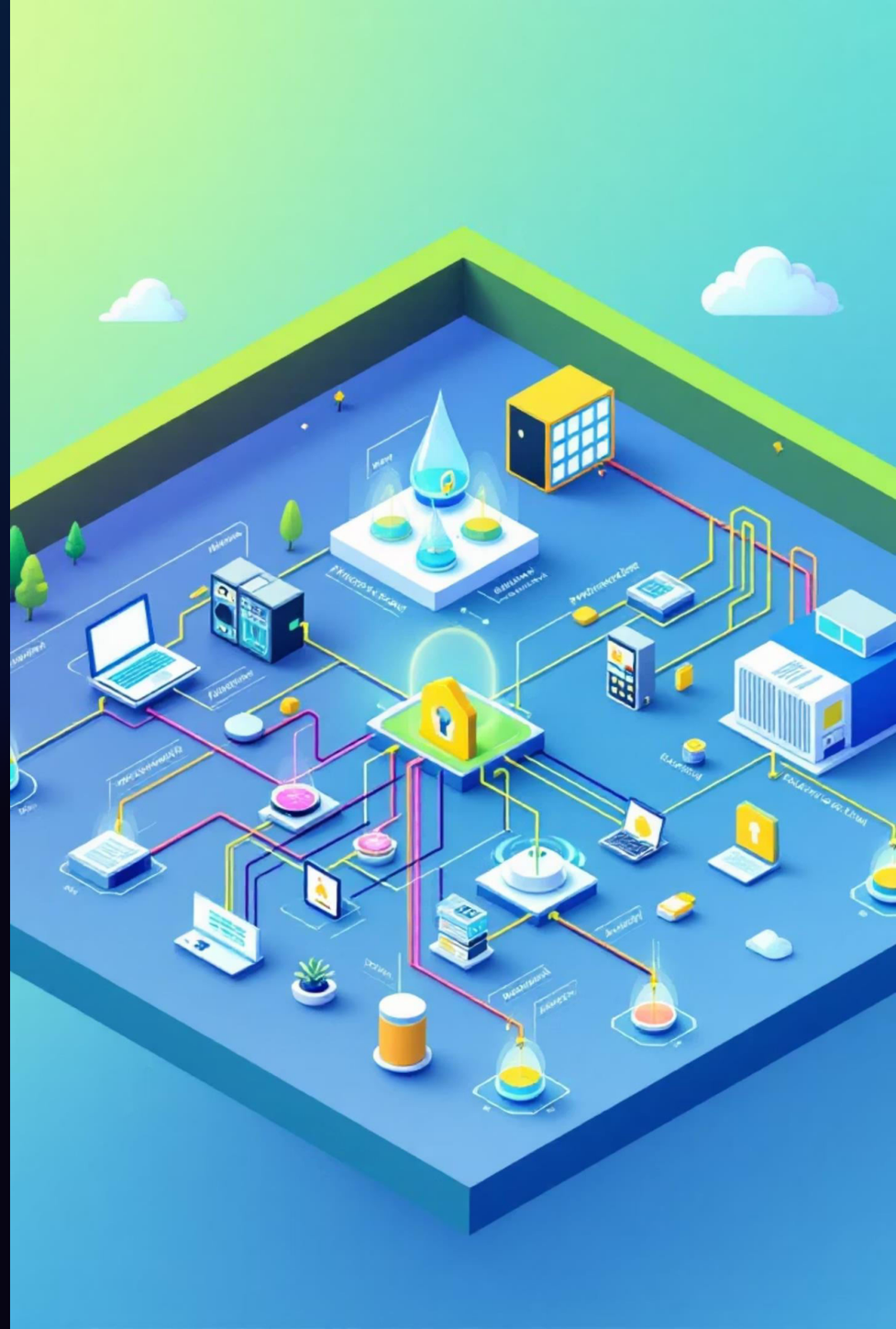
   Deployment of DNS Defense and IP Defense across critical control systems

3. **Policy Configuration**

   Implementation of ICS-CERT and water sector-specific threat intelligence feeds

4. **Training & Monitoring**

   Staff training on new dashboard alerts and incident response procedures



Measurable Benefits & Outcomes

94%

Blocked Threats

Percentage of malicious connection attempts automatically blocked at network edge

68%

Response Time

Reduction in time from threat detection to mitigation

Less than One Hour

Time to Value

Total time required to deploy complete solution across our infrastructure

Real-World Impact

- Complete visibility into attempted connections to known-bad IP addresses
- Automated blocking prevents malware command-and-control communications
- Early warning of potential lateral movement attempts between network zones
- Integration with existing SIEM provides comprehensive security picture
- Tools like ThreatSTOP act as force multipliers for small, resource-constrained agencies. Instead of hiring an additional full-time or part-time employee, organizations can deploy automation to strengthen security posture and reduce workload.
- For many public sector environments, hiring another FTE is not feasible due to budget limitations. A fully burdened security hire can cost 1.5 times their base salary. ThreatSTOP helps close that gap by delivering protections that may not be attainable even with an additional hire—offering both operational relief and enhanced defense.

ThreatSTOP

Recommendations for Utility Providers

Segment Thoroughly

Implement strict segmentation between IT, OT, and SCADA networks with monitored interconnection points

Layer Defenses

Deploy overlapping security technologies that provide defense-in-depth against sophisticated attacks

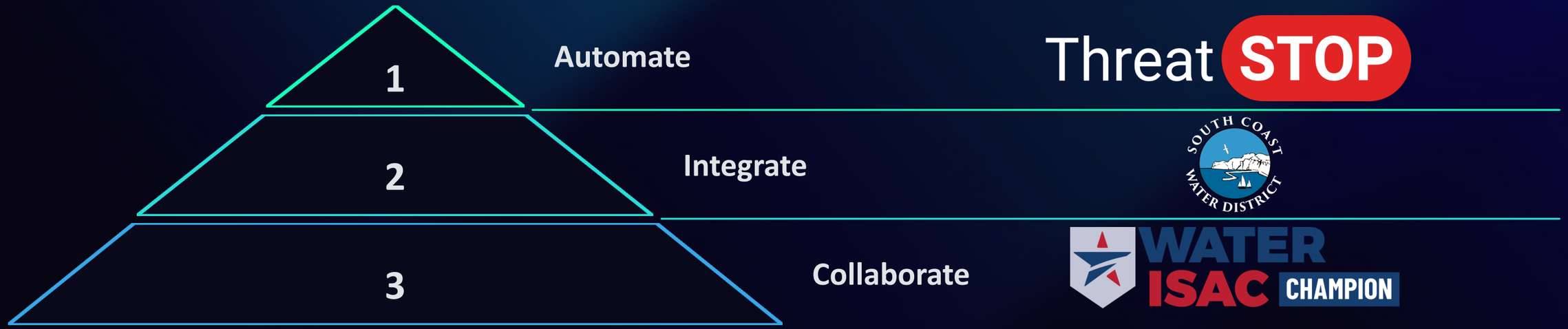
Train Everyone

Security awareness must extend beyond IT to all operations staff who interact with control systems

Collaborate Actively

Share threat intelligence with sector ISACs and participate in joint exercises with other utilities

Key Takeaways



1. **Automate defensive responses** to reduce the burden on limited staff while maintaining 24/7 protection against emerging threats.

2. **Integrate security solutions** with existing infrastructure to maximize ROI and minimize disruption to critical operations.

3. **Collaborate across the sector** by sharing intelligence and best practices through WaterISAC and similar organizations.

Securing Our Water Infrastructure Together

Contact Information

Dustin Luedke, Sales Coordinator with ThreatSTOP

dluedke@threatstop.com

(760) 542-1550 ext.4444

SCAN ME

Next Steps from WaterISAC

- Register for Exclusive Trial: Free ThreatSTOP Trial
- Use code WISAC2025 for a free trial.
- No credit card required. No commitment.
- WaterISAC members receive exclusive pricing.
- All webinar attendees are welcome to try ThreatSTOP – WaterISAC member status will be verified after sign-up